

## SFS-EN ISO/IEC 27002:2022

### Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot

Information security, cybersecurity  
and privacy protection. Information  
security controls (ISO/IEC 27002:2022)

Vahvistettu 2022-11-18

1 (322)

2. painos

Korvaa standardien ISO/IEC 27002:2022:fi painoksen 1 ja SFS-EN ISO/IEC 27002:2017 painoksen 1

2nd edition

Replaces standards ISO/IEC 27002:2022:fi edition 1 and SFS-EN ISO/IEC 27002:2017 edition 1

Ristiriitatapauksissa pätee englanninkielinen teksti.  
Suomenkielisen käänökseen päivämäärä 2022-12-09In case of interpretation disputes the English text applies.  
Date of translation into Finnish 2022-12-09

## Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot

### Information security, cybersecurity and privacy protection.

### Information security controls (ISO/IEC 27002:2022)

Tämä standardi sisältää eurooppalaisen standardin EN ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection. Information security controls (ISO/IEC 27002:2022)" englanninkielisen tekstin.

Standardi sisältää myös englanninkielisen tekstin suomenkielisen käänöksen.

Eurooppalainen standardi EN ISO/IEC 27002:2022 on vahvistettu suomalaiseksi kansalliseksi standardiksi.

This standard consists of the English text of the European Standard EN ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection. Information security controls (ISO/IEC 27002:2022)".

The Standard also contains a Finnish translation of the English text.

The European Standard EN ISO/IEC 27002:2022 has the status of a Finnish national standard.

Standardista vastaava toimialayhteisö:  
Suomen Standardisoimislaitto SFS ry

Standards writing body responsible for the standard:  
Finnish Standards Association SFS

**Suomen Standardisoimislaitto SFS ry**  
Malminkatu 34, PL 130, 00101 Helsinki  
p. 09 149 9331, [www.sfs.fi](http://www.sfs.fi), [sales@sfs.fi](mailto:sales@sfs.fi)

**Finnish Standards Association SFS**  
P.O. Box 130, FI-00101 Helsinki, (Malminkatu 34)  
Tel. +358 9 149 9331, [www.sfs.fi](http://www.sfs.fi), [sales@sfs.fi](mailto:sales@sfs.fi)

## **Monta tapaa tilata**

### **Pysy ajan tasalla**

Tietopalvelumme tarjoaa monia helpoja tapoja pysyä ajan tasalla toimialaasi kuuluvista standardeista. Lue lisää [www.sfs.fi/tietopalvelu](http://www.sfs.fi/tietopalvelu).

Haluatko tietoa uusista julkaisuista sähköpostilla?

Tilaa sähköinen uutiskirje haluamastasi aiheesta [www.sfs.fi/uutiskirjetilaus](http://www.sfs.fi/uutiskirjetilaus).

### **Asiakaspalvelu auttaa**

SFS:n asiakaspalvelusta voit tilata kaikki tarvitsemasi julkaisut.

Ota yhteyttä [sales@sfs.fi](mailto:sales@sfs.fi) tai p. 09 1499 3353.

### **SFS-kauppa**

Verkkokaupassa voit tarkistaa julkaisujen ajantasaiset tiedot. Voit myös ladata useimmat standardit omalle koneellesi saman tien ja tilata uusia julkaisuja. Astu sisään osoitteessa [sales.sfs.fi](http://sales.sfs.fi).

### **SFS Online**

SFS Online -palvelussa oma standardikokoelmanne on aina ajan tasalla internetissä. Kiinnostuitko? Kysy lisää SFS:n asiakaspalvelusta [sales@sfs.fi](mailto:sales@sfs.fi).

-  [facebook.com/Stardardeista](https://facebook.com/Stardardeista)
-  [@standardeista](https://twitter.com/@standardeista)
-  [Suomen Standardisoimisliitto SFS ry](https://www.linkedin.com/in/suomen-standardisoimisliitto-sfs-ry/)

## **SFS-EN ISO/IEC 27002:2022**

Aihealueluokitus: SFS/ICS 35.030; 03.100.06; 03.100.12; 03.100.70; 96.030.10

Julkaistu: SFS 2022-12

Copyright © SFS. Osittainenkin julkaiseminen tai kopiointi sallittu vain SFS:n luvalla.  
Tätä julkaisua myy Suomen Standardisoimisliitto SFS

© ISO/IEC 2022 – All rights reserved

© SFS 2022 for the translation

# SFS-EN ISO/IEC 27002:2022

EUROOPPALAINEN STANDARDI  
EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

EN ISO/IEC 27002

November 2022

ICS 35.030

Supersedes EN ISO/IEC 27002:2017

English Version

## Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Moyens de maîtrise de l'information (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

This European Standard was approved by CEN on 30 October 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2022 CEN

All rights of exploitation in any form and by any means reserved  
worldwide for CEN national Members

Ref. No. EN ISO/IEC 27002:2022: E

## Sisällystoiminta

Sivu

Eurooppalainen esipuhe.....	5
Esipuhe (ISO).....	6
Johdanto.....	7
1 Soveltamisala .....	10
2 Velvoittavat viitaukset.....	10
3 Termit, määritelmät ja lyhenteet .....	10
3.1 Termit ja määritelmät .....	10
3.2 Lyhenteet.....	15
4 Tämän asiakirjan rakenne .....	17
4.1 Kohdat.....	17
4.2 Teemat ja attribuutit .....	17
4.3 Hallintakeinon kuvaus .....	18
5 Organisaatioon liittyvät hallintakeinot .....	19
5.1 Tietoturvallisuutta koskevat toimintaperiaatteet .....	19
5.2 Tietoturvaroolit ja -vastuut .....	21
5.3 Tehtävien eriyttäminen .....	22
5.4 Johdon vastuu .....	23
5.5 Yhteydet viranomaisiin .....	23
5.6 Yhteydet osaamisyhteisöihin .....	24
5.7 Uhkatiedon seuranta .....	25
5.8 Tietoturvallisuus projektinhallinnassa .....	26
5.9 Tietojen ja niihin liittyvien omaisuuserien luettelo .....	28
5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö .....	29
5.11 Omaisuuden palauttaminen .....	30
5.12 Tiedon luokittelu .....	31
5.13 Tiedon merkintä .....	33
5.14 Tietojen siirtäminen .....	34
5.15 Pääsynhallinta .....	36
5.16 Identiteetin hallinta .....	38
5.17 Tunnistautumistiedot .....	39
5.18 Pääsyoikeudet .....	41
5.19 Tietoturvallisuus toimittajasuheteissa .....	43
5.20 Toimittajasopimusten tietoturvallisuus .....	45
5.21 Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa .....	47
5.22 Toimittajien palvelujen seuranta, katselointi ja muutoksenhallinta .....	49
5.23 Pilvipalvelujen tietoturvallisuus .....	50
5.24 Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu .....	52
5.25 Tietoturvatapahtumien arvointi ja niitä koskevien päätösten tekeminen .....	54
5.26 Tietoturvahäiriöihin reagointi .....	54
5.27 Tietoturvahäiriöstä oppiminen .....	55
5.28 Todisteiden kerääminen .....	56
5.29 Tietoturvallisuus häiriötilanteessa .....	57
5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa .....	58
5.31 Lainsäädäntöön, asetuksiin, viranomaismäääräyksiin ja sopimuksiin sisältyvät vaatimukset .....	59
5.32 Immateriaalioikeudet .....	61
5.33 Tallenteiden suojaaminen .....	62
5.34 Tietosuoja ja henkilötietojen suojaaminen .....	63
5.35 Tietoturvallisuuden riippumaton katselointi .....	64
5.36 Tietoturvallisuutta koskevien toimintaperiaatteiden, sääntöjen ja standardien noudattaminen .....	65
5.37 Dokumentoidut toimintaohjeet .....	66

<b>6</b>	<b>Henkilöstöön liittyvät hallintakeinot</b>	<b>67</b>
6.1	Taustatarkistus.....	67
6.2	Työsuhteen ehdot.....	69
6.3	Tietoturvatietoisuus, -opastus ja -koulutus.....	70
6.4	Kurinpitoprosessi .....	71
6.5	Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut.....	72
6.6	Salassapito- ja vaitiilositoumukset.....	73
6.7	Etätyöskentely .....	74
6.8	Tietoturvatapahtumista raportointi.....	75
<b>7</b>	<b>Fyysiset hallintakeinot</b>	<b>76</b>
7.1	Fyysiset turva-alueet.....	76
7.2	Kulunvalvonta .....	77
7.3	Toimistojen, tilojen ja laitteistojen suojaus.....	79
7.4	Fyysisen turvallisuuden valvonta .....	80
7.5	Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan.....	81
7.6	Turva-alueilla työskentely .....	82
7.7	Puhdas pöytä ja puhdas näyttö .....	82
7.8	Laitteiden sijoitus ja suojaus .....	83
7.9	Toimitilojen ulkopuolelle viedyn omaisuuden turvallisuus.....	84
7.10	Tallennusvälineet .....	85
7.11	Tukipalvelut .....	87
7.12	Kaapeloinnin turvallisuus.....	88
7.13	Laitteiden huolto .....	89
7.14	Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen .....	90

<b>8 Teknologiset hallintakeinot</b>	<b>91</b>
8.1 Käyttäjien päätelaitteet	91
8.2 Ylläpito-oikeudet	93
8.3 Tietoihin pääsyn rajoittaminen	94
8.4 Pääsy lähdekoodiin	96
8.5 Turvallinen todentaminen	97
8.6 Kapasiteetinhallinta	99
8.7 Haittaohjelmilta suojautuminen	100
8.8 Teknisten haavoittuvuuksien hallinta	102
8.9 Konfiguraationhallinta	105
8.10 Tietojen poistaminen	107
8.11 Tietojen peittäminen	108
8.12 Tietovuotojen estäminen	110
8.13 Tietojen varmuuskopiointi	111
8.14 Tietojenkäsittelypalvelujen vikasiertoisuus	112
8.15 Lokikirjaukset	113
8.16 Valvontatoiminnot	116
8.17 Kellojen synkronointi	118
8.18 Ylläpito- ja hallintasovellukset	119
8.19 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin	120
8.20 Verkkoturvallisuus	121
8.21 Verkkopalvelujen turvaaminen	122
8.22 Verkkojen eriyttäminen	123
8.23 Verkkosuodatus	124
8.24 Salauksen käyttö	125
8.25 Turvallinen kehittämisen elinkaari	127
8.26 Sovelluksia koskevat turvallisuusvaatimukset	128
8.27 Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet	130
8.28 Turvallinen ohjelmosti	132
8.29 Tietoturvatestaus kehitys- ja hyväksyntävaiheissa	135
8.30 Ulkoistettu kehittäminen	136
8.31 Kehitys-, testaus- ja tuotantoypäristöjen erottaminen	137
8.32 Muutoksenhallinta	139
8.33 Testauksessa käytettävät tiedot	140
8.34 Tietojärjestelmien suojaus auditointitestauksen aikana	141
<b>Liite A (opastava) Attribuuttien käyttö</b>	<b>142</b>
<b>Liite B (opastava) Standardin ISO/IEC 27002:2022 (tämä asiakirja) vastaavuus standardiin ISO/IEC 27002:2013</b>	<b>154</b>
<b>Kirjallisuus</b>	<b>161</b>

## Eurooppalainen esipuhe ([EN](#))

Standardin ISO/IEC 27002:2022 on laatinut ISO (International Organization for Standardization) ja IEC:n (International Electrotechnical Commission) yhteinen tekninen komitea ISO/IEC JTC 1 *Information technology*. CENin ja CENELE Cin yhteinen tekninen komitea CEN-CENELEC/JTC 13 *Cybersecurity and Data Protection*, jonka sihteeristönä toimii DIN, on hyväksynyt sen eurooppalaiseksi standardiksi EN ISO/IEC 27002:2022.

Tälle eurooppalaiselle standardille on annettava kansallisen standardin asema joko julkaisemalla standardin kanssa yhtäpitävä teksti tai vahvistamalla asiakirja kansalliseksi standardiksi toukokuun 2023 loppuun mennessä. Lisäksi tämän standardin kanssa ristiriitaiset kansalliset standardit on kumottava toukokuun 2023 loppuun mennessä.

Jotkin tämän asiakirjan yksityiskohdat saattavat olla patenttioikeuksin suojaatua. CEN ja CENELEC eivät vastaa tällaisten patenttioikeuksien yksilöimisestä.

Tämä asiakirja korvaa standardin EN ISO/IEC 27002:2017.

Tästä asiakirjasta voi lähetää palautetta tai kysymyksiä kunkin maan kansalliselle standardisointijärjestölle. Järjestöt on lueteltu CENin ja CENELE Cin verkkosivuilla.

CENin ja CENELE Cin sääntöjen mukaan seuraavien maiden standardisointijärjestöt ovat velvollisia vahvistamaan tämän eurooppalaisen standardin: Alankomaat, Belgia, Bulgaria, Espanja, Irlanti, Islanti, Iso-Britannia, Italia, Itävalta, Kreikka, Kroatia, Kypros, Latvia, Liettua, Luxemburg, Malta, Norja, Pohjois-Makedonia, Portugali, Puola, Ranska, Romania, Ruotsi, Saksa, Serbia, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tšekki, Turkki, Unkari ja Viro.

### Voimaansaattamisilmoitus

CEN ja CENELEC ovat hyväksyneet standardin ISO/IEC 27002:2022 eurooppalaiseksi standardiksi EN ISO/IEC 27002:2022 sellaisenaan.

## Esipuhe (ISO) ([EN](#))

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostavat maailmanlaajuisen standardisointiin erikoistuneen järjestelmän. ISOn tai IEC:n kansalliset jäsenjärjestöt osallistuvat kansainvälisen standardien laadintaan näiden järjestöjen perustamissa teknisissä komiteoissa, jotka käsittelevät eri tekniikan aloja. ISOn ja IEC:n tekniset komiteat tekevät yhteistyötä molempia kiinnostavilla aihealueilla. Työhön osallistuvat myös muut kansainväliset ISOn tai IEC:n kanssa yhteistyössä olevat viranomaiset ja muut organisaatiot.

Tämän asiakirjan laatimiseen käytetyt ja sen ylläpitoon tarkoitettut menettelyt on kuvattu ISOn ja IEC:n sääntöjen osassa 1 (ISO/IEC Directives, Part 1). Erityisesti olisi huomioitava, että erityyppisille asiakirjoille on erilaiset hyväksymiskriteerit. Tämä asiakirja on laadittu ISOn ja IEC:n sääntöjen osassa 2 esitettyjen julkaisujen sisältöä, rakennetta ja asettelua koskevien sääntöjen mukaisesti (katso [www.iso.org/directives](http://www.iso.org/directives) tai [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

Jotkin tämän asiakirjan yksityiskohdat saattavat olla patenttioikeuksin suojaatua. ISO ja IEC eivät vastaa tällaisten patenttioikeuksien yksilöimisestä. Tämän asiakirjan laadintavaiheessa yksilöityjen patenttioikeuksien tarkat tiedot esitetään tämän asiakirjan johdannossa, ISOn ylläpitämässä patentointia koskevien ilmoitusten luettelossa ([www.iso.org/patents](http://www.iso.org/patents)) tai IEC:n ylläpitämässä patentointia koskevien ilmoitusten luettelossa (<http://patents.iec.ch>).

Kauppanimet on annettu pelkästään standardin käyttäjien avuksi, eikä tuotemerkkien mainitseminen standardissa tarkoita, että ISO suosittelee kyseisiä tuotteita.

Standardien käytön vapaaehtoisuudesta, vaativuudenmukaisuuden arviontiin liittyvien ISOn käyttämien termien ja ilmaisuojien merkityksestä sekä kaupan teknisiä esteitä koskevan WTO:n sopimuksen periaatteiden noudattamisesta ISOn toiminnassa on tietoa osoitteessa [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). IEC:n vastaavista käytännöistä on tietoa osoitteessa [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

Tämän asiakirjan on laatinut ISOn ja IEC:n yhteisen teknisen komitean ISO/IEC JTC 1 *Information technology* alakomitea SC 27 *Information security, cybersecurity and privacy protection*.

Tämä kolmas painos kumoaa ja korvaa toisen painoksen (ISO/IEC 27002:2013), jota on uudistettu teknisesti. Tämä koskee myös teknisiä korjauksia ISO/IEC 27002:2013/Cor. 1:2014 ja ISO/IEC 27002:2013/Cor. 2:2015.

Suurimmat muutokset edelliseen painokseen ovat seuraavat:

- Asiakirjan otsikkona on muokattu.
- Asiakirjan rakennetta on muokattu siten, että hallintakeinot esitetään yksinkertaisen luokittelun ja siihen liittyvien attribuuttien avulla.
- Osa hallintakeinoista on yhdistetty, osa on poistettu ja useita uusia hallintakeinoja on lisätty. Asiakirjan hallintakeinojen vastaavuus suhteessa edellisen painoksen hallintakeinoihin on esitetty [liitteessä B](#).

Tämä standardin ISO/IEC 27002:2022 korjattu versio sisältää seuraavat korjaukset:

- Rikkinäiset hyperlinkit on korjattu.
- [Kohdan 5.22](#) taulukossa ja [taulukossa A.1](#) (rivillä [5.22](#)) tunniste #Tietoturvallisuuden\_varmentaminen on siirretty Tietoturvan osa-alueet -sarakkeesta Toiminnalliset kyvykkyydet -sarakkeeseen.

Tästä asiakirjasta voi lähettää palautetta ja kysymyksiä kunkin maan kansalliselle standardisointijärjestölle. Järjestöt on lueteltu osoitteissa [www.iso.org/members.html](http://www.iso.org/members.html) ja [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Johdanto ([EN](#))

### 0.1 Tausta ja toimintaympäristö

Tämä asiakirja on tarkoitettu kaikentyyppisille ja -kokoisille organisaatioille. Asiakirja on tarkoitettu viiteasiakirjaksi tietoturvariskien käsittelyn hallintakeinojen määrittämisen ja toteuttamiseen standardin ISO/IEC 27001 mukaisessa tietoturvallisuuden hallintajärjestelmässä. Asiakirja voidaan hyödyntää myös ohjeistuksena organisaatioissa, jotka määrittävät ja toteuttavat yleisesti hyväksyttyjä tietoturvallisuuden hallintakeinoja. Asiakirja on tarkoitettu käytettäväksi toimiala- tai organisaatiokohtaisten tietoturvallisuuden hallintaohjeiden kehittämisesä, ja siinä otetaan huomioon toimialaa tai organisaatiota koskevat tietoturvallisuuden riskiympäristöt. Muut kuin tähän asiakirjaan sisältyvät organisaatio- tai toimintaympäristökohtaiset hallintakeinot voidaan tarvittaessa määrittää riskien arvioinnin avulla.

Kaiken tyyppiset ja kokoiset organisaatiot (mukaan lukien julkinen ja yksityinen sektori, voittoa tavoittelevat ja voittoa tavoittelemattomat organisaatiot) luovat, keräävät, käsitlevät, tallentavat, siirtävät ja hävittävät tietoa monissa muodoissa, mukaan lukien sähköisessä, fyysisessä ja suullisessa (esim. keskustelut ja esitykset) muodossa.

Arvokasta tietoa on muukin, kuin kirjalliset sanat, numerot ja kuvat. Tietämys, konseptit, ideat ja brändit ovat esimerkkejä tiedon aineettomista muodoista. Yhteen kytkeytyneessä maailmassa tiedot ja niihin liittyvät omaisuuserät ansaitsevat tai vaativat erilaisilta riskilähteiltä suojaamista riippumatta siitä, ovatko riskit sitten luonnollisia, tahattomia tai tahallisia.

Tietoturvallisuus saavutetaan toteuttamalla soveltuva hallintakeinojen järjestelmä, joka koostuu toimintaperiaatteista, säännöistä, prosesseista, menettelyistä, organisaatorakenteista sekä ohjelmisto- ja laitteistotoimintoista. Täytääkseen turvallisuuteen ja liiketoimintaan liittyvät tavoitteensa organisaation olisi määriteltyä ja toteutettava sekä seurattava, katselmoitava ja parannettava näitä hallintakeinoja. Tietoturvallisuuden hallintajärjestelmä (esim. standardin ISO/IEC 27001 mukainen) noudattaa kokonaivaltaista ja koordinoitua lähestymistapaa organisaation tietoturvariskien suhteen, jotta voidaan määritää ja toteuttaa kattava valikoima tietoturvallisuuden hallintakeinoja, jotka toimivat yhtenäisen kokonaiskohtamisjärjestelmän puitteissa.

Monia tietojärjesteliä tai niiden hallintaa ja käyttöä ei ole suunniteltu turvallisiksi standardin ISO/IEC 27001 ja tämän asiakirjan määrittelyjen mukaisesti. Vain teknologian keinoin saavutettavissa olevassa turvallisuuden tasolla on rajansa, ja sitä olisikin tuettava asianmukaisilla hallinnollisilla menettelyillä ja organisaation prosesseilla. Tarvittavien hallintakeinojen tunnistaminen edellyttää huolellista suunnittelua ja paneutumista yksityiskohtiin riskien käsittelyn aikana.

Onnistuneen tietoturvallisuuden hallintajärjestelmän edellytyksenä on organisaation koko henkilöstön tuki. Edellytyksenä voi olla myös muiden sidosryhmien, kuten osakkeenomistajien tai toimittajien, osallistuminen. Lisäksi saatetaan tarvita myös aihealueen asiantuntijoiden neuvoja.

Soveltuva, riittävä ja vaikuttava tietoturvallisuuden hallintajärjestelmä tarjoaa organisaation joholle ja sidosryhmille varmuuden siitä, että niiden tietoja ja niihin liittyviä omaisuuseriä säilytetään kohtuullisesti suojuina ja turvattuna uhkila ja vaaroilta, jotta organisaatio voi saavuttaa ilmoitetut liiketoimintatavoitteensa.

## 0.2 Tietoturvallisuutta koskevat vaatimukset

Organisaation ensiarvoisen tärkeää määrittää tietoturvallisuutta koskevat vaatimuksensa. Tietoturvallisuutta koskeville vaatimuksilla on kolme pääasiallista lähdettä:

- a) Ensimmäinen lähde on organisaation suorittama riskien arvointi, jossa otetaan huomioon organisaation yleinen liiketoimintastrategia ja liiketoiminnan yleiset tavoitteet. Tämä voidaan mahdollistaa tai tästä voidaan tukea tietoturvallisuuteen liittyvien riskien kohdennetulla arvioinnilla. Tämän olisi johdettava siihen, että määritetään hallintakeinot, jotka tarvitaan varmistamaan, että organisaation jäännösriskit täytyvät riskien hyväksymiskriteerit.
- b) Toisen lähteen muodostavat laki ja asetusten sekä viranomaismääräysten ja sopimusten asettamat vaatimukset, jotka organisaation ja sen sidosryhmien (kauppanumppanien, palveluntuottajien jne.) on täytettävä, sekä niiden sosiokulttuurinen ympäristö.
- c) Kolmantena lähteenä ovat organisaation omien toimintojensa tueksi kehittämät tiedon elinkaaren kaikkia vaiheita koskevat periaatteet, tavoitteet ja liiketoimintavaatimukset.

## 0.3 Hallintakeinot

Hallintakeino on toimenpide, jolla riskiä muutetaan tai jolla se säilytetään. Osa tässä asiakirjassa esitetystä hallintakeinoista muuttaa riskiä ja osa säilyttää sen. Esimerkiksi tietoturvapolitiikalla voidaan vain säilyttää riski, kun taas tietoturvapolitiikan noudattamisella sitä voidaan muuttaa. Lisäksi osa hallintakeinoista kuvalee samaa yleisluontoista toimenpidettä eri riskikonteksteissa. Tässä asiakirjassa esitetään yleisluontoinen joukko tietoturvallisuuden hallintakeinoja, jotka kohdistuvat organisaatioon, henkilöstöön sekä fyysisiin ja teknologisiin seikkoihin ja perustuvat kansainvälisesti tunnustettuihin parhaisiin käytäntöihin.

## 0.4 Hallintakeinojen määrittäminen

Hallintakeinojen määrittäminen on riippuvaista organisaation pääöksistä, jotka tehdään selkeästi rajatun riskien arvioinnin jälkeen. Tunnistettuihin riskeihin kohdistuvien pääösten olisi perustuttava riskien hyväksymiskriteereihin, riskien käsittelyvaihtoehtoihin ja organisaatiossa sovellettavaan riskienhallinnan toimintamalliin. Hallintakeinojen määrittämisessä olisi otettava huomioon myös kaikki asianmukaiset kansalliset ja kansainväliset lait ja viranomaismääräykset. Hallintakeinojen määrittäminen riippuu myös siitä, miten hallintakeinot ovat keskinäisessä vuorovaikutuksessa ja tarjoavat parempaa suojaa.

Organisaatiot voivat tarpeen mukaan suunnitella hallintakeinot itse tai tunnistaa ne muista lähteistä. Tällaisten hallintakeinojen määrittelyssä organisaation olisi tarkasteltava hallintakeinon toteuttamiseen ja käyttöön tarvittavia resursseja ja investointeja suhteessa sillä saavutettavaan liiketoiminnalliseen arvoon. Teknisessä raportissa ISO/IEC TR 27016 annetaan ohjeistusta sellaisten pääösten tueksi, jotka koskevat tietoturvallisuuden hallintajärjestelmään tehtäviä investointeja ja niiden taloudellisia seurausia suhteessa vaadittaviin resursseihin.

Hallintakeinojen toteuttamiseen käytettävien resurssien ja kyseisten hallintakeinojen puuttumisesta mahdollisesti seuraavien turvallisuushäiriöiden vaikutusten välillä olisi oltava tasapaino. Riskien arvioinnin tulosten avulla olisi voitava määrittää soveltuват hallintatoimenpiteet ja prioriteetit, joilla tietoturvariskejä hallitaan ja joiden perusteella toteutetaan kyseisiltä riskeiltä suojaavat määritetyt hallintakeinot.

Jotakin tämän asiakirjan hallintakeinoja voidaan pitää yleisinä ohjeellisina tietoturvallisuuden hallintaperiaatteina ja useimpien organisaatioiden käyttöön soveltuvinä. Lisätietoja hallintakeinojen määrittämisestä ja muista riskien käsittelyn vaihtoehtoista löytyy standardista ISO/IEC 27005.

## 0.5 Organisaatiokohtaisten ohjeiden laatiminen

Tätä asiakirjaa voidaan pitää organisaatiokohtaisten ohjeiden kehittämisen lähtökohtana. Kaikkia tässä asiakirjassa esitettyjä hallintakeinoja ja ohjeistuksia ei voida soveltaa kaikkiin organisaatioihin. Organisaation tiettyjen tarpeiden ja tunnistettujen riskien käsittelyyn saatetaan tarvita myös tämän asiakirjan ulkopuolisia hallintakeinoja ja ohjeistuksia. Kun laaditaan lisähohjeita tai hallintakeinoja sisältäviä asiakirjoja, voi olla hyödyllistä sisällyttää niihin tarvittavat viittaukset tämän asiakirjan kohtiin tulevaa käyttöä helpottamaan.

## 0.6 Elinkaareen liittyvät näkökohdat

Tiedolla on elinkaarena aina luomisesta hävittämiseen. Tiedon arvo ja sitä koskevat riskit voivat vaihdella tämän elinkaaren aikana (esim. yhtiön tilinpäätöstietojen luvaton paljastuminen tai niiden varastaminen ei ole merkityksellistä, kun tiedot on julkistettu, mutta niiden eheys on silti ensiarvoisen tärkeää), joten tietoturvallisuus on jossain määrin tärkeää elinkaaren kaikissa vaiheissa.

Tietojärjestelmillä ja tietoturvallisuuteen liittyvillä omaisuuserillä on elinkaaret, joiden aikana ne perustetaan, määritellään, suunnitellaan, kehitetään, testataan ja toteutetaan, jolloin niitä käytetään ja ylläpidetään ja jonka päätyessä ne poistetaan käytöstä ja hävitetään. Tietoturvallisuutta olisi tarkasteltava kaikissa vaiheissa. Uusien järjestelmien kehittämисprojektit ja olemassa oleviin järjestelmiin tehtävät muutokset tarjoavat mahdollisuuden parantaa turvallisuuden hallintakeinoja organisaation riskien ja häiriöistä opittujen asioiden perusteella.

## 0.7 Muut asiaan liittyvät kansainvälist standardit

Tässä asiakirjassa esitettävä ohjeistus koskee laajaa valikoimaa tietoturvallisuuden hallintakeinoja, joita käytetään yleisesti monissa organisaatioissa. Standardisarjan ISO/IEC 27000 muissa asiakirjoissa esitetään täydentäviä ohjeita ja vaatimuksia tietoturvallisuuden kokonaishallintaprosessin muista puolista.

Standardissa ISO/IEC 27000 esitellään tietoturvallisuuden hallintajärjestelmät ja standardisarja yleisellä tasolla. Standardi ISO/IEC 27000 sisältää termiston, jossa määritellään useimmat standardisarjassa käytetyt termit. Lisäksi siinä kuvailaan kunkin sarjaan kuuluvan asiakirjan soveltamisala ja tavoitteet.

Lisäksi on laadittu toimialakohtaisia standardeja, joissa esitellään tiettyihin aihealueisiin kohdennettuja hallintakeinoja (kuten ISO/IEC 27017 ja pilvipalvelut, ISO/IEC 27701 ja tietosuoja, ISO/IEC 27019 ja energia, ISO/IEC 27011 ja teleliikenneorganisaatiot sekä ISO 27799 ja terveys). Nämä standardit on sisällytetty kirjallisuusluetteloon, ja osaan niistä viitataan myös mm. [kohtien 5–8](#) ohjeistuksessa.

## 1 Soveltamisala (EN)

Tässä asiakirjassa esitetään yleislentoisten tietoturvallisuuden hallintakeinojen viitejoukko sekä niitä koskevat toteuttamisohjeet. Tämä opas on tarkoitettu käyttöön organisaatioille

- a) jotka kuuluvat standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toimintaympäristöön
- b) jotka toteuttavat tietoturvallisuuden hallintakeinoja, jotka perustuvat kansainvälisti tunnustettuihin parhaisiin käytäntöihin
- c) jotka laativat omia organisaatiokohtaisia tietoturvallisuuden hallintaohjeitaan.

## 2 Velvoittavat viitaukset (EN)

Asiakirja ei sisällä velvoittavia viitauksia.

## 3 Termit, määritelmät ja lyhenteet (EN)

### 3.1 Termit ja määritelmät (EN)

Tässä asiakirjassa käytetään seuraavia termejä ja määritelmiä.

ISO ja IEC ylläpitävät standardisoinnissa käytettäviä termitietokantoja seuraavissa osoitteissa:

- ISO Online browsing platform osoitteessa <https://www.iso.org/obp>
- IEC Electropedia osoitteessa <https://www.electropedia.org/>

#### 3.1.1 pääsynhallinta

varmistetaan, että *omaisuuteen* (3.1.2) pääsevät fyysisesti ja ohjelmallisesti käsiksi vain luulliset tahot ja että pääsyä rajoitetaan liiketoimintaa ja tietoturvallisuutta koskevien vaatimusten perusteella

#### 3.1.2

#### omaisuus; omaisuuserä<sup>1)</sup>

mikä tahansa asia, jolla on arvoa organisaatiolle

HUOM. Tietoturvallisuudesta puhuttaessa omaisuus voidaan jakaa kahteen tyyppiin:

- ensisijaiset omaisuuserät eli
  - tieto
  - liiketoimintaprosessit (3.1.27) ja liiketoiminnot
- kaikentyyppiset tukea antavat omaisuuserät (joihin ensisijaiset omaisuuserät tukeutuvat), kuten
  - laitteistot
  - ohjelmistot
  - verkko

<sup>1)</sup> Kansallinen huomautus: Suomessa ei ole yhtä kattavaa ja vakiintunutta käsittettä tai käänöstä sanalle *asset*. Sillä viitataan esim. omaisuudenhallinnassa johonkin *omaisuuteen* tai joihinkin *suojattaviin omaisuuseriin* ja yhteiskunnan turvallisuuden standardisoinnissa puhutaan *suojattavista resursseista*. Tässä standardissa käänösten *omaisuus* ja *omaisuuserä* on katsottu parhaiten palvelevan tämän standardin tarkoitusta laajempana yläkäsitteenä. On kuitenkin tärkeää tiedostaa, että termi sisältää myös muuta kuin varsinaista omaisuutta. Hyvä esimerkki tästä on henkilöstö, joka on organisaatioille voimavara, ei omaisuus.

- *henkilöstö* ([3.1.20](#))
- toimipaikka
- organisaation rakenne.

### **3.1.3**

#### **hyökkäys**

onnistunut tai epäonnistunut yritys tuhota *omaisuuserä* ([3.1.2](#)), muuttaa sitä, poistaa se käytöstä tai saada siihen pääsy tai mikä tahansa yritys paljastaa se, varastaa se tai käyttää sitä luvattomasti

### **3.1.4**

#### **todentaminen**

varmistetaan, että jonkin *tahon* ([3.1.11](#)) jokin ominaisuus on, mitä sen väitetään olevan

### **3.1.5**

#### **aitous**

*tahon* ([3.1.11](#)) ominaisuus olla, mitä se väittää olevansa

### **3.1.6**

#### **hallussapitoketju**

materiaalin osoitettavissa oleva omistajuus, siirtäminen ja sijainti jollain aikavälillä

HUOM. Standardin ISO/IEC 27002 yhteydessä materiaalilla tarkoitetaan tietoja ja niihin liittyviä *omaisuuseriä* ([3.1.2](#)).

[Lähde: ISO/IEC 27050-1:2019, [3.1](#), johon on lisätty huomautus 1.]

### **3.1.7**

#### **luottamuksellinen tieto**

tieto, jota ei ole tarkoitettu luvattomien henkilöiden, *tahojen* ([3.1.11](#)) tai *prosessien* ([3.1.27](#)) käyttöön, eikä tietoja luovuteta tällaisille tahoille

### **3.1.8**

#### **hallintakeino**

riskin säilyttävä tai sitä muuttava toimenpide

HUOM. 1 Hallintakeinoja ovat esimerkiksi kaikki riskin säilyttävät tai sitä muuttavat *prosessit* ([3.1.27](#)), *toimintaperiaatteet* ([3.1.24](#)), laitteet, käytännöt tai muut olosuhteet tai toimenpiteet.

HUOM. 2 Hallintakeinoilla ei aina välittämättä ole haluttua tai oletettua muutosvaikutusta.

[Lähde: ISO 31000:2018, 3.8]

### **3.1.9**

#### **häiriö**

odottettu tai odottamaton häiriötilanne, joka aiheuttaa suunnittelemattoman negatiivisen poikkeaman tuotteiden ja palveluiden organisaation tavoitteiden mukaisessa toimittamisessa

[Lähde: ISO 22301:2019, 3.10]

### **3.1.10**

#### **päätelaite**

verkkoon liitetty tieto- ja viestintäteknon laite

HUOM. Päätelaite voi viitata pöytäkoneeseen, kannettavaan tietokoneeseen, älypuhelimeen, tablettiin, kevytpäätteeseen, tulostimeen tai muuhun erikoislaitteistoon, kuten älymittariin ja esineiden internettiin kytkettyyn laitteeseen.

### 3.1.11

#### taho<sup>1)</sup>

kokonaisuus, joka on jonkin aihealueen toiminnan kannalta oleellinen ja joka on selkeästi tunnistettavissa oleva erillinen kokonaisuus

HUOM. Taho voi olla fyysinen tai looginen.

ESIM. Henkilö, organisaatio, laite, laitejoukko, televiestintäpalvelun ihmistilaaja, SIM-kortti, passi, verkkokortti, ohjelmistosovellus, palvelu tai verkkosivusto.

[Lähde: ISO/IEC 24760-1:2019, [3.1.1](#)]

### 3.1.12

#### tietojenkäsittelypalvelu

kaikki tietoja käsitlevät järjestelmät, palvelut tai infrastruktuurit tai fyysiset tilat, joissa nämä sijaitsevat

[Lähde: ISO/IEC 27000:2018, 3.27, jota on muokattu muuttamalla termin osa "palvelut" yksikkömuotoon.]

### 3.1.13

#### tietoturvaloukkaus

tietoturvallisuuden pettäminen, joka johtaa siirrettävän, varastoidun tai muuten käsitellyn tiedon epätoivottuun tuhoutumiseen, häviämiseen, muuttumiseen, julkaisemiseen tai käyttöön

### 3.1.14

#### tietoturvatapahtuma

taaphtuma, joka ilmaisee mahdollisen *tietoturvaloukkauksen* ([3.1.13](#)) tai *hallintakeinojen* ([3.1.8](#)) pettämisen

[Lähde: ISO/IEC 27035-1:2016, 3.3, jonka alkukielistä määritelmää on muokattu vaihtamalla ilmaus "breach of information security" termiin "information security breach".]

### 3.1.15

#### tietoturvahäiriö

yksi tai useampi toisiinsa liittyvä ja tunnistettu *tietoturvatapahtuma* ([3.1.14](#)), joka voi vahingoittaa organisaation *omaisuutta* ([3.1.2](#)) tai vaarantaa sen toimintoja

[Lähde: ISO/IEC 27035-1:2016, 3.4]

### 3.1.16

#### tietoturvahäiriöiden hallinta

*tietoturvahäiriöiden* ([3.1.15](#)) käsittelyn johdonmukaisen ja vaikuttavan toimintamallin toteuttaminen

[Lähde: ISO/IEC 27035-1:2016, 3.5]

### 3.1.17

#### tietojärjestelmä

joukko sovelluksia, palveluita, tietotekniikkaomaisuuksia tai muita tiedonkäsittelykomponentteja

[Lähde: ISO/IEC 27000:2018, 3.35]

### 3.1.18

#### sidosryhmä

henkilö tai organisaatio, joka voi vaikuttaa johonkin päätökseen tai toimintaan tai joka voi olla tai kokea olevansa päätöksen tai toiminnan vaikutuksen kohteena

[Lähde: ISO/IEC 27000:2018, 3.37]

<sup>1)</sup> Kansallinen huomautus: Joitain termin määritelmään kuuluvia asioita olisi normaalissa käytössä parempi kutsua esim. kokonaisuksiksi, mutta tässä käänöksessä käytetään pääasiallisesti käänösvastinetta taho.

### 3.1.19

#### **kiistämättömyys**

kyky osoittaa, että väitetty tapahtuma tai toimenpide on todella tapahtunut ja että sen väitetty alkuperä pitää paikkansa

### 3.1.20

#### **henkilöstö**

organisaation ohjauksessa työskentelevät henkilöt

HUOM. Henkilöstön käsite kattaa organisaation jäsenet, kuten hallituksen, ylimmän johdon, työntekijät, tilapäiset työntekijät, urakoitsijat ja vapaaehtoiset.

### 3.1.21

#### **henkilötieto; PII**

kaikki sellainen tieto, (a) jonka avulla pystytään luomaan yhteys tiedon ja niihin liittyvän luonnollisen henkilön välille tai (b) joka on tai saattaa olla suoraan tai epäsuorasti yhdistetty luonnolliseen henkilöön

HUOM. Määritelmän "luonnollinen henkilö" on *rekisteröity* ([3.1.22](#)). Jotta voidaan selvittää, onko rekisteröity tunnistettavissa olisi selvitettävä kaikki toimet, jotka tietoa säilyttävän tietosuojatoimijan tai jonkin muun tahon voidaan kohtuullisesti olettaa tekevän, kun se haluaa luoda yhteyden henkilötietojen ja kyseisen luonnollisen henkilön välille.

[Lähde: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

### 3.1.22

#### **rekisteröity**

luonnollinen henkilö, johon *henkilötieto* ([3.1.21](#)) liittyy

HUOM. Lainkäytöalueesta ja tarkemmasta tietosuojan ja yksityisyyden suojan lainsäädännöstä riippuen termin *rekisteröity* sijasta voidaan käyttää synonyymeja *tilaaja* tai *käyttäjä*.

[Lähde: ISO/IEC 29100:2011, 2.11]

### 3.1.23

#### **käsittelijä; henkilötietojen käsittelijä**

tietosuojatoimija, joka käsitlee *henkilötietoja* ([3.1.21](#)) rekisterinpitääjän puolesta ja tämän ohjeiden mukaisesti

[Lähde: ISO/IEC 29100:2011, 2.12]

### 3.1.24

#### **politiikka; toimintaperiaatteet<sup>1)</sup>**

organisaation ylimmän johdon esittämä organisaation tarkoitus ja suunta

[Lähde: ISO/IEC 27000:2018, 3.53]

### 3.1.25

#### **tietosuojavaikutusten arviointi; PIA**

tietosuojavaikutuksia koskeva kokonaisprosessi ([3.1.27](#)), jossa tunnistetaan, analysoidaan, konsultoidaan, arvioidaan ja viestitään tietosuojavaikutuksia sekä suunnitellaan niiden käsittelyä suhteessa *henkilötietojen* ([3.1.21](#)) käsittelyyn organisaation laajemman riskienhallinnan puitteissa

[Lähde: ISO/IEC 29134:2017, 3.7, josta on poistettu huomautus 1.]

### 3.1.26

#### **menettely**

toiminnon tai *prosessin* ([3.1.27](#)) määritelty suoritustapa

[Lähde: ISO 30000:2009, 3.12]

<sup>1)</sup> Kansallinen huomautus: Termiä *toimintaperiaatteet* ei käytetä yhdysvalloissa perusosana.

### 3.1.27

#### prosessei

toisiinsa liittyvät tai vaikuttavat toiminnot, jotka muuttavat panokset tuotoksiksi

[Lähde: ISO 9000:2015, 3.4.1, josta on poistettu huomautukset.]

### 3.1.28

#### tallenne

tieto, jonka organisaatio tai henkilö on tuottanut tai vastaanottanut ja jota se ylläpitää todistusaineistona ja *omaisuuseränä* ([3.1.2](#)) osana laillisia velvoitteitaan tai liiketoimintaansa tietovarantona

HUOM. Laillisilla velvoitteilla tarkoitetaan tässä kaikki laki, viranomaisten ja sopimusten vaatimuksia.

[Lähde: ISO 15489-1:2016, 3.14, johon on lisätty huomautus 1.]

### 3.1.29

#### palautustavoite; RPO (*Recovery Point Objective*)

ajankohta, johon tiedot on tarkoitus palauttaa *häiriön* ([3.1.9](#)) jälkeen

[Lähde: ISO/IEC 27031:2011, 3.12.]

### 3.1.30

#### palautumisaikatavoite; RTO (*Recovery Time Objective*)

aika, jonka kuluessa palveluiden tai tuotteiden vähimmäistaso sekä tukijärjestelmät, -sovelluksen tai -toiminnot on tarkoitus palauttaa *häiriön* ([3.1.9](#)) jälkeen

[Lähde: ISO/IEC 27031:2011, 3.13.]

### 3.1.31

#### luotettavuus

ominaisuus, joka tarkoittaa, että aiotti käytös ja tulokset ovat yhdenmukaisia

### 3.1.32

#### sääntö

hyväksytty periaate tai ohje, missä ilmoitetaan organisaation odotukset siitä, mitä täytyy tehdä ja mikä on sallittua tai kiellettyä

HUOM. Säännöt voidaan ilmaista muodollisesti *kohdennettuina toimintaperiaatteina* ([3.1.35](#)) sekä muissa asiakirjatyypeissä.

### 3.1.33

#### arkaluonteinen tieto

tiedot, jotka on suojaava käytön estymiseltä, luvattomalta käytöltä, muokkaamiselta tai julkaisemiselta, koska niillä olisi haitallisia vaikutuksia henkilölle, organisaatiolle, kansalliselle turvallisuudelle tai yleiselle turvallisuudelle

### 3.1.34

#### uhka

mahdollinen syy epätoivottuun tapahtumaan, josta voi seurata haittaa järjestelmälle tai organisaatiolle

[Lähde: ISO/IEC 27000:2018, 3.74]

### 3.1.35

#### kohdennetut toimintaperiaatteet

organisaation asianmukaisen tason johdon virallisesti esittämä tiettyä aihetta tai asiaa koskeva tarkoitus ja suunta

HUOM. 1 Kohdennetut toimintaperiaatteet voidaan ilmaista *sääntöinä* ([3.1.32](#)) tai organisaation sisäisinä standardeina.

HUOM. 2 Jotkin organisaatiot käyttävät näistä kohdennetuista toimintaperiaatteista myös muita ilmauksia.

HUOM. 3 Tässä asiakirjassa kohdennetut toimintaperiaatteet liittyvät tietoturvallisuuteen.

ESIM. *Pääsynhallintaa* ([3.1.1](#)) koskevat kohdennetut toimintaperiaatteet, puhtaan pöydän ja puhtaan näytön -käytäntöjä koskevat kohdennetut toimintaperiaatteet.

### 3.1.36

#### käyttäjä

*sidosryhmä* ([3.1.18](#)), jolla on pääsy organisaation *tietojärjestelmiin* ([3.1.17](#))

ESIM. *Henkilöstö* ([3.1.20](#)), asiakkaat, toimittajat.

### 3.1.37

#### käyttäjän päätelaite

*päätelaite* ([3.1.10](#)), jonka avulla käyttäjät käyttävät tietojenkäsittelypalveluita

HUOM. Käyttäjän päätelaite voi viitata pöytäkoneeseen, kannettavaan tietokoneeseen, älypuhelimeen, tablettiin, kevytpäätteeseen jne.

### 3.1.38

#### haavoittuvuus

*omaisuuden* ([3.1.2](#)) tai *hallintakeinon* ([3.1.8](#)) heikkous, jota yksi tai useampi *uhka* ([3.1.34](#)) voi käyttää hyväkseen

[Lähde: ISO/IEC 27000:2018, 3.77]

## 3.2 Lyhenteet ([EN](#))

ABAC	attribuuttiperustainen pääsynhallinta
ACL	pääsynhallintalista
BIA	liiketoiminnan vaikutusanalyysi
BYOD	<i>bring your own device</i> eli käytetään omia laitteita
CAPTCHA	täysin automaattinen julkinen Turingin testi, jolla on tarkoitus erottaa tietokoneet ja ihmiset toisistaan
CPU	keskusyksikkö
DAC	harkinnanvarainen pääsynhallinta
DNS	verkkotunnusjärjestelmä
GPS	maailmanlaajuisen paikannusjärjestelmä
IAM	identiteetti- ja käyttöövaltuushallinta
ICT	tieto- ja viestintätekniikka
ID	tunniste
IDE	integroitu kehitysympäristö
IDS	tietomurtohälytin
IoT	esineiden internet
IP	internetyhteyskäytäntö, internetprotokolla
IPS	tunkeutumisenestojärjestelmä

IT	tietotekniikka, informaatioteknologia
ISMS	tietoturvallisuuden hallintajärjestelmä
MAC	pakollinen pääsynhallinta
NTP	verkkoaikeita käytäntö
PIA	tietosuojavaikutusten arviointi
PII	henkilötieto
PIN	henkilökohtainen tunnusluku
PKI	julkisen avaimen järjestelmä, PKI-järjestelmä
PTP	PTP-protokolla kellojen synkronisointiin verkossa
RBAC	rooliperustainen pääsynhallinta
RPO	palautustavoite
RTO	palautumisaikatavoite
AST	lähdekoodin analyysi analyysityökaluilla
SD	<i>Secure Digital</i> -muistikortti
SDN	ohjelmistoverkko
SD-WAN	ohjelmistoalueverkko
SIEM	turvallisuuteen liittyvien tietojen ja tapahtumien hallinta
SMS	lyhytsanomapalvelu
SQL	rakenteinen kyselykieli
SSO	kertakirjautuminen
SWID	ohjelmiston tunnistaminen
UEBA	käyttäjien ja tahojen käyttäytymisen analysointi
UPS	katkoton virransyöttö
URL	URL-osoite
USB	sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen
VM	virtuaalikone
VPN	virtuaalinen yksityisverkko, VPN-verkko
WiFi	langaton verkko

## 4 Tämän asiakirjan rakenne [\(EN\)](#)

### 4.1 Kohdat [\(EN\)](#)

Tämä asiakirja on jäsennelty seuraavasti:

- a) organisaatioon liittyvät hallintakeinot ([kohta 5](#))
- b) henkilöstöön liittyvät hallintakeinot ([kohta 6](#))
- c) fyysiset hallintakeinot ([kohta 7](#))
- d) teknologiset hallintakeinot ([kohta 8](#)).

Lisäksi on kaksi opastavaa liitettä:

- [Liite A](#): Attribuuttien käyttö
- [Liite B](#): Vastaavuus standardin ISO/IEC 27002:2013 kanssa.

[Liitteessä A](#) kerrotaan, miten organisaatio voi hyödyntää attribuutteja (ks. [kohta 4.2](#)) omien näkymiensä luomiseen tässä asiakirjassa määriteltyjen tai sen itse luomien hallintakeinoja koskevien attribuuttiensa perusteella.

[Liitteessä B](#) esitetään standardin ISO/IEC 27002 tässä painoksessa olevien hallintakeinojen vastaavuudet standardin edellisen painoksen (ISO/IEC 27002:2013) hallintakeinoihin.

### 4.2 Teemat ja attribuutit [\(EN\)](#)

[Kohdissa 5–8](#) esiteltyjä hallintakeinojen luokitteluja kutsutaan teemoiksi.

Hallintakeinot luokitellaan

- a) henkilöstöön liittyviksi hallintakeinoiksi, jos ne koskevat yksittäisiä henkilöitä
- b) fyysisiksi hallintakeinoiksi, jos ne koskevat fyysisiä esineitä
- c) teknologisiksi hallintakeinoiksi, jos ne koskevat teknologiaa
- d) organisaatioon liittyviksi hallintakeinoiksi, jos mikään aiemmista luokista ei koske niitä.

Organisaatio voi attribuuttien avulla luoda erilaisia näkymiä, jotka ovat teemojen eri näkökulmasta tapahtuvan tarkastelun tuloksena syntyviä hallintakeinojen luokitteluja. Attribuuttien avulla voidaan myös suodattaa, järjestää tai esittää hallintakeinoja eri näkymissä eri yleisöille. [Liitteessä A](#) kerrotaan, miten tämä voidaan toteuttaa ja siinä esitetään esimerkkejä näkymistä.

Kaikki tässä asiakirjassa olevat hallintakeinot on esimerkinomaisesti yhdistetty viiteen attribuuttiin, joilla on vastaava attribuutin arvo (edessä #-merkki, mikä mahdollistaa niiden hakemisen), seuraavasti:

- a) Hallintakeinon tyyppi

Hallintakeinon tyyppi on attribuutti, jolla hallintakeinoja voidaan tarkastella sen perusteella, milloin ja miten hallintakeino muuttaa riskiä suhteessa tietoturvhäiriön tapahtumiseen. Attribuutin arvot ovat Ehkäisevä (hallintakeinon on tarkoitus estää tietoturvhäiriön tapahtuminen), Havaitseva (hallintakeino käynnistyy, kun tietoturvhäiriö tapahtuu) ja Korjaava (hallintakeino käynnistyy tietoturvhäiriön jälkeen).

- b) Tietoturvaominaisuudet

Tietoturvaominaisuudet on attribuutti, jolla hallintakeinoja voidaan tarkastella sen perusteella, minkä tiedon ominaisuuden säilyttämistä hallintakeino edistää. Attribuutin arvot ovat Luottamuksellisuus, Eheys ja Saatavuus.

c) Kyberturvallisuuteen liittyvät käsitteet

Kyberturvallisuuteen liittyvät käsitteet on attribuutti, jolla hallintakeinoja voidaan tarkastella sen perusteella, miten hallintakeinot liittyvät teknisessä spesifikaatiossa ISO/IEC TS 27110 kuvailun kyberturvallisuuden rakenteen kyberturvallisuuteen liittyviin käsitteisiin. Attribuutin arvot ovat Tunnistus, Suojaus, Havainto, Vaste ja Palautus.

d) Toiminnalliset kyvykkyydet

Toiminnalliset kyvykkyydet on attribuutti, jolla hallintakeinoja voidaan tarkastella toteuttajan tietoturvakykyksiä koskevasta näkökulmasta. Attribuutin arvot ovat Hallintotapa, Omaisuudenhallinta, Tietojen\_suojaaminen, Henkilöstöturvallisuus, Fyysinen\_turvallisuus, Järjestelmän\_ja\_verkon\_turvallisuus, Sovelluksen\_turvallisuus, Turvallinen\_konfigurointi, Identiteetti\_ja\_käyttövaltuushallinta, Uhkien\_ja\_haavoittuvuuksien\_hallinta, Toimittajasuheteiden\_hallinta, Lait\_ja\_vaatimustenmukaisuus, Tietoturvatapahtumien\_hallinta ja Tietoturvallisuuden\_varmentaminen.

e) Tietoturvan osa-alueet

Tietoturvan osa-alueet on attribuutti, jolla hallintakeinoja voidaan tarkastella neljän eri tietoturvallisuuden osa-alueen näkökulmasta. "Hallintotapa ja ekosysteemi" sisältää "Tietojärjestelmien turvallisuuden hallintotavan ja riskienhallinnan" sekä "Ekosysteemin kyberturvallisuuden hallinnan" (sisältäen sisäiset ja ulkoiset sidosryhmät). "Suojaaminen" sisältää "Tietotekniikan turvallisuusarkkitehtuurin", "Tietotekniikan turvallisuudenhallinnan", "Identiteetti-ja\_käyttövaltuushallinnan", "Tietotekniikan turvallisuuden ylläpidon" ja "Fyysisen ja ympäristön liittyvän turvallisuuden". "Puolustus" sisältää "Havaitsemisen" ja "Laitteiston turvallisuuden hallinnan". "Kriisinkestävyys" sisältää "Toimintojen jatkuvuuden" ja "Kriisinhallinnan". Attribuutin arvot ovat Hallintotapa\_ja\_ekosysteemi, Suojaaminen, Puolustus ja Kriisinkestävyys.

Tässä asiakirjassa annetut attribuutit on valittu sillä perusteella, että niiden katsotaan olevan riittävän yleislumoisia erityyppisten organisaatioiden käyttöön. Organisaatiot voivat päättää, etteivät ne käytä joitain tässä asiakirjassa annettuja attribuutteja. Ne voivat myös laatia omat attribuuttinsa (ja niitä vastaavat attribuuttien arvonsa) omien organisaationäkymiensä luomista varten. [Kohdassa A.2](#) on esimerkkejä tällaisista attribuuteista.

### 4.3 Hallintakeinon kuvaus (EN)

Kunkin hallintakeinon kuvaus sisältää seuraavat kohdat:

- **Hallintakeinon nimi:** Hallintakeinon lyhyt nimi.
- **Attribuuttitaulukko:** Taulukko, jossa esitetään hallintakeinon kunkin attribuutin arvo(t).
- **Hallintakeino:** Mikä hallintakeino on.
- **Tarkoitus:** Miksi hallintakeino olisi toteutettava.
- **Ohjeistus:** Miten hallintakeino olisi toteutettava.
- **Lisätiedot:** Selittävää tekstiä tai viittaus muihin asiaan liittyviin asiakirjoihin.

Joidenkin hallintakeinojen ohjeteksteissä käytetään väliotsikoita, kun ohjeistus on pitkää ja käsitlee monia aiheita, koska ne parantavat luettavuutta. Väliotsikoita ei ole kuitenkaan käytetty kaikissa ohjetekstiosuuksissa. Väliotsikot on alleviivattu.

## 5 Organisaatioon liittyvät hallintakeinot [\(EN\)](#)

### 5.1 Tietoturvallisuutta koskevat toimintaperiaatteet [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Kriisinkestävyys

#### Hallintakeino

Tietoturvapolitiikka ja kohdennetut toimintaperiaatteet olisi määriteltävä, ylimmän johdon olisi hyväksyttävä ne, ne olisi julkaistava, niistä olisi viestittävä asiaankuuluville henkilöön jäsenille ja sidosryhmille, näiltä olisi saatava kuittaus tietojen vastaanottamisesta, ja ne olisi katselmoitava suunnitelluin aikavälein ja aina kun tapahtuu merkittäviä muutoksia.

#### Tarkoitus

Varmistetaan johtamisen jatkuva soveltuvuus, riittävyys, vaikuttavuus sekä tuki tietoturvallisuudelle liiketoiminnallisten, lakiens, asetusten, viranomaisten ja sopimuksiin sisältyvien vaatimusten mukaisesti.

#### Ohjeistus

Ylimmällä tasolla organisaation olisi määriteltävä tietoturvapolitiikka, jonka ylin johto hyväksyy ja jossa määritellään organisaation lähestymistapa tietoturvallisuuden hallintaan.

Tietoturvapolitiikassa olisi otettava huomioon vaatimukset, jotka on johdettu

- liiketoimintastrategiasta ja liiketoiminnallisista vaatimuksista
- lainsäädännöstä, viranomaismääräyksistä ja sopimuksista
- nykyisistä ja ennustetuista tietoturvallisuuteen kohdistuvista riskeistä ja uhkista.

Tietoturvapolitiikan olisi käsiteltävä ainakin

- tietoturvallisuuden määrittelyä
- tietoturvatavoitteita tai niiden asettamisen perustaa
- periaatteita, jotka ohjaavat kaikkea tietoturvallisuuteen liittyvää toimintaa
- sitoutumista tietoturvallisuutta koskevien vaatimusten täyttämiseen
- sitoutumista tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen
- tietoturvallisuuden hallintaa koskevien vastuiden osoittamista määritellyille rooleille
- prosesseja, joilla käsitellään poikkeuksia ja poikkeamia.

Ylimmän johdon olisi hyväksyttävä kaikki tietoturvapolitiikkaan tehtävät muutokset.

Alemalla tasolla tietoturvapolitiikkaa olisi tarvittaessa tuettava kohdennetuilla toimintaperiaatteilla tai politiikoilla, jotka täydentävät vaatimuksia tietoturvallisuuden hallintakeinojen toteuttamiseksi. Kohdennetut toimintaperiaatteet ovat yleensä rakenteeltaan sellaisia, että ne vastaavat organisaation tiettyjen kohderyhmien tarpeisiin tai kattavat tiettyt tietoturvallisuuteen liittyvät alueet. Kohdennettujen toimintaperiaatteiden olisi oltava yhdennäköisiä organisaation tietoturvapolitiikan kanssa ja täydennettävä sitä.

Esimerkkejä tällaisista toimintaperiaatteista ovat

- a) pääsynthallinta
- b) fyysinen turvallisuus ja ympäristön turvallisuus
- c) omaisuudenhallinta
- d) tiedonsiirto
- e) käyttäjien päätelaitteiden turvallinen konfigurointi ja käsittely
- f) verkkoturvallisuus
- g) tietoturvahäiriöiden hallinta
- h) varmuuskopiointi
- i) salauksen hallinta ja avaintenhallinta
- j) tietojen luokittelu ja käsittely
- k) teknisten haavoittuvuuksien hallinta
- l) turvallinen kehittäminen.

Vastuu kohdennettujen toimintaperiaatteiden laadinnasta, katselmoinnista ja hyväksymisestä olisi annettava henkilöstölle, joka osaa laatia toimintaperiaatteita, joka voidaan valtuuttaa hyväksymään ne ja jolla on asiantuntemus aiheeseen. Katselmoinnin olisi sisällettävä organisaation tietoturvapolitiikan ja kohdennettujen toimintaperiaatteiden parantamismahdollisuuksien arvointi. Lisäksi olisi arvioitava, onko tietoturvallisuuden hallintaa muutettava, kun muutoksia kohdistuu

- a) organisaation liiketoimintastrategiaan
- b) organisaation tekniseen ympäristöön
- c) viranomaismääräyksiin, asetuksiin, lakeihin ja sopimuksiin
- d) tietoturvariskeihin
- e) nykyiseen tietoturvallisuuden uhkaympäristöön ja sen ennakoitaviin muutoksiin
- f) tietoturvatapahtumista ja -häiriöistä opittuihinasioihin.

Tietoturvapolitiikan ja kohdennettujen toimintaperiaatteiden katselmoinneissa olisi otettava huomioon johdon katselmountien ja auditointien tulokset. Yhdenmukaisuuden ylläpitämiseksi olisi otettava huomioon muiden asiaan liittyvien toimintaperiaatteiden katselmounti ja päivittäminen, kun yhteen toimintaperiaatteeseen tehdään muutoksia.

Tietoturvapolitiikasta ja kohdennetuista toimintaperiaatteista olisi viestittävä asiaankuuluvalle henkilöstölle ja sidosryhmille muodossa, joka on aiotulle kohderyhmälle soveltuva, saavutettava ja ymmärrettävä. Toimintaperiaatteiden vastaanottajat olisi velvoitettava vahvistamaan ymmärtävänsä toimintaperiaatteet ja sitoutuvansa noudattamaan niitä soveltuvin osin. Organisaatio voi määrittää näiden toimintaperiaateasiakirjojen muodot ja nimet siten, että ne ovat organisaatiolle sopivat. Joissain organisaatioissa tietoturvapolitiikka ja kohdennetut toimintaperiaatteet voivat olla yhtenä asiakirjana. Organisaatio voi nimetä nämä kohdennetut toimintaperiaatteet standardeiksi, toimintaohjeiksi, politiikoiksi tai vastaaviksi.

Jos tietoturvapolitiikoita tai kohdennettuja toimintaperiaatteita jaetaan organisaation ulkopuolelle, olisi pidettävä huoli siitä, ettei luottamuksellista tietoa pääse asiattomiin käsiin.

Taulukossa 1 esitetään tietoturvapolitiikan ja kohdennettujen toimintaperiaatteiden väliset erot.

## Taulukko 1 Tietoturvapolitiikan ja kohdennetun toimintaperiaatteiden väliset erot

	Tietoturvapolitiikka	Kohdennettu toimintaperiaate
Yksityiskohtaisuuden taso	Yleinen tai ylätaso	Kohdennettu ja yksityiskohtainen
Laatija ja virallinen hyväksyntä	Ylin johto	Asianmukaisen tason johto

### Lisätiedot

Kohdennetut toimintaperiaatteet voivat vaihdella organisaatioittain.

## 5.2 Tietoturvaroolit ja -vastuut (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Kriisinkestävyys

### Hallintakeino

Tietoturvaroolit ja -vastuut olisi määriteltävä organisaation tarpeiden mukaisesti.

### Tarkoitus

Laaditaan ja hyväksytään selkeät ja yksinkertaiset vastuut, joiden avulla organisaation tietoturvallisuutta toteutetaan, käytetään ja hallitaan.

### Ohjeistus

Tietoturvaroolit ja -vastuut olisi jaettava tietoturvapolitiikkojen ja kohdennettujen toimintaperiaatteiden mukaisesti (ks. [kohta 5.1](#)). Organisaation olisi määriteltävä ja hallittava vastuita, jotka koskevat

- tietojen ja niihin liittyvien omaisuuserien suojaamista
- määriteltyjen tietoturvallisuuteen liittyvien prosessien suorittamista
- tietoturvariskien hallintatoimintoja sekä erityisesti riskien omistajien tekemää jäännösriskien hyväksymistä
- kaikkea henkilöstöä, jotka käyttävät organisaation tietoja ja niihin liittyviä omaisuuseriä.

Näitä vastuita olisi tarvittaessa täydennettävä yksittäisiä toimipaikkoja ja tietojenkäsittelypalveluita koskevalla yksityiskohtaisemmassa ohjeistuksella. Henkilöt, joilla on nimettyjä tietoturvallisuusvastuita, voivat siirtää näitä suojaamistehtäviä muille. Vastuu säilyy kuitenkin alkuperäisillä henkilöillä, joiden olisi selvitettävä, että siirretyt tehtävät on suoritettu oikein.

Yksittäisten henkilöiden vastuulla olevat turvallisuuteen liittyvät alueet olisi määriteltävä ja dokumentoitava, ja niistä olisi viestittävä. Olisi määriteltävä ja dokumentoitava, mihin päätöksiin henkilön valtuudet riittävät. Tietyt tietoturvaroolin vastuulleen ottavilla henkilöillä olisi oltava roolin vaativat tiedot ja taidot, ja heitä olisi tuettava osaamisen kehittämisen ja taitojen pitämisen ajan tasalla.

### Lisätiedot

Organisaatiot nimeävät usein tietoturvapäällikön, joka kantaa päävastuun tietoturvallisuuden kehittämisestä ja toteuttamisesta sekä riskien ja niitä lieventävien hallintakeinojen tunnistamisesta.

Vastuu resurssien jakamisesta ja hallintakeinojen toteuttamisesta jää kuitenkin usein yksittäisille esimiehille. Eräs yleinen käytäntö on määritätä kullekin omaisuuserälle omistaja, joka on vastuussa omaisuuden jokapäiväisestä suojaamisesta.

Organisaation koosta ja resursseista riippuen tietoturvallisuus saatetaan kattaa tarkoitusta varten luodulla rooleilla, tai sitten siihen liittyvät vastuut hoidetaan jo olemassa olevien roolien lisänä.

### 5.3 Tehtävien eriyttäminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Hallintotapa #Identiteetti_-ja_-käyttövaltuushallinta	#Hallintotapa_ ja _ekosysteemi

#### Hallintakeino

Keskenään ristiriitaiset tehtävät ja vastuualueet olisi eriyttää toisistaan.

#### Tarkoitus

Vähennetään petoksiin, virheisiin ja tietoturvallisuuden hallintakeinojen ohittamiseen liittyviä riskejä.

#### Ohjeistus

Tehtävien ja vastuualueiden eriyttämisellä pyritään erottamaan ristiriitaiset tehtävät eri ihmislle, jotta voidaan välittää tilanne, jossa yksittäinen henkilö tekee mahdollisesti keskenään ristiriitaisia tehtäviä yksinään.

Organisaation olisi määritettävä, mitkä tehtävät ja vastuualueet tätyy eriyttää. Seuraavassa on esimerkkejä toimintoista, joita voi olla syytä eriyttää toisistaan:

- aloite muutokset tekemisestä, sen hyväksyminen ja muutoksen toteuttaminen
- pääsyoikeuksien pyytäminen, hyväksyminen ja myöntäminen
- ohjelmistokoodin suunnittelu, toteuttaminen ja katselointi
- ohjelmistojen kehittäminen ja jo tuotantokäytössä olevien järjestelmien hallinta
- sovellusten käyttö ja hallinta
- sovellusten käyttö ja tietokantojen hallinta
- tietoturvallisuuden hallintakeinojen suunnittelu, auditointi ja varmentaminen.

Pahantahtoisen yhteistoiminnan mahdollisuus olisi otettava huomioon eriyttämisen hallintakeinojen suunnittelussa. Pienissä organisaatioissa tehtävien eriyttäminen voi osoittautua vaikeaksi, mutta periaatetta olisi sovellettava mahdollisuksien mukaan. Mikäli tehtäviä ei pystytä eriyttämään, olisi syytä harkita muita hallintakeinoja, kuten toiminnan teknistä valvontaa, kirjausketuja ja tapahtumien kirjaamista lokiin ja esihenkilöiden tekemää toiminnan valvontaa.

Rooliperustaista pääsynhallintaa käytettäessä olisi oltava erityisen tarkka, jotta voidaan varmistaa, ettei henkilöille annetta ristiriitaisia rooleja, joihin liittyy jääviysriski. Jos rooleja on paljon, organisaation olisi harkittava automaattisten työkalujen käyttöä näiden löytämisen ja poistamisen helpottamiseksi. Roolien olisi oltava tarkkaan määriteltyjä ja tarvittaessa useammalle henkilölle jaettuja, jotta voidaan minimoida ongelmat, jos rooli poistetaan tai se annetaan toiselle henkilölle.

#### Lisätiedot

Ei lisätietoja.

## 5.4 Johdon vastuut (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvalli-suuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi

### Hallintakeino

Johdon olisi edellytettävä, että koko henkilöstö toteuttaa tietoturvallisuutta organisaation turvallisuuspolitiikan, kohdennettujen toimintaperiaatteiden ja tietoturvamenettelyjen mukaisesti.

### Tarkoitus

Varmistetaan, että johto ymmärtää roolinsa tietoturvallisuudessa ja tekee toimenpiteitä, joilla pyritään varmistamaan, että koko henkilöstö on tietoinen tietoturvallisuuteen liittyvistä vastuistaan ja toteuttaa ne.

### Ohjeistus

Johdon olisi osoitettava, että se tukee tietoturvapolitiikkaa, kohdennettuja toimintaperiaatteita, tietoturvamenettelyjä ja turvallisuuden hallintakeinoja.

Johdon vastuisiin olisi kuuluttava sen varmistaminen, että henkilöstö

- a) on saanut asianmukaista opastusta tietoturvarooleistaan ja -vastuistaan ennen pääsyoikeuden antamista organisaation tietoihin ja niihin liittyviin omaisuuseriin
- b) on saanut ohjeistusta, jossa kerrotaan tietoturvallisuutta koskevat odotukset sen roolille organisaatiossa
- c) on velvoitettu noudattamaan organisaation tietoturvapolitiikkaa ja kohdennettuja toimintaperiaatteita
- d) saavuttaa riittävän tietoturvallisuuden osaamistason (ks. [kohta 6.3](#))
- e) noudattaa työsuhteen tai muun sopimussuhteen ehtoja, joihin sisältyvät myös organisaation tietoturvapolitiikka ja asianmukaiset työskentelymenetelmät
- f) hallitsee riittävät tietoturvaan liittyvät taidot ja pätevyydet jatkuvan koulutuksen avulla
- g) voi mahdollisuuksien mukaan käyttää luottamuksellista kanavaa tietoturvallisuuspolitiikkaan, kohdennettuihin toimintaperiaatteisiin tai tietoturvamenettelyihin liittyvien rikkomusten raportointiin (väärinkäytösten paljastaminen), eli voidaan joko mahdollistaa nimetön raportointi tai varmistaa, että raportoijan henkilöllisyys on vain raportteja käsitlevän tiedossa
- h) saa käyttöönsä riittävät resurssit ja ajan organisaation turvallisuuteen liittyvien prosessien ja hallintakeinojen toteuttamiseen.

### Lisätiedot

Ei lisätietoja.

## 5.5 Yhteydet viranomaisiin (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus #Kriisinkestävyys

### Hallintakeino

Organisaation olisi luotava yhteydet toimivaltaisiin viranomaisiin sekä ylläpidettävä näitä yhteyksiä.

## Tarkoitus

Varmistetaan, että tieto liikkuu tietoturvallisesti organisaation ja toimivaltaisten viranomaisten välillä.

## Ohjeistus

Organisaation olisi määriteltävä, milloin ja kenen olisi otettava yhteyttä viranomaisiin (esim. poliisiin tai valvoviin viranomaisiin) sekä se, miten tunnistetuista tietoturvahäiriöistä olisi raportoitava viivyttelemättä.

Yhteydet viranomaisiin voivat myös auttaa ymmärtämään, miten viranomaismääräysten odotetaan muuttuvan tulevaisuudessa (esim. tietoturvallisuuteen liittyvä lainsääädäntö).

## Lisätiedot

Hyökkäyksen kohteena oleva organisaatio voi pyytää viranomaisilta hyökkäyksen lähteeseen kohdistuvia toimia.

Tällaisten yhteyksien ylläpito voi olla edellytys tietoturvahäiriöiden hallinnalle (ks. [kohdat 5.24–5.28](#)) tai poikkeusoloihin varautumisen suunnittelulle ja liiketoiminnan jatkuvuuden hallinnalle (ks. [kohdat 5.29 ja 5.30](#)). Yhteydet valvoviin viranomaisiin saattavat myös auttaa ennakoimaan ja varautumaan organisaatioon vaikuttavien lakiens tai asetusten muutoksiin. Yhteydet muihin viranomaisiin käsittävät yhteiskunnan perusinfrastruktuuripalveluiden tarjoajat, hätäpalveluiden tarjoajat, energiayhtiöt sekä terveys- ja turvallisuuspalvelut, esimerkiksi palolaitokset (liittyen liiketoiminnan jatkuvuuteen), tietoliikenepalvelujen tuottajat (liittyen tietoliikenneyhteyksien rakentamiseen) ja lämmön- ja vedenjakeluun (liittyen laitteiden jäähdytystoimintoihin).

## 5.6 Yhteydet osaamisyhteisöihin (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvalli-suuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus
#Korjaava	#Eheys #Saatavuus			

## Hallintakeino

Organisaation olisi luotava ja ylläpidettävä yhteyksiä asiantuntijaryhmiin tai muihin foorumeihin sekä ammatillisiiin yhteisöihin.

## Tarkoitus

Varmistetaan, että tietoa tietoturvallisuudesta on saatavilla.

## Ohjeistus

Osaamisyhteisöjen tai muiden vastaavien ryhmien jäsenyys olisi nähtävä keinona

- a) lisätä tietoa suositeltavista käytännöistä ja pysyä ajan tasalla tärkeästä turvallisuustiedosta
- b) varmistaa, että ymmärtämys tietoturvaympäristöstä on ajantasaista
- c) saada ennakkovaroituksia hyökkäyksiin ja haavoittuvuuksiin liittyvistä hälytyksistä, suosituksista ja päivityksistä
- d) saada pääsy tietoturva-asiantuntijoiden neuvoihin
- e) jakaa ja vaihtaa tietoa uudesta teknikasta, tuotteista, palveluista, uhkista tai haavoittuvuuksista
- f) tarjota tietoa siitä, miin otetaan yhteys, kun käsitellään tietoturvahäiriötä (ks. [kohdat 5.24–5.28](#)).

## Lisätiedot

Ei lisätietoja.

## 5.7 Uhkatiedon seuranta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Havainto #Vaste	#Uhkien_ja_haavoittuvuuksien_hallinta	#Puolustus #Kriisinkestävyys

### Hallintakeino

Tietoturvauhkiin liittyvää tietoa olisi kerättävä ja analysoitava, jotta kyettään tuottamaan uhkia koskevaa tietoa.

### Tarkoitus

Tarjotaan parempaa tietoa organisaation uhkaympäristöstä, jotta asianmukaiset lieventämistoimenpiteet kyettään toteuttamaan.

### Ohjeistus

Nykyisiin ja tuleviin uhkiin liittyvää tietoa kerätään ja analysoidaan, jotta kyettään

- edesauttamaan tietoon perustuvia toimenpiteitä, joilla pyritään estämään uhkien organisaatiolle aiheuttamien haittojen toteutuminen
- vähentämään toteutuneiden uhkien aiheuttamia haitallisia vaikutuksia.

Uhkatiedon seuranta voidaan jakaa kolmeen osaan, joita kaikkia olisi tehtävä:

- Strategisten uhkien seuranta: uhkaympäristön muutoksiin (kuten hyökkääjä- tai hyökkäystyyppiin) liittyvien ylätason tietojen vaihto.
- Taktisten uhkien seuranta: tietoa hyökkääjien käyttämistä tavoista, työkaluista ja teknologioista.
- Operationaalisten uhkien seuranta: yksityiskohtia tietyistä hyökkäystavoista, etenkin siitä, miten nämä kyettään havaitsemaan.

Uhkatiedon seurannan olisi oltava

- merkityksellistä (eli liityttävä organisaation suojaamiseen)
- syvälistä (eli tarjottava organisaatiolle tarkka ja yksityiskohtainen ymmärrys uhkaympäristöstä)
- asiayteyssidonnaista, jolloin se parantaa tilannetietoutta (eli tarjoaa parempaa kontekstia perustuen tapahtumien ajankohtaan, tapahtumapaikkaan, aiempiin kokemuksiin ja esiintyvyyteen muissa vastaavissa organisaatioissa)
- toiminnan mahdollistavaa (eli organisaatio voi toimia tietojen perusteella nopeasti ja vaikuttavasti).

Uhkatiedon seurannan toimintoihin olisi sisällyttää

- tavoitteet, joita uhkiin liittyvälle tiedon hankinnalle asetetaan
- sisäisten ja ulkoisten tietolähteiden tunnistaminen, arvointi ja valinta, jotta voidaan varmistaa, että nämä lähteet ovat hyödyllisiä ja antavat oikeaa tietoa uhista
- tietojen kerääminen valituista sisäisistä ja ulkoisista lähteistä
- kerättyjen tietojen käsittely analysointia varten (esim. kielen käänäminen, esittäminen toisessa muodossa tai tietoja tukevien tai niitä kumoavien tietojen hankkiminen)

e) tietojen analysointi, jotta voidaan ymmärtää, miten se liittyy organisaatioon ja on sen kannalta merkityksellistä

f) tietojen viestintä ja jakaminen keskeisille henkilöille muodossa, jonka he voivat ymmärtää.

Uhkatiledon seurannasta saadut tiedot olisi analysoitava, ja niitä olisi myöhemmin käytettävä

a) toteuttamalla prosessit, joilla uhkatiledon seurannassa kerättyt tiedot ovat organisaation tietoturvariskien hallintaprosessin käytettävissä

b) tietotekniin estäviin ja havaitseviin hallintakeinoihin, kuten palomuureihin, tietomurtohälyttimiin tai haittaohjelmien torjuntaratkaisuihin konfiguroinnin ja hallinnan apuna

c) apuna suunniteltaessa tietoturvallisuuden testausta.

Organisaation olisi jaettava uhkiin liittyvää tietoa muiden organisaatioiden kanssa, jotta uhkatiledon seurannan kokonaiskuvaa kyetään parantamaan.

### Lisätiedot

Organisaatiot voivat uhkatiledon seurannan avulla estää ja havaita uhkia sekä reagoida niihin.

Organisaatiot voivat tuottaa uhkiin liittyvää tietoa, mutta useimmiten ne vastaanottavat ja hyödyntävät muiden lähteiden tuottamaa uhkiin liittyvää tietoa.

Uhkatiledon seurantaa koskevia tietoja on saatavilla niihin erikoistuneista yrityksistä, tietoturvallisuuden asiantuntijoilta, valtionhallinnosta sekä alan osaamisyhteisöiltä.

Tiettyjen hallintakeinojen, kuten [5.25](#), [8.7](#), [8.16](#) tai [8.23](#), vaikuttavuus riippuu käytössä olevan uhkiin liittyvän tiedon laadusta.

## 5.8 Tietoturvallisuus projektinhallinnassa ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Suojaaminen

### Hallintakeino

Tietoturvallisuus olisi integroitava osaksi projektinhallintaa.

### Tarkoitus

Varmistetaan, että projekteihin ja projektien tuotoksiin liittyviä tietoturvariskejä käsitellään projektinhallinnassa projektin koko elinkaaren ajan.

### Ohjeistus

Tietoturvallisuus olisi integroitava osaksi projektinhallintaa, jotta voidaan varmistaa, että tietoturvariskejä käsitellään osana projektinhallintaa. Tätä voidaan soveltaa minkä tahansa tyypiseen projektiin sen monimutkaisudesta, koosta, kestosta, aiheesta tai soveltamisalueesta riippumatta (esim. ydinliiketoimintaprosessiin, tieto- ja viestintätekniikkaan, toimitilojen hallintaan tai muihin tukiprosesseihin liittyvä projekti).

Käytössä olevassa projektinhallinnassa olisi edellytettävä, että

- tietoturvariskejä arvioidaan ja käsitellään sekä varhaisessa vaiheessa että säännöllisesti läpi projektin elinkaaren
- tietoturvavaatimuksia (esim. sovelluksia koskevat turvallisuusvaatimukset [\[8.26\]](#), immateriaalioikeuksien noudattamista koskevat vaatimukset [\[5.32\]](#)) käsitellään varhaisessa vaiheessa projektia

- c) projektin aikaisia tietoturvariskejä, kuten sisäiseen ja ulkoiseen viestintään liittyviä näkökohtia, tarkastellaan ja käsitellään läpi projektin elinkaaren
- d) tietoturvariskien käsittelyn edistymisen katselmoidaan ja että käsittelyn vaikuttavuutta arvioidaan ja testataan.

Soveltuvien henkilöiden tai hallintoelinten, kuten projektin ohjausryhmän, olisi tarkasteltava tietoturvariskeihin liittyvien näkökohtien ja toimintojen asianmukaisuutta ennalta määritetyissä projektin vaiheissa.

Projektin kannalta tärkeimmät tietoturvallisuutta koskevat vastuu ja valtuudet olisi määriteltävä ja niistä vastaavat roolit olisi päättävä.

Projektissa tuotettavia tuotteita tai palveluita koskevat tietoturvavaatimukset olisi määritettävä erilaisin menetelmin, esim. johtamalla vaatimuksia tietoturvapolitiikasta, kohdennetuista toimintaperiaatteista ja viranomaismääräyksistä. Lisää tietoturvavaatimuksia voidaan saada esimerkiksi uhkien mallintamisesta, tietoturvatapahtumien arvioinneista, sen arvioinnista, miten vakavat ohjelmistohaavoittuvuudet korjataan ja mitkä ei sekä varautumissuunnittelusta, ja näin varmistaa, että tietojärjestelmän arkitehtuuri ja suunnittelu on tehty toimintaympäristön tunnettujen uhkien mukaan.

Tietoturvavaatimukset olisi määritettävä kaikentyyppisille projekteille, ei pelkästään tieto- ja viestintäteknikkaan liittyville projekteille. Seuraavia asioita olisi myös tarkasteltava, kun näitä vaatimuksia määritetään:

- a) Mitä tietoa asiaan liittyy (tietojen määrittäminen), mitkä ovat vastaavat tietoturvallisuuteen liittyvät tarpeet (luokittelu, ks. [kohta 5.12](#)) ja mahdolliset liiketoimintaan kohdistuvat negatiiviset vaikutukset, joita riittämättömästä turvallisuudesta voi seurata.
- b) Asiaan liittyvien tietojen ja niihin liittyvien omaisuuserien vaatimat suojaustarpeet koskien etenkin luottamuksellisuutta, eheyttä ja saatavuutta.
- c) Henkilön tunnistamiselta vaadittu luottamus- tai varmuustaso, jotta voidaan johtaa todentamista koskevat vaatimukset.
- d) Pääsyn myöntämisen ja todentamisen prosessit sekä asiakkaille ja muille liiketoimintakäyttäjille että ylläpito-oikeuksin varustetuille tai teknisille käyttäjille, kuten projektin jäsenille, mahdolliselle käyttöhenkilöstölle tai ulkoisille toimittajille.
- e) Käyttäjien tehtävien ja vastuiden viestiminen heille.
- f) Liiketoimintaprosesseista johdetut vaatimukset, kuten transaktiolokit ja näiden valvonta, kiistämättömyysvaatimukset.
- g) Muiden tietoturvallisuuden hallintakeinojen edellytykset, esim. käyttöliittymän lokkirauhasten ja niiden valvontan rajapinnat tietojärjestelmiin tai tietovuotojen havaitsemisjärjestelmä.
- h) Organisaatioon kohdistuvien lakiens, asetusten ja viranomaismääräysten ja sopimusten noudattaminen.
- i) Luottamus- tai varmuustaso, joka vaaditaan kolmansilta osapuolilta, jotta niiden voidaan katsoa täyttävän organisaation tietoturvapolitiikka ja kohdennetut toimintaperiaatteet mukaan lukien turvallisuuteen liittyvät sopimusehdot.

## Lisätiedot

Projektin kehitysmallin, kuten ns. vesiputoismallin tai ketterän kehityksen mallin, olisi tuettava tietoturvallisuutta tavalla, joka voidaan sopeuttaa tietoturvariskien arvioituun vakavuuteen projektin luonteen perusteella. Varhaisessa vaiheessa tehty tuotetta tai palvelua koskevien tietoturvavaatimusten tarkastelu (esim. määrittely- ja suunnitteluvaiheissa) voi johtaa laatua ja tietoturvallisuutta parantaviin ratkaisuihin, jotka ovat vaikuttavampia ja kustannustehokkampia. Standardeissa ISO 21500 ja ISO 21502 kuvataan tärkeitä projektinhallinnan käsitteitä ja annetaan projektinhallinnan prosesseja koskevaa ohjeistusta.

Standardissa ISO/IEC 27005 on opastusta riskienhallintaprosesseista, joilla voidaan tunnistaa hallintamekanismit, joilla täytetään tietoturvavaatimukset.

## 5.9 Tietojen ja niihin liittyvien omaisuuserien luettelo (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Omaisuudenhallinta	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

### Hallintakeino

Olisi laadittava omaisuusluettelo tieto-omaisuudesta ja muihin niihin liittyvistä omaisuuseristä sekä tieto näiden omistajista. Luettelo olisi ylläpidettävä.

### Tarkoitus

Tunnistetaan organisaation tieto-omaisuus ja muut niihin liittyvät omaisuuserät, jotta voidaan ylläpitää niiden tietoturvallisuutta ja varmistua siitä, että näillä on omistajat.

### Ohjeistus

#### Luettelo

Organisaation olisi yksilöitvä sen tiedot sekä niihin liittyvät omaisuuserät sekä määritettävä niiden tietoturvallisuutta koskeva tärkeys. Dokumentaatiota olisi ylläpidettävä tarkoitusta varten laadituissa tai jo olemassa olevissa luetteloissa.

Tietoja ja niihin liittyviä omaisuuseria koskevan omaisuusluettelon olisi oltava tarkka, ajantasainen, johdonmukainen ja muiden luetteloiden kanssa yhtenevä. Vaihtoehtoja tietojen ja niihin liittyvien omaisuuserien luettelon tarkkuuden varmistamiseen ovat mm.

- tietojen ja niihin liittyvien omaisuuserien säännöllinen katselointi ja vertaaminen omaisuusluetteloon
- omaisuusluettelon automaattinen päivittäminen, kun omaisuuseriä asennetaan, muutetaan tai poistetaan.

Omaisuuserän sijainti olisi tarvittaessa sisällytettävä omaisuusluetteloon.

Omaisuusluettelon ei tarvitse olla yksi tietojen ja niihin liittyvien omaisuuserien luettelo. Koska asianomaisten toimintojen olisi ylläpidettävä omaisuusluettelo, sitä voidaan tarkastella joukkona erillisä omaisuusluetteloita, kuten tieto-omaisuutta, laitteistoja, ohjelmistoja, virtuaalikoneita, toimitiloja, henkilöstöä, pääevyyksiä, kyvykkyyksiä ja tallenteita koskevat omaisuusluettelot.

Kuin omaisuuserä olisi luokiteltava omaisuuserään liittyvän tiedon luokituksen (ks. [kohda 5.12](#)) mukaisesti.

Tietoja ja niihin liittyviä omaisuuseria koskevan omaisuusluettelon hienojakoisuuden olisi oltava organisaation tarpeiden mukaisella tasolla. Toisinaan joitain omaisuuseriä ei ole järkevää dokumentoida niiden luontesta johtuen. Esimerkiksi yksittäinen virtuaalikoneen instanssi voi olla olemassa vain hyvin lyhyen aikaa.

### Omistajuus

Kunkin yksilöidyn tiedon ja siihen liittyvän omaisuuserän omistajuus olisi osoitettava nimetylle henkilölle tai ryhmälle ja sen luokitus olisi yksilöitvä (ks. [kohdat 5.12 ja 5.13](#)). Olisi toteutettava prosessi, jolla varmistetaan oikea-aikaisesti tapahtuva omaisuuserän omistajuuden osoittaminen. Omistajuus olisi osoitettava, kun omaisuuserä luodaan tai siirretään organisaatioon. Omaisuuserien omistajuus olisi

uudelleenositettava tarpeen mukaan, kun senhetkiset omistajat lähtevät organisaatiosta tai vaihtavat työroolejaan.

### Omistajan tehtävät

Omaisuuserän omistajan olisi oltava vastuussa suojattavan omaisuuden asianmukaisesta hallinnasta koko sen elinkaaren ajan ja varmistettava, että

- a) tieto ja siihen liittyvät omaisuuserät on inventoitu
- b) tieto ja siihen liittyvät omaisuuserät on luokiteltu ja asianmukaisesti suojattu
- c) luokittelut katselmoidaan säännöllisesti
- d) teknologisia omaisuuseriä tukevat komponentit on luetteloitu, ja linkitetty, mihin prosessiin tai tietojärjestelmään ne liittyvät; esim. tietokanta, tallennusjärjestelmä tai tietovarasto, ohjelmistokomponentit ja alikomponentit
- e) tiedon ja siihen liittyvien omaisuuserien hyväksyttävää käytötä koskevat vaatimukset (ks. [kohta 5.10](#)) on laadittu
- f) pääsyoikeudet tietoon vastaavat luokittelua, ovat toimivia ja ne katselmoidaan säännöllisesti
- g) tietoa ja siihen liittyviä omaisuuseriä käsitellään poiston ja tietoja sisältäneen tietovälilineen hävittämisen yhteydessä turvallisesti ja ne poistetaan omaisuusluettelosta
- h) osallistuvat omaisuuseriinsä liittyvien riskien tunnistamiseen ja hallintaan
- i) tukevat henkilöstöä, joilla on kyseisten tietojen hallintaa koskevia rooleja ja vastuita.

### Lisätiedot

Tietojen ja siihen liittyvien omaisuuserien inventointi on usein välttämätöntä, jotta voidaan varmistaa, että tietojen suojaus on vaikuttavaa. Sitä voidaan tarvita myös muista syistä, jotka voivat liittyä esimerkiksi työturvallisuteen, vakuutuksiin tai taloushallinnon pitämään omaisuuskirjanpitoon. Tietojen ja siihen liittyvien omaisuuserien luettelolla voidaan tukea myös riskienhallintaa, auditointia ja tilintarkastusta, haavoittuvuuksien hallintaa, häiriötilanteisiin reagoimista ja toipumissuunnittelua.

Tehtävät ja vastuut voidaan delegoida (esim. valvojalle, joka vastaa omaisuuserien päivittäisestä huolehtimisesta), mutta lopullinen vastuu säilyy tehtävänsä tai vastuunsa delegoineella henkilöllä tai ryhmällä.

Voi olla hyödyllistä jaotella tiedot ja niihin liittyvät omaisuuserät niin, että ne muodostavat ryhmiä, jotka toimivat yhdessä tuottaen tietyn palvelun. Tällaisessa tapauksessa palvelun omistaja on lopullisessa vastuussa palvelun toimittamisesta, mukaan lukien sen suojattavan omaisuuden toiminnasta.

Standardissa ISO/IEC 19770-1 annetaan tietoteknisten omaisuuserien hallintaa koskeva lisätietoa. Standardissa ISO/IEC 55001 annetaan omaisuudenhallintaa koskeva lisätietoa.

### **5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö ([EN](#))**

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen

### **Hallintakeino**

Tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön säännöt ja menettelyt olisi yksilöitävä, dokumentoitava ja vietävä käytäntöön.

## Tarkoitus

Varmistetaan, että tiedot ja niihin liittyvät omaisuuserät on suojattu asianmukaisesti ja että niitä käytetään ja käsitellään asianmukaisesti.

## Ohjeistus

Henkilöstön ja ulkopuolisten käyttäjien, jotka käyttävät organisaation tietoja ja niihin liittyviä omaisuuseriä tai joilla on pääsy niihin, olisi oltava perillä tietoturvavaatimuksista, jotka liittyvät organisaation tietojen ja niihin liittyvien omaisuuserien suojaamiseen ja käsittelyyn. Heidän olisi oltava vastuussa siitä, että he noudattavat näitä vaatimuksia.

Organisaation olisi laadittava tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille, jotka käyttävät tai käsittelevät tietoja ja niihin liittyviä omaisuuseriä. Hyväksyttävän käytön kohdennettujen toimintaperiaatteiden olisi tarjottava selkeä ohjeistus siitä, mikä on hyväksyttävää käytöä. Kohdennetuissa toimintaperiaatteissa olisi ilmoitettava

- a) henkilöiden sallitut ja ei-sallitut toimet tietojen turvallisen käsittelyn kannalta
- b) tietojen ja niihin liittyvien omaisuuserien sallittu ja ei-sallittu käyttö
- c) organisaation tekemä valvonta tietojen käytöstä.

Hyväksyttävän käytön menettelyt olisi laadittava tietojen koko elinkaarelle sen luokittelun (ks. [kohta 5.12](#)) ja tietoon liittyvien riskien perusteella. Seuraavat seikat olisi otettava huomioon:

- a) pääsyoikeudet, jotka tukevat kunkin luokitustason suojausvaatimuksia
- b) tietojen ja niihin liittyvien omaisuuserien käyttöön oikeutettujen henkilöiden tietojen ylläpitäminen
- c) tiedon väliaikaisten ja pysyvien kopioiden suojaaminen samantasoisesti kuin alkuperäinen tieto
- d) tietoihin liittyvien omaisuuserien säilyttäminen valmistajan ohjeiden mukaisesti (ks. [kohta 7.8](#))
- e) selkeät merkinnät kaikkiin (sähköisiin tai fyysisiin) tallenteisiin ja tallennusvälineisiin käyttöön oikeutettua vastaanottajaa varten (ks. [kohta 7.10](#))
- f) tietojen ja niihin liittyvien omaisuuserien hävittämisen hyväksymismenettely sekä hyväksytty tavat tietojen poistamiseksi (ks. [kohta 8.10](#)).

## Lisätiedot

On mahdollista, että omaisuuserät eivät ole suoraan organisaation hallinnassa, kuten julkiset pilvipalvelut. Tällaisten kolmannen osapuolen omaisuuserien ja tällaisiin kolmannen osapuolen omaisuuseriin liittyvien organisaatioiden omaisuuserien (esim. tieto, ohjelmisto) käyttö olisi yksilöitäävä soveltuvalla tavalla, ja sitä olisi hallittava esim. pilvipalvelun tuottajan kanssa tehtävän sopimuksen avulla. Tästä olisi huolehdittava myös, kun toimitaan yhteistyöympäristössä.

## 5.11 Omaisuuden palauttaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvalli-suuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta	#Suojaaminen

## Hallintakeino

Henkilöstön ja muiden sidosryhmien olisi palautettava kaikki hallussaan oleva organisaation omaisuus työsuhteeseen tai sopimuksen päättyessä tai muuttuessa.

## Tarkoitus

Suojataan organisaation omaisuuseriä osana työsuhteen tai sopimuksen päättymis- tai muutosprosessia.

## Ohjeistus

Työsuhteen muutos- tai päättymisprosessin olisi oltava selkeästi määritelty siten, että siihen sisältyy kaiken aiemmin saadun organisaation omistaman tai sillle luovutetun fyysisen tai sähköisen omaisuuden palauttaminen.

Jos henkilöstö tai sidosryhmä ostaa organisaation laitteistoja tai käyttää omia henkilökohtaisia laitteitaan, olisi noudatettava menettelyjä, joilla varmistetaan kaiken tärkeän tiedon seuranta ja siirtäminen organisaatiolle ja sen turvallinen poistaminen laitteistosta (ks. [kohta 7.14](#)).

Jos henkilöstöllä tai muilla sidosryhmillä on toiminnan jatkumisen kannalta tärkeää tietoa, tämä tieto oli dokumentoitava ja siirrettävä organisaatiolle.

Erityisesti irtisanomisaihana mutta myös sen jälkeen organisaation olisi estettävä irtisanottua tai -sanoutunutta henkilöstöä kopioimasta organisaation tärkeää tietoa (esim. aineetonta omaisuutta) luvattomasti.

Organisaation olisi selkeästi yksilöitvä ja dokumentoitava kaikki palautettavat tiedot ja niihin liittyvät omaisuuserät. Näitä voivat olla esim.

- a) käyttäjien päätelaitteet
- b) siirrettävät tallennusvälineet
- c) muut välineet ja laitteet
- d) tietojärjestelmien, toimipaikkojen ja fyysisen tallenteiden tunnistautumisvälineet (esim. mekaaniset avaimet, tunnistuslaitteet tai älykortit)
- e) tietojen fyysiset kopiot.

## Lisätiedot

Voi olla vaikeaa palauttaa tietoja, joita säilytetään välineissä, joita organisaatio ei omista. Näissä tapauksissa on tärkeää rajoittaa tietojen käyttöä muilla tietoturvallisuuden hallintakeinoilla, kuten pääsyoykeuksien hallinnalla ([5.18](#)) tai salauksen käytöllä ([8.24](#)).

## 5.12 Tiedon luokittelu [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvali-suuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Tietojen_suojaaminen	#Suojaaminen #Puolustus

## Hallintakeino

Tieto olisi luokiteltava organisaation tietoturvatarpeiden mukaisesti perustuen luottamuksellisuuteen, eheyteen, saatavuuteen ja keskeisten sidosryhmien vaatimuksiin.

## Tarkoitus

Varmistetaan, että tietoa suojataan oikein ja sen mukaisesti, miten tärkeää se on organisaatiolle.

## Ohjeistus

Organisaation olisi laadittava tiedon luokitusta koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille tärkeimmille sidosryhmiille.

Organisaation olisi luokitteluperiaatteissa otettava huomioon luottamuksellisuutta, eheyttä ja saatavuutta koskevat vaatimukset.

Tiedon luokittelussa ja sen suojaamisen hallintakeinoissa olisi otettava huomioon liiketoiminnallinen tarve tiedon jakamiseen ja pääsyoykeuksien rajoittamiseen, tiedon eheyden suojaamiseen ja sen saatavuuden varmistamiseen sekä tiedon luottamuksellisuutta, eheyttä tai saatavuutta koskevat juridiset velvoitteet. Tiedon lisäksi myös muut omaisuuserät voidaan luokitella sen tiedon perusteella, joka niihin on tallennettu tai jota niissä käsitellään tai jota niillä suojataan.

Tiedon omistajien olisi oltava vastuussa tietojensa luokittelusta.

Luokitteluperiaatteiden olisi sisällettävä kriteerit, joilla luokittelut käytännössä tehdään ja miten luokittelut ilmaistaan sekä kriteerit luokittelun arvioinnille tulevaisuudessa. Luokittelun tuloksia olisi päivitetä tiedon koko elinkaaren aikana sen muuttuneen arvon, arkaluonteisuuden ja kriittisyyden mukaisesti.

Periaatteiden olisi oltava pääsynhallinta (ks. [kohta 5.1](#)) koskevien toimintaperiaatteiden kanssa linjassa ja niiden olisi vastattava organisaation liiketoiminnallisia tarpeita.

Luokitus voidaan määrittää sen perusteella, miten merkittävä vaikutus tietojen vaarantumisella olisi organisaatiolle. Kullekin periaatteissa määritellylle tasolle olisi annettava kuvaava nimi, joka helpottaa tiedon oikeaa käsitelyä sen luokan mukaisesti.

Periaatteiden olisi oltava yhdenmukaiset koko organisaatiossa ja sisältyä tietojen käsitelyn prosesseihin ja menettelyihin, jotta kaikki luokittelevat tietoja ja niihin liittyviä omaisuuseriä samalla tavalla. Tällöin kaikki ymmärtävät suojausvaatimukset samalla tavalla ja toteuttavat oikeanlaisen suojaukseen.

Organisaatiossa käytetyt luokitteluperiaatteet eivät väältämättä vastaa muissa organisaatioissa käytettäviä periaatteita, vaikka tasojen nimet olisivat samoja. Lisäksi organisaatioiden välillä liikkuvan tiedon luokitus voi vaihdella riippuen sen asiayhteydestä kussakin organisaatiossa, vaikka luokitteluperiaatteet olisivatkin identtisiä. Siksi muiden organisaatioiden kanssa tehtäviin sopimuksiin, joihin sisältyy tietojen vaihtoa, olisi sisällettävä menettely, joilla varmistetaan, että tiedot saavat saman suojan, vaikka käytetyt luokitteluperiaatteet eroavat. Eri periaatteiden keskinäinen vastaavuus voidaan määrittää tarkastelemalla, miten niiden käsitely- ja suojausmenetelmät vastaavat toisiaan.

## Lisätiedot

Luokitelut antavat tietoja käsitteleville henkilöille yksiselitteisen tiedon siitä, miten tietoa pitää käsitellä ja suojata. Tätä voidaan edesauttaa luomalla tietoryhmää, joilla on samanlaiset suojaustarpeet, ja määrittelemällä tietoturvamenettelyt, jotka koskevat kaikkia kyseisen ryhmän tietoja. Tämä lähestymistapa vähentää tarvetta tapauskohtaisiin riskien arvointeihin ja hallintakeinoihin.

Tieto voi lakata olemasta arkaluonteista tai kriittistä tietyn ajan jälkeen. Esimerkiksi kun tieto on julkistettu, siihen ei enää kohdistu luottamuksellisuuteen liittyviä vaatimuksia, mutta sen eheys ja saatavuus saattavat vaatia suojaamista. Olisi otettava huomioon, että liian korkea luokitus voi johtaa tarpeettomien hallintakeinojen toteuttamiseen ja lisäkustannuksiin. Toisaalta taas liian alhainen luokitus voi johtaa siihen, että toteutetut hallintakeinot eivät riitä tiedon suojaamiseen.

Tiedon luottamuksellisuutta koskevat luokitteluperiaatteet voivat koostua esim. seuraavista neljästä tasosta:

- a) tietojen paljastaminen ei aiheuta haittaa
- b) tietojen paljastaminen aiheuttaa vähäistä maine- tai muuta haittaa tai sillä on vähäisiä toiminnallisia vaiktuksia
- c) tietojen paljastamisella on huomattavia lyhyen aikavälin vaiktuksia toimintoihin tai liiketoiminnalliisiin tavoitteisiin
- d) tietojen paljastamisella on vakavia vaiktuksia pitkän aikavälin liiketoiminnalliisiin tavoitteisiin, tai se vaarantaa koko organisaation olemassaolon.

## 5.13 Tiedon merkintä [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Tietojen_suojaaminen	#Puolustus #Suojaaminen

### Hallintakeino

Tiedon merkitsemistä koskevat menettelyt olisi laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti.

### Tarkoitus

Varmistetaan, että tietojen luokittelu on kaikkien sitä käsitlevien tiedossa sekä tuetaan tietojenkäsittelyn ja -hallinnan automatisointia.

### Ohjeistus

Tiedon merkitsemistapojen olisi katettava kaikissa muodoissa olevat tiedot ja niihin liittyvät omaisuuserät. Merkintöjen olisi oltava [kohdassa 5.12](#) esitetyjen luokitteluperiaatteiden mukaisia. Merkintöjen olisi oltava helposti tunnistettavia. Menettelyissä olisi ohjeistettava, mihin ja miten luokittelumerkinnät laitetaan ottaen huomioon tiedon käyttötapa tai suojaavan omaisuuden käsittelytapa eri tallennusvälinetavoissa. Menettelyissä voidaan määritellä

- tapauksia, joissa merkinnät voidaan jättää pois, esim. ei-luottamuksellisen tiedon merkitsemättä jättäminen tarpeettoman työn vähentämiseksi
- miten merkitään tietoa, jota lähetetään tai varastoidaan sähköisesti tai fyysisesti tai missä tahansa muussa muodossa
- miten toimitaan tapauksissa, joissa merkintää ei ole mahdollista tehdä (esim. teknisten rajoitusten takia).

Esimerkkejä merkintätavoista ovat

- fyysiset merkinnät
- ylätunnisteet ja alatunnisteet
- metadata
- vesileimat
- leimat.

Digitaalisen tiedon kanssa olisi hyödynnettävä metadataa, jotta tietoja voidaan tunnistaa, käsittellä ja ohjata tiedon kulkua etenkin luottamuksellisuuden näkökulmasta. Metadatan olisi mahdollistettava myös tietojen tehokas ja tarkka haku. Metadatan olisi edistettävä ominaisuuksia, joilla tietojärjestelmät ehdottavat suojaustasoja ja mahdollistavat oikean suojaustason helpon valinnan sekä tukevat päättöksentekoa asiaan liittyvien luokittelumerkintöjen perusteella.

Menettelyissä olisi kuvaltava, miten metadata liitetään tietoon, mitä merkintöjä käytetään ja miten tietoja olisi käsitteltävä organisaation käyttämän tietomallin ja tietoteknisen arkkitehtuurin mukaisesti.

Järjestelmien olisi lisättävä merkityksellistä lisämetatietoja, mikäli tietojen luokka sallii tämän.

Henkilöstön ja muiden sidosryhmien olisi oltava perillä tietojen luokittelusta ja merkinnöistä. Koko henkilöstön olisi saatava riittävä koulutus, jotta voidaan varmistaa, että tieto on oikein merkityä ja sitä käsittellään merkintöjen mukaisesti.

Arkaluonteiseksi tai kriittiseksi luokiteltua tietoa sisältävien järjestelmien tulosteet olisi varustettava asianmukaisin luokittelumerkinnöin.

## Lisätietoa

Salaisen tiedon selkeä merkitseminen on erittäin tärkeää, kun tietoa luovutetaan organisaation ulkopuolelle.

Muuta tietoon liitettävää hyödyllistä metadataa ovat tiedon luonut organisaation prosessi tai yksikkö, kuka tiedon on laatinut ja kuka sen omistaa sekä tiedon laatimisen ajankohta.

Tietojen ja niihin liittyvien omaisuuserien merkitsemisellä voi toisinaan olla haitallisia vaikutuksia. Pahantahtoisten toimijoiden saattaa olla helpompi kohdistaa väärinkäyttö salaisiksi luokiteltuihin omaisuuseriin.

Joissain järjestelmissä yksittäisiä tiedostoja tai tietokantatallenteita ei merkitä mitenkään, vaan kaikkea tietoa suojataan järjestelmän sisältämien erillisten tietokohteiden korkeimman luokituksen mukaisesti. Tällaisissa järjestelmissä on yleistä määrittää ja merkitä tiedot vasta, kun niitä viedään ulos järjestelmästä.

## 5.14 Tietojen siirtäminen [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen	#Suojaaminen

### Hallintakeino

Kaiken tyypillisellä organisaation sisäisellä, organisaatioiden välisellä ja sidosryhmille tapahtuvalla tietojen siirtämisellä olisi oltava säännöt, menettelyt tai sopimukset.

### Tarkoitus

Ylläpidetään organisaation sisällä tai ulkopuolisen sidosryhmän kanssa siirretyn tiedon suojausta.

### Ohjeistus

#### Yleistä

Organisaation olisi laadittava tietojen siirtämistä koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille olennaisille sidosryhmillä. Siirrettävien tietojen suojaamista koskevien sääntöjen, menettelyiden ja sopimusten olisi oltava siirrettävien tietojen luokitteluiden mukaisia. Kun tietoa siirretään organisaation ja kolmansien osapuolten välillä, olisi laadittava siirtosopimukset, johon sisältyy velvoite tunnistaa tietoja vastaanottava osapuoli luotettavasti, ja ylläpidettävä niitä sopimuksia, jolloin tietoja kyetään suojaamaan siirtotavasta riippumatta (ks. [kohta 5.10](#)).

Tietoja voidaan siirtää sähköisesti, fyysisen tallennusvälineiden avulla tai suullisesti.

Tietojen kaikentyyppistä siirtämistä koskevien sääntöjen, menettelyjen ja sopimusten olisi sisällettävä seuraavat asiat:

- Hallintakeinot, joilla suojataan siirrettyä tietoa salakuuntelulta, luvattomalta käytöltä, kopioinnilta, muokkaamiselta, väärin reitittämiseltä, tuhoamiselta ja käytön estolta. Näiden olisi sisällettävä pääsynhallinnan keinot, jotka ovat asiaan liittyvien tietojen luokitusten mukaisia sekä erityishallintakeinot arkaluonteisten tietojen suojaamiseen, kuten salausteknikoiden käyttö (ks. [kohta 8.24](#)).
- Hallintakeinot, joilla varmistetaan tietojen jäljitettävyys ja kiistämättömyys, mukaan lukien tiedon hallussapitoketjun ylläpitäminen siirron aikana.
- Siirtoon liittyvien yhteishenkilöiden, kuten tietojen omistajien, riskin omistajien, turvallisuuspäälliköiden ja tietojen säilyttäjän, tunnistaminen tarpeen mukaan.

- d) Velvollisuudet ja vahinkovastuuut tietoturvhäiriöiden tapahtuessa, kuten fyysisen tallennusvälineen tai tiedon häviämisessä.
- e) Arkaluonteisen ja kriittisen tiedon merkitseminen siten, että merkintöjen tarkoitus on helposti ymmärrettävissä ja että tieto on riittävästi suojattu (ks. [kohta 8.2](#)).
- f) Siirtopalvelun luotettavuus ja käytettävyys.
- g) Tiedonsiirtopalveluiden hyväksyttävää käyttöä koskevat kohdennetut toimintaperiaatteet tai ohjeet (ks. [kohta 5.10](#)).
- h) Säilytys- ja hävittämisojjeet, jotka koskevat kaikkia liiketoimintaan liittyviä tallenteita, mukaan lukien sähköiset viestit.

HUOM. Paikalliset lait ja viranomaismääräykset voivat koskea liiketoimintaan liittyvien tallenteiden säilyttämistä ja hävittämistä.

- i) Tietojen siirtämiseen liittyvät lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvien vaatimusten (ks. [kohdat 5.31, 5.32, 5.33 ja 5.34](#)) tarkastelu (esim. sähköistä allekirjoitusta koskevat vaatimukset).

#### Sähköinen siirtäminen

Kun tietoja siirretään sähköisten viestintäpalveluiden avulla, olisi säännöissä, menettelyissä ja sopimuksissa otettava huomioon myös seuraavat asiat:

- a) sähköisen viestinnän kautta levävien haittaohjelmien havaitseminen ja niiltä suojaaminen (ks. [kohta 8.7](#))
- b) sähköpostin tai muun sähköisen viestinnän liitteenä lähetetyn arkaluonteisen sähköisen tiedon suojaaminen
- c) viestien yhteydessä lähetettävien asiakirjojen ja viestien väärään osoitteeseen tai numeroon lähetämisestä
- d) hyväksytä ulkoisten julkisten palvelujen, kuten pikaviestien, sosiaalisten verkostojen tiedostojen jakamisen tai pilvitallennuksen, käytölle ennen näiden ottamista käyttöön
- e) käyttäjien ja tietojärjestelmien vahvempi tunnistaminen, kun tietoja siirretään julkisissa verkoissa
- f) rajoitukset, jotka liittyvät sähköisten viestintäpalvelujen käyttöön (esim. sähköpostin automaattiseen uudelleenohjaukseen estäminen ulkoisiin sähköpostiosoitteisiin)
- g) ohje henkilöstölle ja muille sidosryhmille siitä, että eivät lähetä kriittisiä tietoja tekstiviesteissä tai pikaviesteissä, koska viestit saatetaan lukea julkisilla paikoilla (ja näin ollen päätyä sivullisten lukemaksi) tai tallentaa riittämättömästi suojatuille laitteille
- h) ohje henkilöstölle ja muille sidosryhmille seuraavista faksilaitteiden tai -palveluiden käyttöön liittyvistä ongelmista:
  - 1) luvaton pääsy laitteiden muistissa oleviin sanomiin
  - 2) tietoinen tai tahaton laitteiden ohjelointi lähettämään viestejä väärin numeroihin.

#### Fyysisien tallennusvälineiden siirtäminen

Kun siirretään fyysisiä tallennusvälineitä (myös paperia), sääntöjen, menettelyjen ja sopimusten olisi sisällettävä myös seuraavat asiat:

- a) vastuu siirtojen, lähetysten ja vastaanottojen hallinnasta ja niistä ilmoittamisesta
- b) viestin oikean osoitteen ja kuljetuksen varmistaminen

- c) pakaus, joka suojaa sisältöä kuljetuksen aikaisilta fyysisiltä vahingoilta ja on valmistajan määrittelyjen mukainen, esimerkiksi suojaus tallennusvälineen palauttamismahdollisuuksesta vaarantavilta ympäristötekijöiltä, kuten kuumuus, kosteus ja sähkömagneettiset ketät; muut pakkaukselle asetettavat tekniset vähimmäisvaatimukset (esim. läpinäkymättömät kirjekuoret)
- d) luettelo johdon hyväksymistä ja luotettavista kuljetuspalveluista
- e) kuljetushenkilöstön tunnistamisen tavat
- f) luvattoman avaamisen osoittavien tai luvattomalta muuttamiselta suojaavien hallintakeinojen (esim. pussit, salkut) käyttö tallennusvälineessä olevien siirrettäväksi tarkoitettujen tietojen luokitustason mukaan
- g) menettelyt kuljetushenkilöstön henkilöllisydden tarkistamiseen
- h) luettelo kuljetus- ja kuriiripalveluita tarjoavista hyväksytyistä kolmansista osapuolista tietojen luokituksen mukaisesti
- i) lokitiedot, joissa yksilöidään tallennusvälineen sisältö ja siihen sovellettava suojaus sekä tieto luvallisista vastaanottajista ja joihin kirjataan, milloin tallennusväline luovutettiin kuljetuksesta vastaanalle ja milloin se vastaanotettiin kohteessa.

#### Suullinen siirtäminen

Henkilöstöä ja muita sidosryhmiä olisi tietojen suullisen siirtämisen suojaamiseksi muistutettava siitä, että

- a) luottamuksellisia keskusteluja ei saisi käydä julkisella paikalla tai suojaamattoman yhteyden kautta, jotta ulkopuoliset eivät kuule keskustelua
- b) luottamuksellista tietoa sisältäviä viestejä ei saisi jättää puhelinvastaajiin tai ääniviesteinä, koska ulkopuoliset voivat kuunnella ne tai ne voivat tallentua yhteiskäytössä oleviin järjestelmiin tai väärin paikkoihin näppäilyvirheen vuoksi
- c) heille olisi tehtävä taustatarkistukset ja turvallisuusselvitykset sillä tasolle, että heillä on lupa kuunnella keskustelua
- d) heidän olisi varmistettava, että keskustelutila on riittävän turvallinen (esim. äänieristys, ovi kiinni)
- e) he aloittavat arkaluonteiset keskustelut sillä huomautuksella, että paikallaolijat tietävät pian kuolemien tietojen luokitustason ja tietojen käsittelyä koskevat rajoitukset.

#### Lisätiedot

Ei lisätietoja.

### **5.15 Pääsynhallinta (EN)**

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttövaltuushallinta	#Suojaaminen

#### **Hallintakeino**

Säännöt, joilla hallitaan fyysisistä ja ohjelmallista pääsyä tietoihin ja niihin liittyviin omaisuuseriin, olisi laadittava ja toteutettava liiketoimintaa ja tietoturvallisuutta koskevien vaatimusten mukaisesti.

#### **Tarkoitus**

Varmistetaan luvallinen pääsy tietoihin ja niihin liittyviin omaisuuseriin sekä estetään luvaton pääsy niihin.

## Ohjeistus

Tietojen ja niihin liittyvien omaisuuserien omistajien olisi määritettävä pääsynhallintaan liittyvät tietoturvallisuutta koskevat ja liiketoiminnalliset vaatimukset. Olisi määriteltävä pääsynhallintaa koskevat kohdennetut toimintaperiaatteet, joissa otetaan huomioon nämä vaatimukset ja jotka olisi viestittävä tärkeimmille sidosryhmille.

Näissä vaatimuksissa ja kohdennetuissa toimintaperiaatteissa olisi tarkasteltava seuraavia asioita:

- a) sen määrittäminen, ketkä tarvitsevat minkä tyypisen pääsyn tietoihin ja niihin liittyviin omaisuuseriin
- b) sovellusten turvallisuus (ks. [kohta 8.26](#))
- c) fyysinen pääsy, jota olisi tuettava asianmukaisella kulunvalvonnalla (ks. [kohdat 7.2, 7.3](#) ja [7.4](#))
- d) tietojen jakaminen ja sen edellytykset (esim. periaate tiedon levittämisestä ainoastaan asianosaisille) sekä tietojen luokittelusta aiheutuvat vaatimukset (ks. [kohdat 5.10, 5.12](#) ja [5.13](#))
- e) pääkäyttäjä- ja ylläpito-oikeuksien rajoukset (ks. [kohta 8.2](#))
- f) tehtävien eriyttäminen ja jääviys (ks. [kohta 5.3](#))
- g) lainsäädäntö, viranomaismääräykset ja kaikki sopimuksiin perustuvat velvoitteet, jotka koskevat tietoihin tai palveluihin pääsyn rajoittamista (ks. [kohdat 5.31, 5.32, 5.33, 5.34](#) ja [8.3](#))
- h) pääsynhallintatoimintojen eriyttäminen (esim. pääsyoikeuksien hakeminen, pääsyn myöntäminen, oikeuksien hallinnointi)
- i) pääsyoikeuspyyntöjen hyväksyminen organisaation pääöksenteossa noudattamien yleisten menettelyiden mukaisesti (ks. [kohdat 5.16](#) ja [5.18](#))
- j) pääsyoikeuksien hallinta (ks. [kohta 5.18](#))
- k) lokikirjaukset (ks. [kohta 8.15](#)).

Pääsynhallintaa koskevat säännot olisi toteutettava määrittelemällä ja kartoittamalla, mitä pääsyoikeuksia ja -rajoituksia on ja miten niiden olisi oltava (ks. [kohta 5.16](#)). Pääsyoikeus voidaan antaa ihmiselle tai tekniselle tai loogiselle kohteelle (esim. kone, laite tai palvelu). Pääsynhallintaa voidaan yksinkertaistaa kohdistamalla määritellyt roolit käyttäjäryhmille.

Pääsynhallintaa koskevien sääntöjen määrittelyssä ja toteuttamisessa olisi otettava huomioon seuraavat asiat:

- a) pääsyoikeuksien ja tietojen luokittelun sovittaminen toisiinsa
- b) pääsyoikeuksia ja turvallista toimitilaan koskevien tarpeiden ja vaatimusten sovittaminen yhteen
- c) kaikkien hajautetuissa tietojenkäsittely-ympäristöissä olevien tietoliikenneyhteyksien, liittymien ja rajapintojen tarkastelu, jotta myönnetään pääsy vain niihin tietoihin ja niihin liittyviin omaisuuseriin, koskien myös verkkoon ja verkkopalveluita, joihin käyttövaltuudet on tarpeen myöntää
- d) se, kuinka käyttäjän dynaamisen todentamiseen liittyvät tekijät voidaan ottaa huomioon.

## Lisätiedot

Pääsynhallinnassa käytetään usein yleisiä periaatteita. Kaksi yleisimmin käytettyä periaatetta ovat seuraavat:

- a) Tarve tietää (need-to-know): henkilölle myönnetään pääsyoikeus vain sellaiseen tietoon, jota hän tarvitsee työtehtävänsä tekemiseen (eri tehtävillä ja rooleilla on erilaiset tietotarpeet ja täten erilaiset pääsyprofiliit).

- b) Tarve käyttää (need-to-use): pääsyoikeus tietoteknologiseen infrastruktuuriin vain, kun siihen on selkeä tarve.

Pääsynhallintasääntöjä määriteltäessä olisi otettava huomioon erityisesti seuraavat asiat:

- Sääntöjä luotaessa lähtökohtana olisi oltava ennenmin vähimmän oikeuden periaate (*principle of least privilege*) eli "kaikki on kiellettyä, ellei sitä erikseen sallita" mieluummin kuin joustavampi "kaikki on sallittua, ellei sitä erikseen kielletä".
- Muutokset tietojen luokittelumerkinnöissä (ks. [kohta 5.13](#)), jotka tietojenkäsittelypalvelu käynnistää automaattisesti tai jotka käynnistää käyttäjä.
- Muutokset käyttöoikeuksissa, jotka tietojärjestelmä käynnistää automaattisesti tai jotka pääkäyttäjä tekee.
- Miten säännöt hyväksytään ja miten tehdään niiden säennöllinen katselointi.

Pääsynhallintasääntöjen tukena olisi oltava dokumentoituja menettelyjä (ks. [kohdat 5.17, 5.18, 8.2, 8.3, 8.4, 8.5 ja 8.18](#)) ja määriteltyjä vastuita (ks. [kohdat 5.2 ja 5.17](#)).

Pääsynhallinnan toteuttamiseen on erilaisia tapoja, kuten pakollinen pääsynhallinta (MAC), harkinnavarainen pääsynhallinta (DAC), rooliperustainen pääsynhallinta (RBAC) ja attribuuttiperustainen pääsynhallinta (ABAC).

Pääsynhallintaa koskevat säännöt voivat sisältää myös dynaamisia elementtejä (esim. toiminnon, joka arvoo aiempia käyttökertoja tai määriteltyjä ympäristöä koskevia arvoja). Pääsynhallintaa koskevat säännöt voidaan toteuttaa eritasoisella tarkkuudella, aina kokonaista verkoista tai järjestelmistä rajattuihin tietokenttiin asti, ja voivat ottaa myös huomioon esimerkiksi käyttäjän sijainnin tai käytetyn verkkoyhteyden tyypin. Näillä periaatteilla ja pääsynhallinnan tarkkuudella voi olla merkittäviä kustannusvaikutuksia. Tiukemmat säännöt ja korkeampi tarkkuus johtaa yleensä suurempia kustannuksiin. Liiketoiminnallisten vaatimusten ja riskejä koskevien näkökohtien avulla olisi määriteltävä, mitä pääsynhallinnan em. sääntöjä käytetään ja mikä tarkkuustaso vaaditaan.

## 5.16 Identiteetin hallinta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttövaltuushallinta	#Suojaaminen

### Hallintakeino

Identiteettien koko elinkaarta olisi hallittava.

### Tarkoitus

Mahdollistetaan organisaation tietoja ja niihin liittyviä omaisuuseriä käyttävien henkilöiden ja järjestelmien yksilöllinen tunnistaminen sekä pääsyoikeuksien asianmukainen hallinnointi.

### Ohjeistus

Identiteetin hallinnassa käytettävien prosessien olisi varmistettava, että

- henkilölle myönnettävistä käyttäjätunnusista kukin on sidottu vain yhteen henkilöön, jolloin tämä on vastuussa kaikista kyseisen identiteetin tekemistä toimenpiteistä
- useammille henkilölle myönnetty käyttäjätunnukset (esim. jaetut identiteetit) ovat sallittuja vain silloin, kun ne ovat välttämättömiä liiketoiminnallisista tai toiminnallisista syistä ja niiden myöntäminen edellyttää nimenomaisen hyväksynnän ja asian dokumentoinnin

- c) muille kuin luonnollisille henkilöille myönnettyjen identiteettien hyväksyntä on asianmukaisesti eriytettyä muiden tunnusten myöntämisestä ja niiden jatkuva valvonta on järjestetty ja on riippumatonta oikeuksien myöntämisestä
- d) identiteeteiltä poistetaan pysyvästi toimintaoikeudet tai se jäädytetään viivyttelemättä, kun niille ei ole enää tarvetta (esim. jos niihin liitettyä henkilö ei enää ole, identiteettiä ei enää käytetä tai jos identiteettiin liitetty henkilö on poistunut organisaatiosta tai hänen roolinsa on vaihtunut)
- e) kussakin toimintaympäristössä yhtä tahoa vastaa vain yksi identiteetti (eli vältetään useampien identiteettien osoittamista samalla taholle samassa toimintaympäristössä [kaksoisidentiteettejä])
- f) säilytetään kaikki tärkeät käyttäjäidentiteettien käyttöä ja hallintaa sekä tunnistautumistietoja koskevat tiedot.

Organisaatiolla olisi oltava tukiprosessi, joilla se käsittelee käyttäjäidentiteetteihin liittyvien tietojen muutokset. Nämä prosessit voivat sisältää henkilön tunnistamisen uudelleen luotettavista asiakirjoista.

Kun käytetään kolmannen osapuolen tarjoamia tai myöntämiä identiteettejä (kuten sosiaalisen median varmennukset), organisaation olisi varmistettava, että kolmannen osapuolen tarjoamat identiteetit antavat riittävän luottamustason ja kaikki niihin liittyvät riskit ovat tiedossa ja käsitelty riittävällä tasolla. Tämä voi sisältää kolmansia osapuolia liittyviä hallintakeinoja (ks. [kohta 5.19](#)) sekä asiaa koskeviin tunnistautumistietoihin liittyviä hallintakeinoja (ks. [kohta 5.17](#)).

### Lisätiedot

Pääsyn myöntäminen tai peruminen tietoihin ja niihin liittyviin omaisuuseriin on yleensä monivaiheinen prosessi:

- a) luotavaa identiteettiä koskevien liiketoiminnallisten vaatimusten todentaminen
- b) tahan identiteetin todentaminen ennen sähköisen identiteetin myöntämistä
- c) identiteetin luominen
- d) identiteetin konfigurointi ja aktivoiminen, mihin sisältyy myös varsinaisen todennuspalvelun konfigurointi ja käyttöönotto
- e) pääsyoikeuksien myöntäminen identiteetille tai näiden peruminen noudattaen asianmukaisia hyväksymismenettelyjä (ks. [kohta 5.18](#)).

### 5.17 Tunnistautumistiedot (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttöövaltuushallinta	#Suojaaminen

#### Hallintakeino

Tunnistautumistietojen osoittamista ja hallintaa olisi ohjattava hallintaprosessilla, johon sisältyy henkilöstön perehdyttäminen tunnistautumistietojen asianmukaiseen käsittelyyn.

#### Tarkoitus

Varmistetaan tahojen asianmukainen tunnistaminen sekä estetään tunnistusprosessin virheet.

#### Ohjeistus

##### Tunnistautumistietojen käsittely

Tunnistus- ja hallintaprosessintietojen käsitteily- ja hallintaprosessin olisi varmistettava, että

- a) ennen ensimmäistä käyttökertaa järjestelmän luomat henkilökohtaiset salasanat tai tunnusluvut (PIN-koodit) ovat kertakäytöisiä, eivät ole helposti arvattavissa, ovat yksilöllisiä kullekin identiteetille, ja niiden vaihtaminen on pakollista ensimmäisen käytön yhteydessä
- b) luodaan menettelyt, joilla varmistetaan käyttäjän henkilöllisyys ennen uuden, korvaavan tai tilapäisen käyttäjätunnuksen myöntämistä
- c) tunnistautumisessa tarvittavat tiedot, mukaan lukien väliaikaiset tunnistautumistiedot, välitetään käyttäjille turvallisesti (esim. salatun ja tunnistusta vaativan kanavan kautta), ja vältetään suojaamattomien sähköpostiviestien käytöä tähän tarkoitukseen
- d) käyttäjä kuittaa tunnistautumistiedot vastaanotetuksi
- e) valmistajan määrittelemät oletustunnistautumistiedot vaihdetaan heti järjestelmän tai ohjelmiston asentamisen jälkeen
- f) tallenteet tunnistautumistietojen myöntämiseen ja hallintaan liittyvistä merkittävistä tapahtumista säilytetään, niiden luottamuksellisuus säilyy ja tallenteiden ylläpitomenetelmät ovat hyväksyttyjä (esim. käytetään hyväksyttyä salasanojen säilytystyökalua).

#### Käyttäjän vastuut

Kaikkia, joilla on pääsy tunnistautumistietoihin tai jotka käyttävät niitä, olisi opastettava varmistamaan, että

- a) salaiset tunnistautumistiedot, kuten salasanat, pysyvät luottamuksellisina eikä henkilökohtaisia salaisia tunnistautumistietoja jaeta muiden kanssa. Useammille käyttäjille tai muille kuin ihmisseille myönnetyjä salaisia tunnistautumistietoja jaetaan vain niiden käyttöön oikeutetuille henkilöille
- b) vaarantuneet tai paljastuneet tunnistautumistiedot vaihdetaan heti, kun tällaisesta saadaan ilmoitus tai tällaisesta on merkkejä
- c) kun tunnistautumistietoina käytetään salasanoja, valitaan suositeltavien käytäntöjen mukaisia vahvoja salasanoja, jotka
  - 1) eivät perustu sellaiseen tietoon, joka ulkopuolisen on helppo arvata tai päätellä henkilöön liittyvien tietojen (kuten nimen, puhelinnumeron tai syntymäajan) perusteella
  - 2) eivät perustu sanakirjasta löytyviin sanoihin tai tällaisten yhdistelmiin
  - 3) ovat helposti muistettavia salalauseita, joihin pyritään sisällyttämään aakkosnumeerisia merkkejä ja erikoismerkkejä
  - 4) ovat vähintään tietyn mittaisia
- d) samoja salasanoja ei käytetä erillisissä palveluissa ja järjestelmissä
- e) velvoite näiden sääntöjen noudattamiseen on myös työsuhteen ehdoissa (ks. [kohta 6.2](#)).

#### Salasanojen hallintajärjestelmä

Kun tunnistautumistietoina käytetään salasanoja, salasanojen hallintajärjestelmän olisi

- a) sallittava käyttäjien valita ja vaihtaa itse omat salasanansa ja sisällettävä varmistamismenettely kirjoitusvirheiden varalta
- b) vaadittava vahvoja salasanoja parhaita käytäntöjä koskevien suositusten mukaisesti (ks. "Käyttäjän vastuut" -kohdan luetelma kohta c)
- c) pakotettava käyttäjät vaihtamaan tilapäinen salasana ensimmäisellä kirjautumiskerralla

- d) pakotettava käyttäjät vaihtamaan salasanansa tarvittaessa esim. turvallisuuspoikkeaman jälkeen tai kun käyttäjän työsuhde päättyy ja hänellä on tiedossa olevia salasanoja aktiiviseksi jääville identiteeteille (esim. jaetut identiteetit)
- e) estettävä aiemmin käytettyjen salasanojen käyttö uudelleen
- f) estettävä yleisesti käytettyjen salasanojen sekä tietomurreissa järjestelmissä käytettyjen käyttäjänimien ja salasanojen yhdistelmien käyttö
- g) oltava näyttämättä salasanaa näytöllä, kun sitä kirjoitetaan
- h) säilytettävä ja lähetettävä salasanat salattuna.

Salasanat olisi salattava ja niistä lasketun tiivisteen laskenta olisi tehtävä hyväksytyillä ja turvallisilla salausalgoritmeilla (ks. [kohta 8.24](#)).

### Lisätiedot

Salasanat tai salalauseet ovat yleinen tunnistautumistietojen tyyppi, joilla tavallisesti todennetaan käyttäjän henkilöllisyys. Muun tyyppisiä tunnistautumistietoja ovat salausavaimet ja tunnistevälineille (esim. sirukorteille) tallennetut tiedot, jotka tuottavat todennuksessa tarvittavat tiedot ja biometriset tiedot, kuten tiedon iiriksestä tai sormenjäljistä. Lisätietoja löytyy standardisarjasta ISO/IEC 24760.

Salasanojen taajaan tapahtuva vaihtamisen vaativinen voi olla ongelmallista, sillä käyttäjät voivat tuskastua salasanan jatkuvaan vaihtamiseen, unohtaa uuden salasanansa, kirjata salasanan ylös turvattomaan paikkaan tai valita heikkoja salasanoja. Kertakirjautumistyökalujen (*Single-Sign-On*) tai muiden tunnistautumistietojen hallintatyökalujen (esim. salasanaholvien) käyttö vähentää käyttäjien tarvitsemien tunnistautumistietojen määriä ja voi näin parantaa hallintakeinon toimivuutta. Nämä työkalut saattavat kuitenkin pahentaa tunnistautumistietojen paljastumisen seurauksia.

Jotkin sovellukset edellyttävät riippumattoman kolmannen osapuolen luomaa salasanaa. Näissä tapauksissa "Salasanojen hallintajärjestelmä" -kohdan luetelmakohdat a), c) ja d) eivät ole voimassa.

## 5.18 Pääsyoikeudet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti- ja käyttövaltuushallinta	#Suojaaminen

### Hallintakeino

Pääsyoikeuksia tietoihin ja niihin liittyviin omaisuuseriin olisi myönnnettävä, katselmoitava, muokattava ja poistettava organisaation pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden ja sääntöjen mukaisesti.

### Tarkoitus

Varmistetaan, että tietoihin ja muihin niihin liittyviin omaisuuseriin pääsy on määritelty ja hyväksytty liiketoiminnallisten vaatimusten mukaisesti.

### Ohjeistus

#### Pääsyoikeuksien myöntäminen ja poistaminen

Todennetulle identiteeteille myönnettyjen fyysisien tai ohjelmallisten pääsyoikeuksien myöntämis- tai kumoamisprosessin olisi sisällettävä:

- a) Tietojen ja niihin liittyvien omaisuuserien omistajalta saatu valtuutus niiden käyttöön (ks. [kohta 5.9](#)). Toisinaan voi olla asianmukaista hankkia johdolta erillinen hyväksyntä pääsyoikeudelle.
- b) Liiketoiminnallisten vaatimusten ja organisaation pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden ja sääntöjen ottaminen huomioon.

- c) Otettava huomioon tehtävien eriyttäminen, mukaan lukien pääsyoikeuksien hyväksynnästä ja toteuttamisesta vastaan roolien eriyttäminen ja ristiriitaisten roolien eriyttäminen.
- d) Varmistetaan tarpeettomien pääsyoikeuksien poistaminen tietoihin ja muihin niihin liittyviin omaisuuseriin. Erityisesti on varmistettava, että pääsyoikeudet poistetaan viivyttelemättä käyttäjiltä, jotka ovat poistuneet organisaatiosta.
- e) Harkitaan, että myönnetyään väliaikaisia, määriteltyä aikana poistettavia pääsyoikeuksia etenkin tilapäistyövoimalle tai siinä tapauksessa, että henkilöstö tarvitsee tilapäistä pääsyä jostain erityisestä syystä.
- f) Todennetaan, että myönnetty pääsytaulo on linjassa pääsynhallintaa (ks. [kohta 5.15](#)) koskevien kohdennettujen toimintaperiaatteiden kanssa ja yhdenmukainen muiden tietoturvavaatimusten, kuten tehtävien eriyttämisen (ks. [kohta 5.3](#)), kanssa.
- g) Varmistetaan, että pääsyoikeudet aktivoidaan (esim. palveluntuottajalta) vasta, kun hyväksymismenettely on saatettu loppuun.
- h) Keskitetyn rekisterin ylläpitäminen käyttäjätunnuselle (tunnus, looginen tai fyysinen) myönnetyistä pääsyoikeuksista tietoihin ja niihin liittyviin omaisuuseriin.
- i) Roolia tai tehtävää vaihtaneiden tai organisaatiosta poistuneiden käyttäjien pääsyoikeuksien muokkaaminen tarpeen mukaan.
- j) Fyysisen ja ohjelmallisten pääsyoikeuksien poistaminen tai muokkaaminen, mikä voidaan tehdä poistamalla, kumoamalla tai korvaamalla avaimet, tunnistautumistiedot, henkilökortit tai palveluiden tilaukset.
- k) Käyttäjän fyysisen ja loogisen pääsyoikeuksien muutoksia koskevien tallenteiden ylläpitäminen.

#### Pääsyoikeuksien uudelleenarvointi

Fyysisen ja ohjelmallisten pääsyoikeuksien säännöllisissä katselmoinneissa olisi otettava huomioon seuraavat asiat:

- a) Käyttäjän pääsyoikeudet, kun tämän organisaatiossa tapahtuu muutoksia (esim. työtehtävien muutokset, ylennykset, alennukset) tai työsuhde päättyy (ks. [kohdat 6.1–6.5](#)).
- b) Ylläpito-oikeuksien myöntäminen.

#### Työsuhteen muuttumista tai päätymistä koskevat näkökohdat

Ennen työsuhteen muuttumista tai päätymistä käyttäjän tietoja ja niihin liittyviä omaisuuseriä koskevat pääsyoikeudet olisi katselmoitava seuraavien riskien arvioinnin perusteella:

- a) onko aloite työsuhteen päätymiseen tai muuttamiseen tullut käyttäjältä vai johdolta sekä päätymisen syy
- b) käyttäjän vastuu
- c) sen omaisuuden arvo, johon työntekijällä on pääsyoikeudet.

#### **Lisätietoa**

Liiketoimintavaatimusten perusteella olisi harkittava pääsyrooleja, jotka yhdistäisivät useita pääsyoikeuksia tyypillisiin pääsyoikeusprofilleihin. Pääsyn pyytämistä ja pääsyoikeuksien katselointia on helpompi hallita tällaisten roolien tasolla kuin yksittäisten oikeuksien tasolla.

Olisi syytä harkita, että työ- ja palvelusopimuksiin sisällytetään sanktiot, jotka seuraavat oikeuksien väärinkäytöstä (ks. [kohdat 5.20, 6.2, 6.4 ja 6.6](#)).

Jos kyseessä on organisaation aloitteesta päättynyt työsuhde, tyytymättömät työntekijät tai ulkopuolisen osapuolen käyttäjät saattavat tahallaan turmella tietoa tai sabotoida tietojenkäsittelypalveluita. Jos henkilö irtisanoutuu tai irtisanotaan, hänen voi olla houkutus kerätä tietoa käytettäväksi tulevaisuudessa.

Kloonaus on tehokas tapa myöntää pääsyoikeuksia käyttäjille. Sen olisi kuitenkin perustuttava organisaation selkeästi yksilöimiin erillisin rooleihin eikä vain identiteetin ja kaikkien siihen liittyvien pääsyoikeuksien kloonaamiseen. Kloonaamiseen sisältyy riski siitä, että myönnetään liian laajat pääsyoikeudet tietoihin ja niihin liittyviin omaisuuseriin.

## 5.19 Tietoturvallisuus toimittajasuhdeissa (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuhdeiden_hallinta	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

### Hallintakeino

Olisi määriteltävä ja toteutettava prosessit ja menettelyt, joilla hallitaan toimittajan tuotteiden tai palveluiden käyttöön liittyviä tietoturvariskejä.

### Tarkoitus

Ylläpidetään sovittua tietoturvallisuuden tasoa toimittajasuhdeissa.

### Ohjeistus

Organisaation olisi laadittava toimittajasuhdeita koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille olennaisille sidosryhmille.

Organisaation olisi yksilöitää ja toteutettava prosessit ja menettelyt, joilla käsitellään toimittajan tuotteiden ja palveluiden käyttöön liittyviä tietoturvariskejä. Tämän olisi koskettava myös organisaation käyttämiä pilvipalvelun tuottajien resursseja. Näiden prosessien ja menettelyiden olisi sisällettävä ne, jotka organisaation on tarkoitus toteuttaa, sekä ne, joiden toteuttamista organisaatio edellyttää toimittajalta, kun toimittajan tuotteita tai palveluita otetaan käyttöön tai poistetaan käytöstä. Tällaisia ovat esimerkiksi

- a) sellaisten toimittajaryhmien (esim. tieto- ja viestintätekniset palvelut, logistiikkapalvelut, taloushallinto ja tietotekniset infrastruktuurikomponentit) tunnistaminen ja dokumentointi, joilla voi olla vaikutusta organisaation tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen
- b) menetelmien laatiminen toimittajien arviontiin ja valintaan tietojen, tuotteiden ja palveluiden arkaluonteisuuden perusteella (kuten markkina-analyysit, asiakasreferenssit, asiakirjojen katselointi, toimipaikalla tapahtuva arvointi, sertifiointi)
- c) sellaisten toimittajien tuotteiden ja palveluiden arviontiin pohjautuva valinta, joilla on riittävä tietoturvallisuuden hallintakeinot, sekä niiden katselointi; erityisesti niiden toimittajan toteuttamien hallintakeinojen tarkkuus ja kattavuus, jotka varmistavat toimittajan tietojen ja tietojenkäsittelyn eheyden ja näin organisaation tietoturvallisuuden
- d) sellaisten organisaation tietojen, tieto- ja viestintäteknisten palveluiden ja fyysisen infrastruktuurien määrittelemisen, joihin toimittajilla on pääsy ja jota ne voivat seurata, hallita tai käyttää
- e) toimittajien toimittamien sellaisten tieto- ja viestintäteknisten komponenttien ja palveluiden tyyppejen määrittelemisen, joilla voi olla vaikutusta organisaation tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen
- f) seuraaviin asioihin liittyvien turvallisuusriskien arvointi ja hallinta:
  - 1) toimittajan organisaation tietojen ja niihin liittyvien omaisuuserien käyttöön liittyvät riskit, mukaan lukien riskit, jotka syntyvät toimittajan mahdollisten pahantahtoisten työntekijöiden toimista
  - 2) toimittajan toimittamien tuotteiden (myös näiden tuotteiden ohjelmistokomponenttien ja alikomponenttien) tai palveluiden toimintahäiriöihin tai haavoittuvuuksiin liittyvät riskit

- g) laadittujen tietoturvavaatimusten noudattamisen valvonta kullekin toimittaja- ja pääsytyypille, mukaan lukien kolmannen osapuolen katselmoinnit ja tuoteearvioinnit
- h) toimittajan tietoturvaan liittyvän vaatimustenvastaisuuden poikkeamien käsitteily riippumatta siitä, havaittiinko ne tilaajan tekemällä valvonnalla vai jotenkin muuten
- i) toimittajien tuotteisiin ja palveluihin liittyvien häiriöiden ja poikkeustilanteiden käsitteily mukaan lukien organisaation ja toimittajien vastuu
- j) kriisinsietokyky- ja tarvittaessa palautumis- ja poikkeustilannejärjestelyt, joilla varmistetaan toimittajan tietojen ja tietojenkäsittelyn saatavuus ja näin myös organisaation tietojen saatavuus
- k) toimittajan henkilöstön kanssa tekemissä olevan organisaation henkilöstön koulutus koskien toimintasääntöjä, kohdennettuja toimintaperiaatteita, prosesseja ja menettelyjä sekä toimintaa, joihin vaikuttavat toimittajan ominaisuudet ja toimittajan pääsyoikeudet organisaation järjestelmiin tai tietoon
- l) tietojen, niihin liittyvien omaisuuserien ja kaiken muun, minkä siirtäminen on tarpeen, siirtämisen hallinta, sekä sen varmistaminen, että tietoturvallisuutta ylläpidetään koko siirron ajan
- m) vaatimukset, joilla varmistetaan toimittajasuhteen turvallinen päätäminen, mukaan lukien
  - 1) pääsyoikeuksien poistaminen
  - 2) tietojen käsitteily suhteen päättymisen yhteydessä ja sen jälkeen
  - 3) yhteistyön aikana syntyneen aineettoman omaisuuden omistajuuden määrittäminen
  - 4) tietojen siirrettävyys toimittajan muutoksissa tai siirtämisessä takaisin tilaajalle
  - 5) asiakirjojen hallinta
  - 6) omaisuuden palauttaminen
  - 7) tietojen ja niihin liittyvien omaisuuserien turvallinen hävittäminen
  - 8) luottamuksellisuuteen liittyvät vaatimukset, jotka jäävät voimaan
- n) toimittajan henkilöstöltä ja toimitiloilta vaadittu henkilöstöturvallisuuden ja fyysisen turvallisuuden taso.

Olisi tarkasteltava menettelyjä tietojenkäsittelyn jatkamiseen siinä tapauksessa, että toimittaja ei kykene enää toimittamaan tuotteitaan tai palveluitaan (esim. häiriötilanteen takia, koska toimittaja on ajautunut konkurssiin tai ei enää tarjoa joitain komponentteja teknologian kehityksen vuoksi), jotta voidaan välttää viipeet korvaavien tuotteiden tai palveluiden hankinnassa (esim. tunnistetaan vaihtoehtoinen toimittaja etukäteen tai käytetään korvaavia toimittajia säännöllisesti).

## Lisätiedot

Jos organisaatiolla ei ole mahdollisuutta asettaa toimittajaa koskevia vaatimuksia, organisaation olisi

- a) otettava tässä hallintakeinossa esitetty ohjeistus huomioon, kun se tekee päätöksiä toimittajan ja sen tuotteiden tai palveluiden valinnasta
- b) toteutettava riskien arviointiin perustuvia kompensoivia hallintakeinoja.

Toimittajan riittämätön tietoturvallisuuden hallinta voi altistaa tiedot riskeille. Olisi määritettävä ja otettava käyttöön hallintakeinot, joilla hallitaan toimittajan pääsyä tietoihin ja niihin liittyviin omaisuuseriin. Jos esimerkiksi tiedon luottamuksellisuuden suojaaminen on erityisen tärkeää, vaitiolositoumus tai tietojen salaus voivat tulla kyseeseen. Toinen esimerkki ovat tietosuojariskit, kun toimittajasopimukseen sisältyy tiedon siirtoa tai käyttöä maan rajojen yli. Organisaation täytyy olla tietoinen siitä, että laillinen tai sopimuksellinen vastuu tiedon suojaamisesta säilyy organisaatiolla.

Myös toimittajan toimittamia tieto- ja viestintäteknisen infrastruktuurin komponentteja tai palveluita koskevat riittämättömät hallintakeinot voivat aiheuttaa riskejä. Komponenttien tai palveluiden toimintahäiriöt tai haavoittuvuudet voivat aiheuttaa organisaatioon tai sen sidosryhmään kohdistuvia tietoturvaloukkauksia (esim. ne voivat aiheuttaa haittaohjelmatartunnan, hyökkäyksen tai muuta haittaa myös muille kuin vain organisaatiolle).

Katso lisätietoja standardista ISO/IEC 27036-2.

## 5.20 Toimittajasopimusten tietoturvallisuus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden hallinta	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

### Hallintakeino

Kunkin toimittajan kanssa olisi laadittava ja sovittava asianmukaiset tietoturvavaatimukset, jotka perustuvat kyseisen toimittajasuhteen tyyppiin.

### Tarkoitus

Ylläpidetään sovittua tietoturvallisuuden tasoa toimittajasuhdeissa.

### Ohjeistus

Toimittajasopimukset olisi laadittava ja dokumentoitava sen varmistamiseksi, että organisaation ja toimittajan välillä on selkeä ymmärrys osapuolten velvoitteista tietoturvavaatimusten täyttämisessä.

Seuraavien ehtojen sisällyttämistä sopimuksiin voidaan harkita, jotta voidaan täyttää tietoturvavaatimukset:

- a) toimitettavan tai käytettävän tiedon sekä tiedon toimittamiseen tai käyttöön käytettävien menetelmien kuvaus
- b) tietojen luokittelun organisaation luokitteluperiaatteiden mukaisesti (ks. [kohdat 5.10, 5.12 ja 5.13](#))
- c) organisaation omien luokitteluperiaatteiden ja toimittajan luokitteluperiaatteiden vertailu
- d) laki, asetukset, viranomaisten ja sopimusten vaatimukset mukaan lukien tietosuoja, immateriaalioikeudet ja tekijänoikeudet sekä kuvaus siitä, miten niiden täyttyminen varmistetaan
- e) velvoite kullekin sopimusosapuolelle sovittujen hallintakeinojen toteuttamisesta mukaan lukien pääsynhallinta, suorituskyvyn arviointi, muu seuranta, raportointi ja auditointi sekä toimittajan vastuu noudattaa organisaation turvallisuusvaatimuksia
- f) tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön säännöt, mukaan lukien kielletty käyttö
- g) organisaation tietoja ja niihin liittyviä omaisuuseriä koskevien käyttövaltuuksien myöntäminen toimittajan henkilöstölle sekä niiden poistaminen toimittajan henkilöstöltä (esim. tarkka luettelo toimittajan henkilöstöstä, jolla on valtuudet käyttää organisaation tietoja ja niihin liittyviä omaisuuseriä)
- h) toimittajan tieto- ja viestintäteknistä infrastruktuuria koskevat tietoturvavaatimukset ja etenkin vähimmäistietoturvavaatimukset kullekin tieto- ja pääsytyypille, joka toimii perustana yksittäisille toimittajasopimuksille organisaation liiketoimintatarpeiden ja riskikriteerien perusteella
- i) korvaukset ja sanktiot tilanteissa, joissa palveluntuottaja ei kykene täytämään vaatimuksia
- j) häiriöiden hallintaa koskevat vaatimukset ja menettelyt (etenkin ilmoittaminen ja yhteistyö häiriöiden korjaamisen aikana)

- k) sovittujen toimintatapojen ja tilaajan tietoturvavaatimusten vuoksi tehtävä koulutus esim. häiriöihin reagoimiselle ja oikeuksien myöntämiselle
- l) alihankintaa koskevat säännöt mukaan lukien tarvittavat hallintakeinot, kuten alihankkijoiden käytöstä sopiminen (esim. edellytetäänkö, että niillä on samat velvoitteet kuin toimitajalla, alihankkijoista on saatavilla luettelo ja mahdollisista muutoksista ilmoitetaan)
- m) yhteyshenkilöt mukaan lukien tietoturvaongelmien yhteyshenkilö
- n) toimitajan henkilöstölle tehtäviä taustatarkistuksia ja turvallisuusselvityksiä (jos tämä on laissa sallittua) koskevat asiat, kuten vastuu taustatarkistusten ja turvallisuusselvitysten teettämisestä ja ilmoitusmenettelyt, jos taustatarkistusta tai turvallisuusselvitystä ei ole tehty tai sen tuloksissa on huomautettavaa
- o) aineisto, jolla toimittaja osoittaa prosessiensa vaatimustenmukaisuuden, kuten kolmannen osapuolen auditoinnit sekä riippumattoman arvioijan tekemä muu raportti hallintakeinojen toimivuudesta
- p) lupa auditoida sopimukseen liittyvät toimittajan prosessit ja hallintakeinot
- q) toimitajan velvollisuus toimittaa säännöllisesti raportti hallintakeinojen toimivuudesta sekä hyväksyntä raportissa esille tuotujen merkittävien ongelmien ripeästä korjaamisesta
- r) palvelun tai tuotteen puutteiden korjaaminen ja ristiriitojen ratkaisuprosessi
- s) tietojen varmuuskopioointia koskeva suunnitelma, joka on organisaation tarpeiden mukainen (suhteessa tietojen tallennuksen kapasiteettiin, tallenteiden fyysiseen ja loogiseen sijaintiin, varmuuskopioinnin suoritusvälisiin sekä varmuuskopioilta palauttamisen nopeuteen)
- t) varmistetaan, että käytettävässä on vaihtoehtoinen toimipaikka (eli toipumisen aikaiseen toimintaan tarkoitettut tilat), joka ei ole alttiina samoille uhkille kuin pääasiallinen toimipaikka, sekä varahallintakeinot (vaihtoehtoiset hallintakeinot) tilanteisiin, joissa pääasialliset hallintakeinot eivät toimi
- u) muutoksenhallinnan prosessi, jolla varmistetaan, että organisaatio saa ennakkotiedon muutoksista ja että organisaatiolla on mahdollisuus olla hyväksymättä näitä
- v) fyysisen turvallisuuden hallintakeinot, jotka ovat tietojen luokitusta vastaavalla tasolla
- w) tietojen siirtämistä koskevat hallintakeinot, joilla tietoa suojataan siirron ja lähetämisens aikana
- x) sopimusehdot sopimuksen päättyessä, mukaan lukien tallenteiden hallinta, omaisuuden palauttaminen, tietojen ja niihin liittyvien omaisuuserien turvallinen hävittäminen sekä luottamuksellisuutta koskevat velvoitteet, jotka ovat voimassa sopimuksen päättyy
- y) vaatimus tavoista, joilla organisaation toimittajan hallussa olevat tiedot poistetaan turvallisesti heti, kun niille ei ole enää tarvetta
- z) varmistetaan, että sopimuksen päättyessä toimittajalla on velvollisuus tukea palvelun siirtoa toiselle toimittajalle tai takaisin organisaatiolle.

Organisaation olisi luotava ja ylläpidettävä rekisteriä kolmansien osapuolten kanssa solmituista sopimuksista (ns. sopimusrekisteri, esim. sopimukset, aiepöytäkirjat ja tiedonvaihtosopimukset), jotta se tietää, mihin sen tietoja siirretään. Organisaation olisi säännöllisesti katselmoitava, arvioitava tarpeellisuus ja päivitetävä kolmansien osapuolten kanssa solmitut sopimuksensa, jotta voidaan varmistaa, että ne ovat yhä tarpeellisia ja tietoturvavaatimusten mukaisia.

## Lisätiedot

Sopimukset saattavat olla hyvin erilaisia eri organisaatioiden ja erityyppisten toimittajien välillä. Siksi olisi syytä olla huolellinen siinä, että kaikki tärkeimmät toimittajalle asetettavat tietoturvavaatimukset sisältyvät sopimukseen.

Lisätietoja toimittajasopimuksista on standardisarjassa ISO/IEC 27036. Lisätietoja pilvipalveluita koskevista sopimuksista on standardisarjassa ISO/IEC 19086.

## 5.21 Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen

### Hallintakeino

Olisi määriteltävä ja toteutettava prosesseja ja menettelyjä, joilla hallitaan tieto- ja viestintäteknisten tuotteiden ja palveluiden toimitusketjuihin liittyviä tietoturvariskejä.

### Tarkoitus

Ylläpidetään sovittua tietoturvallisuuden tasoa toimittajasuheteissa.

### Ohjeistus

Yleisten toimittajasuheteita koskevien tietoturvavaatimusten lisäksi olisi otettava huomioon seuraavat asiat, kun tarkastellaan tietoteknisen toimitusketjun turvallisuuteen liittyvää tietoturvallisuutta:

- a) tieto- ja viestintäteknisiä tuotteita koskevien tietoturvavaatimusten määritteleminen
- b) edellytetään, että tieto- ja viestintäteknisten palveluiden toimittajat välittävät organisaation turvallisuusvaatimukset koko toimitusketjuun, jos toimittaja käyttää alihankintaa organisaatiolle toimitettavien tieto- ja viestintätekniikkapalveluiden tuottamisessa
- c) edellytetään, että tieto- ja viestintäteknisten palveluiden toimittajat välittävät asianmukaiset turvallisuuskäytännöt koko toimitusketjuun, jos tuotteisiin sisältyy muita toimittajilta tai muita kolmansilta osapuolilta (esim. alihankinta ohjelmistokehittäjiltä tai ohjelmistokomponenttien toimittajilta) ostettuja tai muutoin hankittuja komponentteja
- d) edellytetään, että tieto- ja viestintäteknisten tuotteiden toimittajat antavat tiedot, joista käy ilmi tuotteissa käytetyt ohjelmistokomponentit
- e) edellytetään, että tieto- ja viestintäteknisten tuotteiden toimittajat antavat tiedot, joista selviää tuotteiden turvallisuusomaisuudet sekä tiedot siitä, miten tuote asennetaan ja otetaan turvallisesti käyttöön (konfigurointi)
- f) tuotteen toiminnan valvontan ja hyväksyttävien todennusmenetelmien käyttämiseen sen todentamisessa, että toimitetut tieto- ja viestintätekniset tuotteet ja palvelut ovat valmistajan ilmoittamien turvallisuusvaatimusten mukaisia; esimerkkejä tällaisista toimittajien katselointimenettelyistä ovat toimittajan tietoturvatoimia koskeva tunkeutumistestaus (penetraatiotestaus) ja kolmannen osapuolen tekemien auditointien ja muiden todennusten kelpuuttaminen näytöksi vaatimustenmukaisudesta (ns. hyväksiluku)
- g) sellaisten tuote- tai palvelukomponenttien tunnistaminen ja dokumentointi, jotka ovat kriittisiä toiminnallisuuden ylläpitämisen kannalta ja tästä syystä vaativat korotettua turvallisuutta, huolellisuutta ja lisävalvontaa, kun ne toteutetaan organisaation ulkopuolella, etenkin jos toimittajat ulkoistavat osia tuotteesta tai palvelusta muille toimittajille
- h) toimittajan vakuutus siitä, että kriittiset komponentit ja niiden alkuperä voidaan jäljittää toimitusketjussa
- i) toimittajan vakuutus siitä, että toimitetut tieto- ja viestintätekniset tuotteet toimivat ilman odottamattomia tai epätoivottuja toimintoja

- j) prosessien toteuttaminen, jotta voidaan varmistaa, että toimittajalta saatavat komponentit ovat aitoja ja alkuperäisiä eikä niitä ole muutettu spesifikaatioiden vastaisiksi; esimerkkejä menetelmistä ovat peukaloinnin osoittavat merkinnät, salaustiivisteiden laskentaan perustuva todentaminen tai sähköinen allekirjoitus; spesifikaatioista poikkeavan toiminnan valvonta voi osoittaa luvattoman muuttamisen tai väärennökset; luvattoman muuttamisen estäminen ja havaitseminen olisi sisällytettävä järjestelmäkehityksen elinkaaren eri vaiheisiin, kuten suunnittelun, kehittämiseen, integrointiin, käyttöön ja ylläpitoon
- k) toimittajan vakuutus siitä, että tieto- ja viestintätekniiset tuotteet saavuttavat vaaditut turvallisuustasot, esim. virallisen sertifioinnin tai muun hyväksynnän kautta; tällainen on esim. *Common Criteria Recognition Arrangement*-järjestely
- l) toimitusketjun ongelmien liittyvän tiedon jakamista organisaation ja toimittajien kesken koskevien sääntöjen määrittelemisen
- m) tieto- ja viestintätekniisten komponenttien elinkaaren ja saatavuuden sekä niihin liittyvien turvallisuusriskien hallintaa koskevien prosessien toteuttaminen. Tämä sisältää sellaisten riskien hallinnan, jotka liittyvät komponentteihin, joita ei ole enää saatavilla, koska toimittaja ei ole enää toiminnassa tai ei enää toimita näitä komponentteja teknologisen kehityksen johdosta. Vaihtoehtoisten toimittajien selvittäminen sekä ohjelmiston ja sen hallinnan edellyttämän osaamisen siirtäminen toiselle toimittajalle olisi myös tarkasteltava.

## Lisätiedot

Tieto- ja viestintätekniikan toimitusketjun riskienhallintakäytännöt perustuvat yleisille tietoturvallisuuden, laadun, projektinhallinnan ja järjestelmäsuunnittelun periaatteille, mutta ne eivät korvaa niitä.

Organisaatioita kehotetaan työskentelemään toimittajien kanssa, jotta he ymmärtävät tieto- ja viestintätekniikan toimitusketjun toiminnan ja kaikki siihen liittyvät asiat, joilla on merkittävä vaikutus toimitettaviin tuotteisiin ja palveluihin. Organisaatiot voivat vaikuttaa tieto- ja viestintätekniikan toimitusketjun tietoturvakyötäntöihin tekemällä toimittajasopimuksissa selväksi, mitkä asiat toimittajan olisi hoidettava kuntoon, mitkä taas ovat muiden tieto- ja viestintätekniikan toimitusketjussa olevien toimittajien vastuulla.

Tieto- ja viestintätekniikkaa olisi hankittava ainoastaan hyvämaineisista lähteistä. Ohjelmistojen ja laitteistojen luotettavuus on laadunvarmistukseen liittyvä asia. Vaikka organisaatiolla ei yleensä ole mahdollisuutta tehdä tarkistuksia toimittajiensa laadunvarmistusjärjestelmien toimintaan, se voi tehdä luotettavia arvioita toimittajan maineen perusteella.

Tässä kohdassa tarkoitettu tieto- ja viestintätekniikan toimitusketju sisältää myös pilvipalvelut.

Esimerkkejä tieto- ja viestintätekniikan toimitusketjuista ovat:

- a) pilvipalvelujen tuottaminen siten, että pilvipalvelun tuottajan toiminta perustuu erillisiin ohjelmistonkehittäjiin, televiestintäpalveluiden tuottajiin tai laitteistotoimittajiin
- b) esineiden internet, jossa palvelu sisältää laitevalmistajat, pilvipalvelun tuottajat (esim. IoT-alustojen operaattorit), mobiili- ja verkkopalveluiden kehittäjät sekä ohjelmistokirjastojen toimittajat
- c) isännöintipalvelut, joissa palveluntuottajan toiminta tukeutuu ulkoisiin palvelutiskeihin, sisältäen ensimmäisen, toisen ja kolmannen tason tukipalvelut.

Lisätietoja ja riskien arvointia koskevaa ohjeistusta löytyy standardista ISO/IEC 27036-3.

Ohjelmistotunnisteet (SWID) voivat auttaa saavuttamaan paremman tietoturvallisuuden toimitusketjussa, koska se antaa tietoa ohjelmistojen alkuperästä. Lisätietoja löytyy standardista ISO/IEC 19770-2.

## 5.22 Toimittajien palvelujen seuranta, katselointi ja muutoksenhallinta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden hallinta #Tietoturvallisuuden varmentaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus

### Hallintakeino

Organisaation olisi säännöllisesti seurattava, katselmoitava, arvioitava toimittajan tietoturvallisuuskäytäntöjä ja palveluiden toimittamista ja hallittava niihin kohdistuvia muutoksia.

### Tarkoitus

Ylläpidetään toimittajasopimusten mukaista sovittua tietoturvatasoa ja palveluiden toimitustasoa.

### Ohjeistus

Toimittajan palveluiden seurannan, katselmoinnin ja muutoksenhallinnan olisi varmistettava, että sopimusten tietoturvallisuutta koskevia ehtoja ja vaatimuksia noudatetaan, tietoturvallisuuteen liittyviä häiriöitä ja ongelmia hallitaan oikein ja etteivät toimittajan palveluihin tai liiketoimintaan kohdistuvat muutokset vaikuta palvelun toimittamiseen.

Tämän olisi sisällettävä organisaation ja toimittajan välisen suhteen hallintaprosessi, jotta voidaan

- a) seurata palvelutasoja ja todentaa, että ne noudattavat sopimuksia
- b) seurata toimittajan tekemiä muutoksia, kuten
  - 1) tarjottujen palvelujen parannuksia
  - 2) uusien sovellusten ja järjestelmien kehittämistä
  - 3) toimittajan politiikkojen ja menettelyjen muutoksia tai päivityksiä
  - 4) uusia tai muokattuja hallintakeinoja, joilla korjataan tietoturvahäiriöitä ja parannetaan tietoturvallisuutta
- c) seurata toimittajan palveluihin kohdistuvia muutoksia, kuten
  - 1) verkkojen muutoksia ja parannuksia
  - 2) uusien teknologioiden käyttöä
  - 3) uusien tuotteiden tai uudempien versioiden tai julkaisujen käyttöönnottoa
  - 4) uusia kehitystyökaluja ja -ympäristöjä
  - 5) palvelun tuottamiseen käytettyjen tilojen fyysisen sijainnin muutoksia
  - 6) alihankkijoiden vaihtamista
  - 7) alihankintaa toiselta toimittajalta.
- d) katselmoida toimittajan toimittamia palveluraportteja ja järjestää säännöllisiä sopimusten mukaisia edistymisen seurantakokouksia
- e) auditoida toimittajia ja alihankkijoita, ja käyttää riippumattomia kolmannen osapuolen auditointiraportteja vaatimustenmukaisuuden osoittamiseen sekä ottaa näissä havaitut ongelmat seurantaan

- f) toimittaa tietoturvahäiriötä koskevaa tietoa ja käsitellä tämä tieto sopimusten ja tilaajan omien ohjeiden ja menettelyjen edellyttämällä tavalla
- g) katselmoida toimittajan kirjausketjut ja tallenteet, jotka koskevat tietoturvallisuuden kannalta merkittäviä tapahtumia, toimintaongelmia, häiriöitä, vikojen jäljittämistä ja toimitetun palvelun katkoja
- h) reagoida tietoturvatapahtumiin ja -häiriöihin ja hallita niitä
- i) tunnistaa tietoturvallisuuteen liittyviä haavoittuvuuksia ja hallita niitä
- j) katselmoida tietoturvanäkökohdat toimittajan suhteissa omiin toimittajiinsa
- k) varmistaa, että toimittaja ylläpitää riittävä palvelukapasiteettia sekä toteuttamiskelpoisia suunnitelmia, jotka on tehty varmistamaan palvelun jatkuvuustason ylläpito laajavaikuttaisen palvelun päättämisen tai katastrofin jälkeen (ks. [kohdat 5.29, 5.30, 5.35, 5.36](#) ja [8.14](#))
- l) varmistaa, että toimittaja nimittää vastuuhenkilön katselmoimaan sopimusten noudattamisen ja niiden vaatimusten täytäntöönpanon
- m) arvioida säännöllisesti, että toimittaja ylläpitää riittäviä tietoturvallisuuden tasoja.

Toimittajasuheteiden hallintavastuu olisi osoitettava nimetylle henkilölle tai ryhmälle. Sopimuksen vaatimusten, erityisesti tietoturvavaatimusten, täyttämisen tarkkailuun olisi osoitettava riittävät tekniset taidot ja resurssit. Jos palvelun toimittamisessa havaitaan puutteita, olisi ryhdyttävä asianmukaisiin toimenpiteisiin.

### Lisätiedot

Katso lisätietoja standardista ISO/IEC 27036-3.

## 5.23 Pilvipalvelujen tietoturvallisuus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

### Hallintakeino

Pilvipalvelujen hankinnan, käytön ja hallinnan sekä käytön lopettamisen prosessit olisi laadittava organisaation tietoturvavaatimusten mukaisesti.

### Tarkoitus

Määritellään pilvipalvelujen käytön tietoturvallisuus ja hallita sitä.

### Ohjeistus

Organisaation olisi laadittava pilvipalveluiden käyttöä koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille olennaisille sidosryhmille.

Organisaation olisi määriteltävä ja viestittävä se, miten se aikoo hallita pilvipalveluiden käyttöön liittyviä tietoturvariskejä. Kyse voi olla laajennuksesta tai organisaation olemassa olevia ulkoisten osapuolten palveluiden hallintaa koskevien toimintamallien osasta (ks. [kohdat 5.21](#) ja [5.22](#)).

Pilvipalveluiden käyttö voi sisältää tietoturvallisuutta koskevien vastuiden jakamisen sekä yhteistyön pilvipalvelun tuottajan ja pilvipalvelun asiakkaana toimivan organisaation välillä. On tärkeää, että sekä pilvipalvelun tuottajan että pilvipalvelun asiakkaana toimivan organisaation vastuu on määritelty ja toteutettu asianmukaisesti.

Organisaation olisi määriteltävä

- a) kaikki tarpeelliset pilvipalvelujen käyttöön liittyvät tietoturvavaatimukset.
- b) pilvipalvelujen valintakriteerit sekä miten laajasti pilvipalveluita hyödynnetään
- c) roolit ja vastuut, jotka liittyvät pilvipalvelujen käyttöön ja hallintaan
- d) mitä tietoturvallisuuden hallintakeinoja pilvipalvelun tuottaja hallitsee ja mitä organisaatio hallitsee pilvipalvelun asiakkaana
- e) miten pilvipalvelun tuottajan tarjoama tietoturvallisuuden osaaminen hankitaan ja miten sitä hyödynnetään
- f) miten pilvipalvelun tuottajien toteuttamat tietoturvallisuuden hallintakeinojen toiminnan onnistuminen varmennetaan
- g) miten hallitaan hallintakeinoja ja palvelujen rajapintoja ja muutoksia, kun organisaatio käyttää useita pilvipalveluita, etenkin eri pilvipalvelun tuottajilta
- h) menettelyt, joilla käsitellään pilvipalvelujen käyttöön liittyviä tietoturvahäiriöitä
- i) toimintamalli, jolla se seuraa, katselmoi ja arvioi käytettäviä pilvipalveluja hallitakseen tietoturvariskejä
- j) miten pilvipalvelun käyttöä muutetaan tai miten se lopetetaan, mukaan lukien miten pilvipalveluiden käytön lopettaminen tehdään hallitusti.

Pilvipalvelusopimukset ovat usein valmiita toimittajan sopimuspohjia, eikä niistä voi neuvotella. Organisaation olisi katselmoitava kaikkien pilvipalvelujen pilvipalvelusopimukset yhdessä palvelun tuottajien kanssa. Pilvipalvelusopimuksessa olisi käsiteltävä organisaation luottamuksellisuutta, eheyttä, saatavuutta ja tietojen käsittelyä koskevia vaatimuksia suhteessa pilvipalvelun tasoa koskeviin tavoitteisiin ja pilvipalvelun laatutavoitteisiin. Organisaation olisi toteutettava myös keskeisten riskien arvointi, jotta se voi tunnistaa pilvipalvelun käyttöön liittyvät riskit. Kaikki pilvipalvelun käyttöön liittyvät jäännösriskit olisi yksilöitvä selkeästi ja ne organisaation toimivan johdon olisi hyväksyttävä ne.

Pilvipalvelun tuottajan ja pilvipalvelun asiakkaana toimivan organisaation välisen sopimuksen olisi sisälletävä seuraavat organisaation tietoaineistojen suojaamista ja palveluiden saatavuutta koskevat asiat:

- a) ratkaisut, jotka perustuvat toimialalla tunnustettuihin arkkitehtuuria ja infrastruktuuria koskeviin standardeihin
- b) pilvipalvelun pääsynhallinta, joka täyttää organisaation vaatimukset
- c) haittaohjelmien torjunnan ja niiltä suojautumisen ratkaisujen toteuttaminen
- d) organisaation arkaluonteisten ja henkilötietojen käsittely ja tallennus tapahtuvat hyväksytyissä paikoissa (esim. tietyssä maassa tai tietyllä alueella) tai tietyn lainsäädännön mukaisesti
- e) tuki tilanteisiin, joissa pilvipalvelu ympäristöön kohdistuu tietoturvahäiriö
- f) varmistetaan, että organisaation tietoturvavaatimukset täyttyvät, vaikka pilvipalvelun tuottaminen olisi edelleen ulkoistettu ulkopuoliselle toimittajalle (tai vaihtoehtoisesti pilvipalvelun jatkoulkoistamisen kieläminen)
- g) rikosepäilyn yhteydessä organisaation sähköisten todisteiden keräämisen tukeminen, ottaen huomioon sähköisiä todisteita kansallinen ja kansainvälinen lainsäädäntö
- h) palveluiden tuen ja saatavuuden takaaminen tarpeellisen ajan, kun organisaatio haluaa lopettaa pilvipalvelun käytön
- i) tietoaineistojen ja konfiguraatiotietojen haluttu varmuuskopiointi sekä varmuuskopioiden turvallinen hallinta, mikä perustuu pilvipalvelun asiakkaana toimivan organisaation käyttämän pilvipalvelun tuottajan kyvykkyyksiin

- j) pilvipalvelun asiakkaana toimivan organisaation tietojen, kuten konfiguraatiotiedostojen, lähdekoodien ja tietoaineistojen, luovuttaminen ja palauttaminen, kun niitä pyydetään palvelun hankinnan tai sen päätämisen yhteydessä.

Pilvipalvelun asiakkaana toimivan organisaation olisi selvitettävä, olisiko sopimuksessa velvoitettava pilvipalvelun tuottajia ilmoittamaan etukäteen asiakkaaseen vaikuttavista merkittävistä muutoksista, jotka koskevat palvelun toimittamista organisaatiolle. Tällaisia ovat

- teknisen infrastruktuurin muutokset (esim. siirtäminen, uudelleen konfigurointi tai laitteistojen ja ohjelmistojen muutokset), jotka vaikuttavat tai muuttavat tarjottua pilvipalvelua
- tietojen käsittely tai varastointi uusilla maantieteellisillä alueilla tai lainkäytöalueilla
- pilvipalvelun tuottajien tai muiden alihankkijoiden käyttö (mukaan lukien osapuolten muutokset tai uusien osapuolten käyttö).

Pilvipalvelua käyttävät organisaation olisi pidettävä tiiviisti yhteyttä pilvipalvelujen tuottajiinsa. Tämä yhteydenpito mahdollistaa yhteisen pilvipalvelun tietoturvallisuutta koskevan tietojenvaihdon mukaan lukien tavat, joilla sekä pilvipalvelun tuottajan että pilvipalvelun asiakkaana toimiva organisaatio voivat seurata kutakin palveluominaisuutta ja raportoida sopimukseen sisältyvien sitoumusten täytymättä jäämisistä.

## Lisätiedot

Tässä hallintakeinossa pilvipalvelun turvallisuutta tarkastellaan pilvipalvelun asiakkaan näkökulmasta.

Lisätietoja pilvipalveluista löytyy standardeista ISO/IEC 17788, ISO/IEC 17789 ja ISO/IEC 22123-1. Tarkempia tietoja käytön lopettamisen strategioita tukevasta pilvipalvelun siirrettävyydestä löytyy standardista ISO/IEC 19941. Tarkempia tietoja tietoturvallisuudesta ja julkisista pilvipalveluista löytyy standardista ISO/IEC 27017. Tarkempia tietoja henkilötietojen suojaamisesta henkilötietoja käsittelevissä julkisisissa pilvipalveluissa löytyy standardista ISO/IEC 27018. Lisätietoja pilvipalveluita koskevista toimittajasuheteista löytyy standardista ISO/IEC 27036-4, pilvipalvelusopimuksia ja niiden sisältöjä käsitellään standardisarjassa ISO/IEC 19086, jonka osa ISO/IEC 19086-4 kattaa erityisesti turvallisuuden ja tietosuojan.

## 5.24 Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Hallintotapa #Identiteetti_-ja_käyttövaltuushallinta	#Puolustus

### Hallintakeino

Organisaation olisi suunniteltava ja valmistauduttava tietoturvahäiriöiden hallintaan laativalla tietoturvahäiriöiden hallinnan prosessit, roolit ja vastuu sekä viestimällä niistä.

### Tarkoitus

Varmistetaan, että tietoturvahäiriöihin reagointi on nopeaa, saavuttaa halutut tulokset, on johdonmukaista ja sisältää tietoturvatapahtumista viestinnän.

### Ohjeistus

#### Roolit ja vastuu

Organisaation olisi laadittava tietoturvahäiriöiden asianmukaiset hallintaprosessit. Tietoturvahäiriöiden hallinnan roolit ja vastuu olisi määritettävä, ja niistä olisi viestittävä vaikuttavasti tarvittaville sisäisille ja ulkoisille sidosryhmille.

Seuraavat asiat olisi otettava huomioon:

- a) tietoturvatapahtumien raportoinnin yhtenäisen toimintamallin laatiminen mukaan lukien keihin otetaan yhteyttä tietoturvatapahtumassa (ks. [kohta 6.8](#))
- b) laaditaan tietoturvahäiriöiden hallintaprosessi, jolla organisaatiolle muodostetaan kyky hallita tietoturvahäiriötä mukaan lukien poikkeaman vastatoimien johtaminen, dokumentointi, havaitseminen, seulonta, tärkeyden määritys, analysointi, viestintä ja sidosryhmien koordinointi
- c) tietoturvahäiriön reagointiprosessin laatiminen, mikä tarjoaa organisaatiolle kyyvin arvioida tietoturvahäiriötä, reagoida niihin ja oppia niistä
- d) vain pätevä henkilöstö käsitteli tietoturvahäiriöihin liittyvät asiat organisaatiossa; heille olisi annettava menettelyjä koskeva dokumentaatio sekä säännöllistä koulutusta
- e) laaditaan prosessi tietoturvahäiriöihin reagoivan henkilöstön tarvitsemaan koulutukseen, sertifointeihin ja jatkuvaan ammatilliseen kehittämiseen.

#### Tietoturvahäiriöiden hallinnan menettelyt

Tietoturvahäiriöiden hallinnan tavoitteista olisi sovittava johdon kanssa. Tietoturvahäiriöiden hallinnasta vastaavien henkilöiden olisi myös varmistettava, että he ymmärtävät organisaation prioriteetit tietoturvahäiriöiden käsittelyssä, mukaan lukien mahdollisiin seuraauksiin ja niiden vakavuuksiin perustuvat aikataulut. Häiriötilanteiden hallinnan menettelyt olisi toteutettava siten, että ne täytyvät nämä tavoitteet ja prioriteetit.

Johdon olisi varmistettava, että tietoturvahäiriöiden hallintasuunnitelma on laadittu siten, että siinä tarkastellaan eri skenaarioita ja siihen on laadittu ja toteutettu seuraavia toimintoja koskevat menettelyt:

- a) tietoturvatapahtumien arvointi suhteessa tietoturvahäiriön vakavuuden määrittäviin kriteereihin
- b) tietoturvatapahtumien ja -häiriöiden seuranta (ks. [kohdat 8.15 ja 8.16](#)), havaitseminen (ks. [kohta 8.16](#)), luokittelu (ks. [kohta 5.25](#)), analysointi ja raportointi (ks. [kohta 6.8](#)) (joko ihmisen tekemänä tai koneellisesti)
- c) tietoturvahäiriöiden hallinta niiden päätökseen asti, mukaan lukien vastatoimien aloittaminen ja niiden eskalointi (ks. [kohta 5.26](#)) häiriön vakavuuden mukaan, jatkuvuussuunnitelmiin ja muiden kriisinhallinnan toimien mahdollinen käynnistäminen, hallittu palautuminen häiriöstä ja viestintä sisäisten ja ulkoisten sidosryhmien kanssa
- d) toimenpiteiden koordinointi sisäisten ja ulkoisten sidosryhmien, kuten viranomaisten, ja ulkoisten eturyhmien ja verkon keskusteluryhmien, toimittajien ja asiakkaiden (ks. [kohdat 5.5 ja 5.6](#)) kanssa
- e) häiriönhallinnassa tehtyjen toimenpiteiden ja tapahtumien kirjaaminen
- f) kerätyn todistusaineiston käsittely (ks. [kohta 5.28](#))
- g) häiriön perimmäisten syiden analysointi (juurianalyysi) ja häiriön jälkeinen arvointi
- h) opittujen asioiden tunnistaminen sekä mahdolliset tietoturvahäiriöiden hallinnan menettelyihin tai tietoturvallisuuden hallintakeinoihin tarvittavat parannukset.

#### Ilmoitusmenettelyt

Ilmoitusmenettelyihin olisi sisällyttäävä

- a) tietoturvatapahtuman sattuessa tehtäväät toimenpiteet (esim. kaikkien tärkeiden yksityiskohtien välitön kirjaaminen, kuten tapahtunut toimintahäiriö, näytöllä olevat viestit, asian välitön ilmoittaminen yhteyshenkilölle ja vain koordinoitujen toimenpiteiden tekeminen)
- b) häiriökaavakkeiden käyttö, jotta henkilöstö osaa ilmoittaa tärkeät tiedot tietoturvahäiriöistä
- c) palautteen käsittelymenettely, jolla varmistetaan, että tietoturvatapahtumista ilmoittaneille viestitään, mahdollisuksien rajoissa, tuloksista asian käsittelyn ja sulkemisen jälkeen

d) häiriöraporttien luominen.

Tietoturvahäiriön aiheuttamien toimenpiteiden ja niiden raportoinnissa tärkeimmille sidosryhmille olisi otettava huomioon ulkoiset vaatimukset (esim. tietomurrosta viranomaisille ilmoittamista koskevat vaatimukset).

#### Lisätiedot

Tietoturvahäiriöt voivat ylittää sekä organisaation rajat että kansalliset rajat. Tällaisiin tapauksiin reagoimisessa on hyötyä koordinoida toimenpiteet ja jakaa häiriötä koskevaa tietoa ulkopuolisten organisaatioiden kanssa tarpeen mukaan.

Lisähohjeistusta tietoturvahäiriöiden hallinnasta esitetään standardisarjassa ISO/IEC 27035.

### 5.25 Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturvatapahtumien_hallinta	#Puolustus

#### Hallintakeino

Organisaation olisi arvioitava tietoturvatapahtumat ja päättää, luokitellaanko ne tietoturvahäiriöiksi.

#### Tarkoitus

Varmistetaan tietoturvatapahtumien toimiva luokittelija ja tärkeyden määritys.

#### Ohjeistus

Tietoturvahäiriöiden luokittelun ja tärkeyden määrittämisen menettelystä olisi sovittava, jotta häiriön seuraukset ja tärkeys voidaan arvioda oikein. Menettelyn olisi sisällettävä tapahtumien tietoturvahäiriöiksi luokittelua koskevat kriteerit. Toimintaa johtavan olisi arvioitava kukaan tietoturvatapahtuma sovitun menettelyn mukaisesti.

Tietoturvahäiriöiden koordinoinnista ja niihin reagoinnista vastaavan henkilöstön olisi arvioitava tietoturvatapahtumat ja tehtävä niihin liittyvät päätökset.

Arvioinnin ja päätöksenteon tulokset olisi kirjattava yksityiskohtaisesti, jotta voidaan varautua tuleviin häiriöihin ja jotta voidaan varmistua, että meneillään olevassa häiriötilanteessa on toimittu oikein.

#### Lisätiedot

Lisätietoja häiriötilanteiden hallinnasta löytyy standardisarjasta ISO/IEC 27035.

### 5.26 Tietoturvahäiriöihin reagointi (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Tietoturvatapahtumien_hallinta	#Puolustus

#### Hallintakeino

Tietoturvahäiriöihin olisi reagoitava dokumentoitujen menettelytapojen mukaisesti.

#### Tarkoitus

Varmistetaan tehokas ja vaikuttava reagointi tietoturvahäiriöihin.

## Ohjeistus

Organisaation olisi laadittava menettelyt tietoturvahäiriöihin reagoimiseen ja viestittävä niistä kaikille tarpeellisille sidosryhmille.

Tietoturvahäiriöihin reagointiin olisi oltava sitä varten perustettu ryhmä, jolla on tarpeellinen osaaminen (ks. [kohta 5.24](#)).

Häiriön käynnistämien vastatoimien olisi sisällettävä seuraavat asiat:

- a) häiriölle altistuneiden järjestelmien eristäminen, jos häiriön seuraukset voivat levitä
- b) todisteiden kokoaminen (ks. [kohta 5.28](#)) mahdollisimman pian tapahtuman jälkeen
- c) eskalointi, mukaan lukien kriisinhallinnan keinot sekä liiketoiminnan jatkuvuussuunnitelmien mahdollinen käynnistäminen (ks. [kohdat 5.29](#) ja [5.30](#))
- d) varmistetaan, että kaikki asiaan liittyvät vastetoimenpiteet on kirjattu oikein myöhempää analysointia varten
- e) tietoturvahäiriön tai sitä koskevien yksityiskohtien viestiminen kaikille sisäisille ja ulkoisille sidosryhmille tarve tietää -periaatteella (*need-to-know*)
- f) koordinointi sisäisten ja ulkoisten sidosryhmien, kuten viranomaisten, ja ulkoisten sidosryhmien ja intressiryhmien, toimittajien ja asiakkaiden kanssa, jolla pyritään parantamaan vastatoimien vaikuttavuutta ja pitämään muihin organisaatioihin kohdistuvat seuraukset mahdollisimman vähäisinä
- g) kun häiriö on hoidettu onnistuneesti, selkeä dokumentoitu päätös siitä, että häiriönhallinnan toimet voidaan lopettaa
- h) tietorikostutkinta tarvittaessa (ks. [kohta 5.28](#))
- i) häiriön jälkeisen analyysin tekeminen, jotta tunnistetaan sen syntymisen perimmäiset syyt; varmistetaan, että syy dokumentoidaan ja siitä viestitään määriteltyjen menettelyjen mukaisesti (ks. [kohta 5.27](#))
- j) tietoturvallisuuteen liittyvien haavoittuvuuksien ja heikkouksien tunnistaminen ja hallinta, erityisesti niiden, jotka liittyvät tietoturvallisuuden hallintakeinoihin, jotka ovat aiheuttaneet häiriön, edesauttaneet sitä tai epäonnistuneet sen estämisessä.

## Lisätiedot

Lisätietoja häiriötilanteiden hallinnasta löytyy standardisarjasta ISO/IEC 27035.

### 5.27 Tietoturvahäiriöstä oppiminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietoturvatapahtumien_hallinta	#Puolustus

## Hallintakeino

Tietoturvahäiriöstä saatua tietämystä olisi hyödynnettävä tietoturvallisuuden hallintakeinojen vahvistamisessa ja parantamisessa.

## Tarkoitus

Vähennetään tulevien häiriöiden todennäköisyyttä tai seuraauksia.

## Ohjeistus

Organisaation olisi laadittava menettelyt, jolla määritellään ja seurataan tietoturvahäiriöiden tyyppejä ja määriä sekä niistä aiheutuvia kustannuksia.

Tietoturvahäiriöiden arvioinnista saatua tietoa olisi käytettävä apuna

- häiriötilanteiden hallintasuunnitelman parantamiseen, mukaan lukien skenaariot ja toimenpiteet (ks. [kohta 5.24](#))
- toistuvien tai vaikutukseltaan merkittävien häiriöiden ja niiden syiden tunnistamisessa, jotta voidaan päävittää organisaation tietoturvariskien arvointi sekä määrittää ja toteuttaa tarvittavat uudet hallintakeinot, joilla pienennetään vastaavien tulevien häiriöiden todennäköisyyttä tai seurauskia; näitä ovat esim. häiriöiden tyyppejä, määriä ja kustannusvaikutuksia koskevien tietojen kerääminen, muuttaminen analysoitavaan muotoon ja seuranta
- käyttäjien tietoisuuden ja koulutuksen parantamiseen (ks. [kohta 6.3](#)) antamalla esimerkkejä siitä, mitä voi tapahtua, miten kyseisiin tilanteisiin reagoidaan, ja kuinka niitä voidaan myöhemmin välttää.

## Lisätiedot

Lisätietoja löytyy standardisarjasta ISO/IEC 27035.

## 5.28 Todisteiden kerääminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturvataapau-tien_hallinta	#Puolustus

### Hallintakeino

Organisaation olisi laadittava ja toteutettava menettelyt tietoturvataapautumiin liittyvien todisteiden yksilöimiseen, keräämiseen, muuhun hankkimiseen ja säilyttämiseen.

### Tarkoitus

Varmistetaan, että tietoturvataapautumiin liittyvien kurinpidollisia tai juridisia toimenpiteitä varten kerättävien todistusaineistojen hallinta on johdonmukaista ja vaikuttavaa.

### Ohjeistus

Olisi kehitettävä sisäiset menettelyt, joita noudatetaan, kun käsitellään tietoturvataapautumiin liittyvää todistusaineistoa kuripitotoimenpiteitä tai juridisia toimenpiteitä varten. Eri lainsäädäntöalueiden vaatimukset olisi otettava huomioon, jotta todisteita voidaan käyttää mahdollisimman paljon oikeusprosesseissa kaikilla lainsäädäntöalueilla, joilla niillä on merkitystä.

Näiden todisteiden hallintaa koskevien menettelyjen olisi katettava todisteiden yksilöinti-, keräämis-, hankinta- ja säilyttämisohjeet erilaisten tallennusvälineiden, laitteiden ja laitteiden tilan (päällä vai pois päältä) mukaisesti. Todistusaineisto täytyy kerätä tavalla, joka tekee sen käytöstä hyväksyttävää kansallisessa tuomioistuimissa tai muissa toimielimissä. Olisi kyettävä osoittamaan, että

- tallenteista ei ole jätetty mitään pois, eikä niitä ole muutettu luvattomasti mitenkään
- sähköisten todisteiden kopioiden voidaan todistaa olevan identtisiä alkuperäisten kanssa
- mikä tahansa tietojärjestelmä, josta todistusaineistoa kerättiin, toimi oikein todisteiden keräämishetkellä.

Henkilöstön ja työkalujen sertifiointeja tai muita pätevöittämisiä olisi yritettävä saada, jotta kerätty näyttö on todistusvoimaista.

Sähköistä todistusaineistoa voi syntyä eri organisaatioiden tai lainkäyttöalueiden alueella. Näissä tapauksissa olisi varmistettava, että organisaatiolla on laillinen oikeus kerätä tarvittavat tiedot käytettäväksi sähköisenä todistusaineistonä oikeudenkäynnissä.

### Lisätiedot

Kun tietoturvatapahtuma havaitaan, ei välttämättä ole ilmeistä, johtaako se oikeustoimiin. Tämän vuoksi on olemassa vaara, että tarvittava todistusaineisto tuhotaan tahallaan tai vahingossa, ennen kuin tapahtuman vakavuus ehditään havaita. On suositeltavaa ottaa juridisia asiantuntijoita tai viranomaisia mukaan mahdollisiin oikeustoimiin jo aikaisessa vaiheessa ja pyytää neuvoja tarvittavan todistusaineiston keräämiseen.

Standardissa ISO/IEC 27037 annetaan määritelmät ja ohjeet sähköisen todistusaineiston yksilöintiin, keräämiseen, muuhun hankintaan ja säilyttämiseen.

Standardisarja ISO/IEC 27050 käsittelee sähköistä tietojenkeruuta, mikä sisältää sähköisesti tallennettujen tietojen käsittelyn todistusaineistona.

## 5.29 Tietoturvallisuus häiriötilanteessa [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus #Vaste	#Jatkuvuus	#Suojaaminen
#Korjaava	#Eheys #Saatavuus			#Kriisinkestävyys

### Hallintakeino

Organisaation olisi suunniteltava, miten se ylläpitää riittävää tietoturvallisuustasoa häiriön aikana.

### Tarkoitus

Suojataan tietoja ja niihin liittyviä omaisuuseriä häiriön aikana.

### Ohjeistus

Organisaation olisi määritettävä vaatimukset, jotka koskevat tietoturvallisuuden hallintakeinojen mukauttamista häiriöiden aikana. Tietoturvavaatimusten olisi sisällyttävä liiketoiminnan jatkuvuuden hallintaprosesseihin.

Olisi laadittava, toteutettava, testattava, katselmoitava ja arvioitava suunnitelmat, joiden mukaisesti ylläpidetään tai palautetaan kriittisten liiketoimintaprosessien tietojen turvallisuus katkoksen tai vikaantumisen jälkeen. Tietojen turvallisuus olisi palautettava vaaditulle tasolle vaaditussa ajassa.

Organisaation olisi toteutettava ja ylläpidettävä

- tietoturvallisuuden hallintakeinoja, tukijärjestelmiä ja -työkaluja osana liiketoiminnan jatkuvuus- ja tieto- ja viestintätekniisen jatkuvuussuunnittelmia
- prosesseja, joilla ylläpidetään olemassa olevia tietoturvallisuuden hallintakeinoja häiriötilanteissa
- korvaavat hallintakeinot niille tietoturvallisuuden hallintakeinoille, joita ei voida pitää toiminnassa häiriötilanteissa.

### Lisätiedot

Liiketoiminnan ja tieto- ja viestintätekniisen jatkuvuuden suunnittelussa voi olla tarpeen mukauttaa tietoturvavaatimuksia suhteessa normaalitoimintaan. Tämä riippuu häiriötilanteen tyypistä. Osana liiketoiminnan jatkuvuuden hallinnassa ja häiriöiden vaikutusarvioinnissa (*Business Impact Analysis, BIA*) olisi arvioitava tietojen luottamuksellisuuden ja eheyden vaarantumisen vaikutukset sekä otettava huomioon, millainen saatavuus tiedoille on tarpeen häiriöiden aikana.

Lisätietoa liiketoiminnan jatkuvuuden hallintajärjestelmistä löytyy standardeista ISO 22301 ja ISO 22313. Yksityiskohtaisempaa ohjeistusta liiketoiminnan vaikutusanalyysista löytyy teknisestä spesifikaatiosta ISO/TS 22317.

### 5.30 Tieto- ja viestintätekniikan valmies liiketoiminnan jatkuvuussuunnittelussa (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Korjaava	#Saatavuus	#Vaste	#Jatkuvuus	#Krisinkestävyys

#### Hallintakeino

Tieto- ja viestintätekniikan valmies olisi suunniteltava, toteutettava, ylläpidettävä ja testattava liiketoiminnan jatkuvuustavoitteiden ja tieto- ja viestintätekniikalle asetettujen jatkuvuusvaatimusten perusteella.

#### Tarkoitus

Varmistetaan organisaation tietojen ja niihin liittyvien omaisuuserien saatavuus häiriötilanteen aikana.

#### Ohjeistus

Liiketoiminnan jatkuvuutta koskeva tieto- ja viestintätekniikan valmies on liiketoiminnan jatkuvuuden hallinnan ja tietoturvallisuuden hallinnan tärkeä osa, koska sen avulla voidaan varmistaa, että organisaation tavoitteet voidaan saavuttaa myös häiriötilanteen aikana.

Tieto- ja viestintätekniistä jatkuvuutta koskevat vaatimukset syntyvät liiketoiminnan vaikutusanalyysin (BIA) tuloksena. Liiketoiminnan vaikutusanalyysiprosessissa olisi käytettävä vaikutustyyppejä ja kriteereitä sen arviointiin, millaisia vaikutoksia tuotteita ja palveluita toimittavien liiketoimintojen häiriöillä on, etenkin häiriön jatkuessa. Vaikutuksen arviodun laajuuden ja keston avulla olisi päättää tärkeimmät toiminnot, joille olisi määriteltävä palautumisaikataavoite (*Recovery Time Objective, RTO*). Liiketoiminnan vaikutusanalyysillä olisi seuraavaksi määritettävä, mitä resursseja tarvitaan näiden toimintojen tueksi. Myös näille resursseille olisi määriteltävä palautumisaikataavoite. Tieto- ja viestintätekniisten palveluiden olisi sisällytettävä näihin resursseihin.

Tieto- ja viestintätekniiset palvelut kattavat liiketoiminnan vaikutusanalyysia voidaan jatkaa ja määritellä tieto- ja viestintätekniisten järjestelmien suorituskyky- ja kapasiteettivaatimukset sekä palautustavoitteet (*Recovery Point Objective, RPO*) niille tiedoille, joita käytetään toimintaa jatketaan häiriötilanteessa.

Tieto- ja viestintätekniiset palvelut kattavat liiketoiminnan vaikutusanalyysin ja riskien arvioinnin tuotosten perusteella organisaation olisi tunnistettava ja valittava tieto- ja viestintätekniiset jatkuvuusstrategiat, joissa otetaan huomioon eri vaihtoehtoja häiriöön varautumiseen, häiriön hallintaan ja häiriöstä toipumiseen. Liiketoiminnan jatkuvuusstrategiat voivat koostua useammasta vaihtoehdosta. Strategioiden perusteella olisi laadittava, toteutettava ja testattava suunnitelmat, joilla tärkeiden liiketoimintaprosessien häiriön tai keskeytyksen aikana kyötään ylläpitämään ennalta sovittu saatavuus tieto- ja viestintäteknisille palveluille ja joilla häiriön jälkeen kyötään palauttamaan tieto- ja viestintätekniisten palveluiden saatavuustaso ennalta sovitussa ajassa.

Organisaation olisi varmistettava, että

- on asetettu organisaatio, joka valmistautuu häiriöihin, lieventää niitä ja vastaa niihin käyttämällä henkilöstöä, jolla tarpeelliset vastuut, valtuudet ja pätevyys
- tieto- ja viestintätekniiset jatkuvuussuunnitelmat, joissa on mukana häiriöön reagointi, ja joissa kerrotaan, miten organisaatio aikoo hallita tieto- ja viestintätekniisiä häiriötilanteita,
  - arvioidaan säännöllisesti harjoituksilla ja testaamalla
  - ovat johdon hyväksymiä

- c) tieto- ja viestintätekniset jatkuvuussuunnitelmat sisältävät vähintään seuraavat tieto- ja viestintätekniseen jatkuvuuteen liittyvät tiedot:
- 1) suorituskyky- ja kapasiteettimäärittelyt, jotka täyttävät liiketoiminnan vaikutusanalyysissä asetetut liiketoiminnan jatkuvuutta koskevat vaatimukset ja tavoitteet
  - 2) kunkin kriittisen tieto- ja viestintäteknisen palvelun palautumisaikatavoite sekä menettelyt näiden osien palauttamiseen
  - 3) kunkin kriittisen tieto- ja viestintäteknisen palvelun palautustavoite määriteltyynä tietojen laajuutena ja palautumistoimet niille.

### Lisätiedot

Tieto- ja viestintäteknisen jatkuvuuden hallinta on keskeinen osa saatavuutta koskevia liiketoiminnan jatkuvuuden vaatimuksia, jotta kyötään

- a) reagoimaan ja toipumaan tieto- ja viestintäteknisiin palveluihin kohdistuvista häiriöistä niiden syystä riippumatta
- b) varmistamaan, että tarvittavat tieto- ja viestintätekniset palvelut tukevat tärkeimpien toimintojen jatkuvuutta
- c) reagoimaan ennen kuin tieto- ja viestintäteknisiin palveluihin on kohdistunut varsinaisen toimintaa haittaava häiriö ja kun havaitaan poikkeama, joka voi johtaa tieto- ja viestintäteknisiin palveluihin kohdistuvaan häiriötilanteeseen.

Lisätietoja liiketoiminnan jatkuvuuteen liittyvästä tieto- ja viestintäteknisestä valmiudesta löytyy standardista ISO/IEC 27031.

Lisätietoa liiketoiminnan jatkuvuuden hallintajärjestelmistä löytyy standardeista ISO 22301 ja ISO 22313.

Lisätietoja liiketoiminnan vaikutusanalyysista löytyy teknisestä spesifikaatiosta ISO/TS 22317.

### 5.31 Lainsääädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Lait_ja_vaatimusten-mukaisuus	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

#### Hallintakeino

Lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin perustuvat tietoturvallisuuden kannalta tärkeät vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten olisi yksilöitvä, dokumentoitava ja pidettävä ajantasalla.

#### Tarkoitus

Varmistetaan, että noudatetaan lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyviä vaatimuksia, jotka liittyvät tietoturvallisuuteen.

## Ohjeistus

### Yleistä

Ulkoiset vaatimukset, kuten lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset, olisi otettava huomioon, kun

- a) laaditaan tietoturvapolitiikkoja ja -menettelyjä
- b) suunnitellaan, toteutetaan tai muutetaan tietoturvallisuuden hallintakeinoja
- c) luokitellaan tietoja ja niihin liittyviä omaisuuseriä osana prosessia, jossa asetetaan tietoturvavaatimukset sisäisiä tarpeita varten tai toimittajasopimuksia koskien
- d) tehdään tietoturvariskien arvointeja ja määritetään tietoturvariskien käsitteilytoimiintoja
- e) määritetään tietoturvallisuuteen liittyviä prosesseja sekä niihin liittyviä rooleja ja vastuita
- f) määritetään organisaation kannalta tärkeät toimittajaa koskevat sopimuselliset vaatimukset sekä miten laajasti tuotteita ja palveluita hankitaan.

### Lainsääädäntö ja viranomaismääräykset

Organisaation olisi

- a) yksilöitää kaikki lait ja viranomaismääräykset, jotka ovat tärkeitä organisaation tietoturvan kannalta, jotta se on tietoinen liiketoimintaan kohdistuvista juridisista velvoitteista
- b) otettava huomioon vaatimustenmukaisuus kaikissa niissä valtioissa, joissa organisaatio
  - harjoittaa liiketoimintaa
  - käyttää tuotteita ja palveluita, jotka toimitetaan sellaisista maista, joiden lainsääädäntö ja viranomaismääräykset voivat vaikuttaa organisaatioon
  - siirtää tietoja eri lainsääädäntöalueiden rajojen yli, jos lait ja viranomaismääräykset voivat vaikuttaa organisaatioon
- c) katselmoitava sitä koskevat lait ja viranomaismääräykset säännöllisesti, jotta se pystyy pysymään ajan tasalla lainsääädännön muutoksista ja uudesta lainsääädännöstä
- d) määriteltää ja dokumentoitava näiden vaatimusten täyttämiseen tähtäävät prosessit ja vastuut.

### Salaus

Salaukseen liittyy usein nimenomaisia juridisia vaatimuksia. Seuraavia asioita koskevien sopimusten, lakien ja viranomaismääräysten asettamat vaatimukset olisi otettava huomioon:

- a) salaukseen käytettävien tietokoneohjelmien ja -laitteistojen tuonti- ja vientirajoitukset
- b) tuonti- ja vientirajoitukset tietokoneohjelmille ja -laitteistoille, joihin voidaan lisätä salaustoimintoja
- c) salaustekniikan käytön rajoitukset
- d) eri maiden viranomaisten keinot salatun tiedon saamiseen joko lainsääädännön tai muiden hallinnollisten keinojen nojalla
- e) sähköisten allekirjoitusten, sinettien ja sertifikaattien kelpoisuus.

Juridisen avun käyttöä suositellaan, kun varmistetaan vaatimustenmukaisuus lakiens ja viranomaismääräysten kanssa etenkin, kun kyse on salatun tiedon tai salaustyökalujen siirtämisestä lainkäyttöalueiden rajojen ylitse.

## Sopimukset

Tietoturvallisuuteen liittyvien sopimusvaatimusten olisi sisällettävä ne, jotka on mainittu

- a) asiakkaiden kanssa solmituissa sopimuksissa
- b) toimittajien kanssa solmituissa sopimuksissa (ks. [kohta 5.20](#))
- c) vakuutussopimuksissa.

## Lisätiedot

Ei lisätietoja.

## 5.32 Immateriaalioikeudet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Lait_ ja _vaatimustenmukaisuus	#Hallintotapa_ ja _ekosysteemi

### Hallintakeino

Organisaation olisi toteutettava asianmukaiset menettelyt immateriaalioikeuksien suojaamiseen.

### Tarkoitus

Varmistetaan, että immateriaalioikeuksiin ja muilla oikeuksilla suojattujen tuotteiden (kuten suljetun lähdekoodin ohjelmien) käyttöön liittyviä lakien, asetusten, viranomaismääräysten ja sopimusten asettamia vaatimuksia noudatetaan.

### Ohjeistus

Kun suojataan immateriaalioikeuksien alaiseksi katsottua materiaalia, olisi otettava huomioon seuraavat ohjeet:

- a) immateriaalioikeuksien suojaamista koskevien toimintaperiaatteiden määrittely ja niistä viestiminen
- b) immateriaalioikeuksia koskeva vaatimustenmukaisuutta koskevien menettelyjen julkaiseminen; näissä määritellään ohjelmistojen ja tietotuotteiden vaatimustenmukainen käyttö
- c) ohjelmistojen hankkiminen vain tunnetuista ja hyvämaineisista lähteistä, jotta varmistetaan tekijänoikeuksien toteutuminen
- d) omaisuutta koskevien rekistereiden ylläpitäminen ja kaikkien sellaisten omaisuuserien yksilöiminen, joihin kohdistuu immateriaalioikeuksien suojausvaatimuksia
- e) laillisen saannon osoittavien asiakirjojen, kuten kuittien ylläpitäminen lisenssien, käyttöoppaiden jne. omistajuudesta
- f) varmistetaan, että lisenssin sallima käyttäjien tai resurssien (esim. keskusyksiköiden) käyttäjämäärää ei ylitetä
- g) varmistetaan katselmoinneilla, että ainoastaan sallittuja ohjelmistoja ja lisensoituja tuotteita asennetaan
- h) lisenssiehtojen täytymisen ylläpitoon liittyvien menettelyjen laatiminen
- i) ohjelmiston käytöstä poistamiseen tai siirtämiseen liittyvien menettelyjen laatiminen
- j) julkisista verkoista ja ulkoisista lähteistä hankittuihin ohjelmistoihin ja tietoihin liittyvien rajoitusten ja ehtojen noudattaminen

- k) varmistetaan, että kaupallisia tallenteita (video- tai äänitallenteita) ei kopioida tai muuteta toiseen muotoon eikä niistä tehdä poimintoja muuten kuin tekijänoikeuslain tai asiaankuuluvan lisenssin sallimalla tavalla
- l) varmistetaan, että standardeja (esim. kansainvälisiä ISO/IEC-standardeja), kirjoja, artikkeleita, raportteja tai muita asiakirjoja ei kopioida kokonaan eikä osittain muuten kuin tekijänoikeuslain tai asiaankuuluvan lisenssin sallimalla tavalla.

## Lisätiedot

Immateriaalioikeudet kattavat ohjelmistojen ja asiakirjojen tekijänoikeudet, tuotteen muotoiluun liittyvät oikeudet, tavaramerkit, patentit ja lisenssit.

Omistusoikeuden suojaamat ohjelmistotuotteet toimitetaan tavallisesti lisenssisopimuksilla. Sopimus määrittelee lisenssiehdot, jotka esimerkiksi rajoittavat tuotteiden käytön määriteltyihin koneisiin tai rajoittavat kopioinnin varmuuskopioiden luontiin. Lisätietoja tietoteknisen omaisuuden hallinnasta löytyy standardisarjasta ISO/IEC 19770.

Tietoaineisto voidaan hankkia ulkoisista lähteistä. Tällainen tietoaineisto hankitaan yleensä tiedonjakoa koskevien sopimusten tai vastaavien juridisten mekanismien avulla. Tällaisissa tiedonjakoa koskevissa sopimuksissa olisi kerrottava selkeästi, miten hankittua tietoa on sallittua käsitellä. Myös tietojen alkuperä olisi syytä ilmoittaa selkeästi. Lisätietoja tiedonjakoa koskevista sopimuksista löytyy standardista ISO/IEC 23751.

Lakien, asetusten, viranomaismääräysten ja sopimusten vaatimukset voivat rajoittaa suljetun lähdekoodin ohjelmistojen kopointia. Näissä voidaan erityisesti määräätä, että ainoastaan organisaation itse kehittämää tai lisenssin antajan organisaatiolle lisensioimaa tai muutoin luovuttamaa materiaalia saadaan käyttää. Tekijänoikeuksien loukkaaminen voi johtaa oikeustoimiin, kuten sakkoihin tai rikosoikeudelliseen vastuuseen.

Sen lisäksi, että hallitaan organisaation tarvetta noudattaa kolmansien osapuolten immateriaalioikeuksia koskevia velvoitteita, olisi hallittava myös riskiä, että oma henkilöstö tai kolmas osapuoli rikkoo organisaation omia immateriaalioikeuksia.

## 5.33 Tallenteiden suojaaminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Lait_ja_vaatimustenmukaisuus #Omaisuudenhallinta #Tietojen_suojaaminen	#Puolustus

### Hallintakeino

Tallenteet olisi suojahtava katoamiselta, tuhoutumiselta, väärrentämiseltä, luvattomalta käytöltä ja luvattomalta levittämiseltä.

### Tarkoitus

Varmistetaan, että tallenteiden suojaamista ja saatavuutta koskevia lakienv, asetusten, viranomaisten ja sopimusten asettamia vaatimuksia sekä niihin liittyviä yleisiä ja yhteiskunnan odotuksia noudatetaan.

### Ohjeistus

Organisaation olisi tehtävä seuraavat toimenpiteet, jotta se kykenee suojaamaan tallenteidensa aitoussa, luotettavuutta, eheyttä ja käytettävyyttä, kun organisaation liiketoimintaympäristö ja niitä koskevat vaatimukset muuttuvat:

- a) Organisaation olisi julkaistava tallenteiden säilyttämistä ja käsittelyä koskevaa hallussapitoketjua ja tallenteiden hävittämistä koskevat ohjeet, joihin sisältyy tallenteiden luvattoman muuttamisen

estäminen. Näiden ohjeiden olisi oltava linjassa organisaation tallenteiden hallintaa koskevien kohdennettujen toimintaperiaatteiden ja muiden tallenteita koskevien vaatimusten kanssa.

- b) Organisaation olisi laadittava arkistoitinsiunnitelma, jossa yksilöidään arkistoitavat tallenteet ja niiden säilytysaika.

Tallennus- ja käsittelyjärjestelmän olisi varmistettava, että tallenteet ja niiden säilytysjaksojen pituus määritellään ottamalla huomioon sekä kansalliset tai alueelliset lait ja viranomaismääräykset että yleiset ja yhteiskunnan odotukset. Järjestelmän olisi sallittava tallenteiden hävittäminen säilytysajan umpeuduttua, jos organisaatio ei enää tarvitse niitä.

Kun päätetään, miten organisaation tallenteita suojaan, olisi otettava huomioon tallenteiden sisältämien tietojen luokitus organisaation käytämässä tietojen luokittelijärjestelmässä. Tallenteet olisi luokiteltava eri tallennetyyppiin (esim. kirjanpidon tallenteisiin, sopimuksiin liittyviin tallenteisiin, henkilöstön tietojen tallenteisiin ja juridisiiin tallenteisiin). Kullekin olisi yksityiskohtaisesti määriteltävä säilytysaika ja säilytykseen sallittu tallennusväline, joka voi olla joko fyysinen tai sähköinen.

Aineiston tallennusmenetelmät olisi valittava siten, että tarvittavat tallenteet voidaan hakea kohtuullisessa ajassa ja sopivassa muodossa.

Mikäli tallentamiseen valitaan sähköinen tietoväline, tallenteiden käyttömahdollisuudet (sekä tallennusvälineen että formaatin luettavuus) olisi varmistettava koko säilytysjakson ajaksi luomalla menettelyohjeet, joilla estetään teknologian myöhemmästä kehityksestä johtuva tiedon häviäminen. Tähän liittyvät salausavaimet ja salattuihin arkistoihin tai digitaalisiin allekirjoituksiin liittyvät ohjelmat olisi myös säilytettävä, jotta mahdollistetaan tallenteiden avaaminen koko niiden säilytysajan (ks. [kohta 8.24](#)).

Tallennus- ja käsittelymenettelyjä olisi toteutettava tallennusvälineen valmistajan suositusten mukaisesti. Tallenteiden säilytykseen käytettyjen tietovälineiden mahdollinen rappeutuminen olisi otettava huomioon.

## Lisätiedot

Tallenteissa dokumentoidaan yksittäiset tapahtumat tai transaktiot tai ne voivat muodostaa koosteita, jotka on suunniteltu dokumentoimaan työprosessit tai -toiminnot. Ne ovat todisteita sekä liiketoiminnasta että tieto-omaisuudesta. Mitä tahansa tietojoukkoa voidaan käsitellä tallenteena riippumatta sen rakenteesta tai muodosta. Tällaisia ovat asiakirjat, tietojoukko tai muun tyyppinen sähköinen tai analoginen tieto, joka on luotu ja kerätty osana liiketoimintaa ja jota hallitaan osana sitä.

Tallenteiden hallinnassa metadata on tietoa, joka kuvilee tallenteiden asiayhteyden, sisällön ja rakenteen sekä niiden hallinnan elinkaaren aikana. Metadata on tärkeä osa mitä tahansa tallennetta.

Jotain tallenteita voi olla syytä säilyttää erityisen turvallisesti laki, asetusten, viranomaisten ja sopimusten vaatimusten perusteella samoin kuin liiketoimien tukemista varten. Kansallinen lainsäädäntö ja viranomaisten määräykset voivat asettaa tietojen säilyttämisen määräajan sekä säilytettävien tietojen sisällön. Lisätietoja tallenteiden hallinnasta esitetään standardissa ISO 15489.

## 5.34 Tietosuoja ja henkilötietojen suojaaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietojen_suojaaminen #Lait_ja_vaatimustenmu-kaisuus	#Suojaaminen

### Hallintakeino

Organisaation olisi tunnistettava ja täytettävä vaatimukset, jotka koskevat tietosuojan ylläpitämistä ja henkilötietojen suojaamista, sisältäen sovellettavat lait ja viranomaismääräykset ja sopimusvaatimukset.

### Tarkoitus

Varmistetaan, että noudatetaan lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyviä vaatimuksia, jotka liittyvät henkilötietojen suojaamisen tietoturvanäkökohtiin.

## Ohjeistus

Organisaation olisi laadittava tietosuoja ja henkilötietojen suojaamista koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille tärkeimmille sidosryhmiille.

Organisaation olisi kehitettävä ja toteutettava menettelyt tietosuojan ylläpitämiseen ja henkilötietojen suojaamiseen. Nämä toimintaperiaatteet olisi viestittävä kaikille tärkeimmille sidosryhmiille, jotka ovat tekemisissä henkilötietojen käsittelyn kanssa.

Näiden toimintaperiaatteiden ja kaikkien tietosuojan ylläpitämistä ja henkilötietojen suojaamista koskevien lakiens ja viranomaisten määräysten noudattaminen vaatii asian hoitamiseksi määriteltyjä rooleja, vastuita ja hallintakeinoja. Usein se saavutetaan parhaiten nimittämällä vastuuhenkilö, kuten tietosuojavastaava, jonka olisi annettava opastusta henkilöstölle, palveluntuottajille ja muille sidosryhmiille näiden henkilökohtaisista velvollisuksista ja noudatettavista käsitteilytavoista.

Henkilötietojen käsitteilyä koskeva vastuu olisi varmistettava ottamalla huomioon lait ja viranomaismääräykset.

Henkilötietojen suojaamista varten olisi otettava käyttöön tarpeelliset tekniset ja organisaatioon liittyvät toimenpiteet.

## Lisätiedot

Monessa maassa on säädetty lakeja, jotka edellyttävät hallintakeinojen käyttöönottoa, kun kerätään, käsitellään, siirretään tai poistetaan henkilötietoja. Kansallisesta lainsäädännöstä riippuen tällaiset hallintakeinot voivat lisätä henkilötietoja keräävien, käsittelevien ja välittävien henkilöiden velvoitteita ja myös rajoittaa henkilötietojen siirtoa maasta toiseen.

Standardissa ISO/IEC 29100 esitetään ylätason ohjeet henkilötietojen suojaamiseen tieto- ja viestintätekniikissa järjestelmissä. Lisätietoja henkilötietojen hallintajärjestelmistä löytyy standardista ISO/IEC 27701. Tarkempia tietoja henkilötietojen suojaamisesta henkilötietoja käsittelevissä julkisissa pilvipalveluissa löytyy standardista ISO/IEC 27018.

Standardissa ISO/IEC 29134 annetaan tietosuojavaikutusten arviointia (PIA) sekä tietosuojavaikutusten arviointiraportin rakennetta ja sisältöä koskevia ohjeita. Standardiin ISO/IEC 27005 verrattuna siinä painotetaan enemmän henkilötietojen käsitteilyä ja kyseisiä henkilötietoja käsitteleviä organisaatioita. Tästä voi olla apua tietosuojaan liittyvien riskien tunnistamisessa sekä näiden riskien mahdollisessa lieventämisessä hyväksyttäville tasolle.

## 5.35 Tietoturvallisuuden riippumaton katselointi (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ecosysteemi

## Hallintakeino

Organisaation tietoturvallisuuden johtamisen toimintamalli ja sen toteutus, johon kuuluu henkilöstö, prosessit ja teknologiat, olisi katselmoitava riippumattomasti ja suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia.

## Tarkoitus

Varmistetaan organisaation tietoturvallisuuden hallintaa koskevan johtamisen jatkuva sopivuus, riittävyys ja vaikuttavuus.

## Ohjeistus

Organisaatiolla olisi oltava prosessit riippumattomien katselointien tekemiseen.

Johdon olisi suunniteltava ja käynnistettävä säänölliset riippumattomat katselmoinnit. Katselointien olisi sisällettävä tietoturvallisuuden johtamisen toimintamallin arvointi, mukaan lukien tietoturvapolitiikka, kohdennetut toimintaperiaatteet ja muut hallintakeinot, parantamismahdollisuudet ja muutostarpeet

Tällaisen katselmoinnin tekijöiden olisi oltava henkilötä, jotka ovat riippumattomia katselmoinnin kohteesta (esim. sisäinen auditointi, riippumaton esimies tai tällaisiin katselmuksiin erikoistunut ulkopuolin organisaatio). Katselmuksia tekevillä henkilöillä olisi oltava riittävä pätevyys. Katselointeja tekevä ei saisi olla johtoasemassa suhteessa katselmoitavaan kohteeseen, jotta voidaan varmistaa, että he ovat tarpeeksi riippumattomia arvioinnin tekemiseen.

Riippumattomien katselointien tuloksista olisi raportoitava joholle, joka käynnisti katselmoinnit sekä tarpeen mukaisesti ylimmälle joholle. Nämä raportit on säilytettävä.

Jos riippumattomassa katselmussa organisaation tietoturvallisuuden johtamisen toimintamallin ja sen toteutuksen todetaan olevan riittämätön (esim. dokumentoidut tavoitteet ja vaatimukset eivät täty, tai poikkeavat tietoturvapolitiikoissa tai kohdennetuissa toimintaperiaatteissa [ks. [kohta 5.1](#)] ilmoitetusta tietoturvallisuuden tavoitteista), johdon olisi käynnistettävä korjaavat toimenpiteet.

Säännöllisten riippumattomien katselointien lisäksi organisaation olisi harkittava riippumattomien katselointien tekemistä, kun

- a) organisaatiota koskevissa laeissa ja viranomaismääräyksissä tapahtuu muutoksia
- b) tapahtuu merkittävä häiriö
- c) organisaatio käynnistää uutta liiketoimintaa tai tekee muutoksia nykyiseen
- d) organisaatio alkaa käyttää uusia tuotteita tai palveluita tai muuttaa nykyisten tuotteiden tai palveluiden käyttöä
- e) organisaatio muuttaa tietoturvallisuuden hallintakeinojaan ja -menettelyjään merkittävästi.

## Lisätiedot

Standardissa ISO/IEC 27007 ja teknisessä spesifikaatiossa ISO/IEC TS 27008 annetaan riippumattomien katselointien tekemistä koskevia ohjeita.

### 5.36 Tietoturvallisuutta koskevien toimintaperiaatteiden, sääntöjen ja standardien noudattaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Lait_ja_yaatus-tenmukaisuus #Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ekosysteemi

#### Hallintakeino

Vaativuudenmukaisuutta suhteessa organisaation tietoturvapolitiikkaan, kohdennettuihin toimintaperiaatteisiin, sääntöihin ja standardeihin olisi katselmoitava säänöllisesti.

#### Tarkoitus

Varmistetaan, että tietoturvallisuus on toteutettu ja että sitä noudatetaan organisaation turvallisuuspolitiikkaan, kohdennettujen toimintaperiaatteiden ja sääntöjen ja standardien mukaisesti.

#### Ohjeistus

Esimiesten tai palvelujen, tuotteiden tai tietojen omistajien olisi tunnistettava, miten tietoturvapolitiikassa, kohdennetuissa toimintaperiaatteissa, säänöissä, standardeissa ja muissa sovellettavissa määräyksissä

määritellyt tietoturvavaatimukset katselmoidaan. Automaattisia mittaus- ja raportointityökaluja olisi harkittava vaikuttavan ja säännöllisen katselmoinnin toteuttamista varten.

Jos katselmukseen tuloksena löydetään poikkeamia, esimiesten olisi

- a) tunnistettava poikkeaman syyt
- b) arvioitava tarve korjaaviin toimenpiteisiin vaatimustenmukaisuuden saavuttamista varten
- c) toteutettava asianmukaiset korjaavat toimenpiteet
- d) katselmoitava toteutetut korjaavat toimenpiteet, jotta voidaan todentaa niiden toimivuus ja tunnistaa niiden mahdolliset puutteet tai heikkoudet.

Katselmostien tulokset ja esimiesten tai palvelujen, tuotteiden tai tietojen omistajien tekemät korjaavat toimenpiteet olisi kirjattava ja tästä seuraavia tallenteita olisi ylläpidettävä. Esimiesten olisi raportoitava tuloksista riippumattomien katselmusten tekijöille (ks. [kohta 5.35](#)), kun riippumaton katselmus kohdistuu heidän vastuualueeseensa.

Korjaavat toimenpiteet olisi saatettava loppuun ajassa, joka määritellään poikkeaman aiheuttaman riskin perusteella. Jos korjaavia toimenpiteitä ei ole saatu vietyä loppuun ennen seuraavaa säännöllistä katselmostia, olisi korjaavien toimenpiteiden edistymisen tilanne käsiteltävä tässä yhteydessä.

#### Lisätiedot

Järjestelmän tuotannon ja käytön valvontaa kuvataan [kohdissa 8.15, 8.16 ja 8.17](#).

### 5.37 Dokumentoidut toimintaohjeet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Palautus	#Omaisuudenhallinta #Fyysisen_turvalisuus #Järjestelmän_ja_verkon_turvalisuus #Sovelluksen_turvalisuus #Turvallinen_konfigurointi #Identiteetti_ ja_käyttövaltuushallinta #Uhkien_ja_haavoittuvuuksien_hallinta #Jatkuvuus #Tietoturvatapahtumien_hallinta	#Hallintotapa_ ja_ekosysteemi #Suojaaminen #Puolustus

#### Hallintakeino

Tietojenkäsittelypalveluita koskevat toimintaohjeet olisi dokumentoitava ja niiden olisi oltava kaikkien niitä tarvitsevien henkilöstön jäsenten saatavilla.

#### Tarkoitus

Varmistetaan tietojenkäsittelypalvelujen oikea ja turvallinen toiminta.

## Ohjeistus

Toimintaohjeet olisi laadittava organisaation tietoturvallisuuteen liittyville toiminnoille. Tällaisia tilanteita ovat esimerkiksi ne, joissa

- a) useamman henkilön on kyettävä tekemään tehtävä samalla tavalla
- b) toiminto tehdään harvoin ja sen tekemistä koskevat menettelyt on todennäköisesti silloin jo unohdettu
- c) toiminto on uusi ja siinä on riski tekotavan virheellisyystä
- d) toimintoa ollaan siirtämässä uuden henkilöstön vastuulle.

Toimintaohjeissa olisi määriteltävä

- a) vastuussa olevat henkilöt
- b) järjestelmien turvallinen asentaminen ja asetusten tekeminen
- c) tiedon muokkaus ja käsittely sekä automaattisesti että manuaalisesti
- d) varmuuskopiointi (ks. [kohta 8.13](#)) ja kriisinkestävyys
- e) aikataulutusvaatimukset, mukaan lukien keskinäiset riippuvuussuhteet muiden järjestelmien kanssa
- f) ohjeet virheiden tai muiden poikkeuksellisten tilanteiden käsittelyyn (esim. apuohjelmien käyttörajoitukset (ks. [kohta 8.18](#)), joita voi ilmetä työn tekemisen aikana
- g) tuki- ja eskalointiyhteystiedot, mukaan lukien ulkoiset tukiyytymiset odottamattomien käytööä koskevien tai teknisten vaikeuksien ilmaantuessa
- h) tallennusvälineiden käsittelyohjeet (ks. [kohdat 7.10](#) ja [7.14](#))
- i) järjestelmän uudelleenkäynnistys- ja toipumismenettelyt toiminnan keskeydyttäy
- j) kirjausketjun ja järjestelmän lokitietojen (ks. [kohdat 8.15](#) ja [8.17](#)) sekä videovalvontajärjestelmien (ks. [kohta 7.4](#)) hallinta
- k) seurantamenettelyt, kuten kapasiteetti, suorituskyky ja turvallisuus (ks. [kohdat 8.6](#) ja [8.16](#))
- l) huolto-ohjeet.

Dokumentoituja toimintaohjeita olisi katselmoitava ja päivitetävä tarpeen mukaan. Dokumentoituuihin toimintaohjeisiin tehtävät muutokset olisi valtuutettava. Tietojärjestelmiä olisi hallittava johdonmukaisesti samoilla menettelyillä, työkaluilla ja tukitoiminoilla, mikäli se on teknisesti mahdollista.

## Lisätiedot

Ei lisätietoja.

## 6 Henkilöstöön liittyvät hallintakeinot (EN)

### 6.1 Taustatarkistus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi

## Hallintakeino

Kaikkien työnhakijoiden taustat olisi tarkistettava ennen heidän palkkaamistaan organisaatioon sekä jatkuvana prosessina lakiin, määräysten ja eettisten normien mukaisesti. Tarkistukset olisi suhteutettava liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokituksen ja arvioituihin riskeihin.

## Tarkoitus

Varmistetaan, että henkilöstö on soveltuva niihin rooleihin, joihin heitää harkitaan ja että he säilyttävät kelpoisuutensa ja soveltuuutensa työsuhteen aikana.

## Ohjeistus

Taustatarkistusprosessi olisi kohdistettava koko henkilöstöön, mukaan lukien kokoaikaiset, osa-aikaiset ja tilapäiset työntekijät. Kun nämä henkilöt on hankittu palvelutoimittajien kautta, olisi taustatarkistuksia koskevat vaatimukset sisällytettävä organisaation ja toimittajan välisiin sopimuksiin.

Kaikkia organisaation avoimeen toimeen harkittavia työnhakijoita koskevat tiedot olisi kerättävä ja käsiteltävä ottaen huomioon kyseisen lainsäädäntöalueen lainsäädäntö. Joillain lainsäädäntöalueilla organisaatiolla voi olla lakisäädteinen velvollisuus ilmoittaa työnhakijoille taustatarkistuksesta etukäteen.

Taustatarkistuksissa olisi otettava huomioon kaikki tietosuojaan, henkilötietojen suojaamiseen ja työsuhesiin liittyvä lainsäädäntö. Niiden olisi, jos sallittua, sisällettävä seuraavat asiat:

- a) riittävien suositusten saatavuus (esim. suosittelija liike-elämästä ja henkilökohtainen suosittelija)
- b) hakijan ansioluetteloon aukottomuuden ja oikeellisuuden tarkistaminen
- c) ilmoitetun koulutuksellisen tai ammatillisen pätevyyden varmistaminen
- d) henkilöllisyden tarkistaminen riippumattomasta lähteestä (esim. passi tai muu viranomaisen myöntämä vastaava asiakirja)
- e) yksityiskohtaisempi taustatarkistus, kuten luottotietojen tai rikosrekisterin tarkistus, jos työnhakija hakee työtä, jossa näillä on merkitystä.

Kun henkilö palkataan määritetyyn tietoturvarooliin, olisi organisaation varmistettava, että

- a) työnhakijalla on vaadittu pätevyys turvallisuusrooliin
- b) työnhakijaa pidetään luotettavana rooliin, etenkin, jos rooli on kriittinen organisaation kannalta.

Mikäli työtehtävä joko työsuhteen alusta tai ylennyksen jälkeen sisältää käyttöoikeuksia tietojenkäsittelypalveluihin ja etenkin arkaluonteisia tietoja (esim. taloudellista tietoa tai erittäin luottamuksellisia tietoja) käsitleviin palveluihin, organisaation olisi harkittava yksityiskohtaisempia lisätarkistuksia.

Menettelyissä olisi määriteltävä taustatarkistusten kriteerit ja rajoitukset (esim. kenellä on oikeus tarkistaa ihmisten tietoja ja miten, milloin ja miksi taustatarkistuksia tehtiin).

Tilanteissa, joissa taustatarkistusta ei voida tehdä hyväksytävässä ajassa, olisi otettava käyttöön lieventäviä hallintakeinoja, joita noudatetaan katselmoinnin loppuun asti. Tällaisia ovat esim.

- a) työtehtävien aloittamisen viivyttäminen
- b) organisaation omaisuuserien luovuttamisen viivyttäminen
- c) työtehtävien aloittaminen rajoitetuin pääsyyoikeuksin
- d) työsuhteen päättäminen.

Taustatarkistukset olisi toistettava säännöllisesti, jotta voidaan varmistaa, että henkilöstö on yhä tehtäviinsä soveltuva, riippuen roolin kriittisyydestä.

## Lisätiedot

Ei lisätietoja.

## 6.2 Työsuhteen ehdot (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi

### Hallintakeino

Työsuhteeseen liittyvissä sopimuksissa olisi eriteltävä henkilöstön ja organisaation tietoturvallisuutta koskevat vastuut.

### Tarkoitus

Varmistetaan, että henkilöstön jäsenet ymmärtävät tietoturvallisuutta koskevat vastuunsa heille harkituissa tehtävissä.

### Ohjeistus

Henkilöstön sopimuksellisissa velvoitteissa olisi otettava huomioon organisaation tietoturvapolitiikka ja asianmukaiset kohdennetut toimintaperiaatteet. Lisäksi niissä voidaan selkeyttää ja ilmaista seuraavat asiat:

- salassapito- ja vaitiолоситумус, jotka henkilöstön, jolle myönnetään pääsy luottamukselliseen tietoon, olisi allekirjoitettava ennen kuin heille myönnetään pääsy tietoihin ja niihin liittyviin omaisuuseriin (ks. [kohta 6.6](#))
- juridiset vastuut ja oikeudet, esim. liittyen tekijänoikeus- tai tietosuojalainsäädäntöön (ks. [kohdat 5.32 ja 5.34](#))
- vastuu tiedon luokittelusta ja organisaation tietojen ja niihin liittyvien omaisuuserien hallinnasta, tietojenkäsittelypalvelujen ja henkilöstön käsittelemistä tietopalveluista (ks. [kohdat 5.9 ja 5.13](#))
- vastuu sidosryhmiltä saatujen tietojen käsittelyssä
- toimenpiteet, joihin ryhdytään, jos henkilöstö rikkoo organisaation turvallisuusvaatimuksia (ks. [kohta 6.4](#)).

Tietoturvaroolit ja -vastuut olisi viestittävä työnhakijoille työsuhdetta edeltävän prosessin aikana.

Organisaation olisi varmistettava, että henkilöstö hyväksyy tietoturvallisuutta koskevat ehdot. Näiden ehtojen olisi oltava asianmukaisia suhteessa henkilöstön tietojärjestelmiin ja palveluihin liittyvien organisaation omaisuuserien käyttöoikeuksien luonteeseen ja laajuuteen. Tietoturvallisuutta koskevat ehdot olisi katselmoitava, kun lakeihin, viranomaismääräyksiin, asetuksiin, tietoturvapolitiikkaan tai kohdennettuihin toimintaperiaatteisiin tulee muutoksia.

Työsuhteen ehtoihin sisältyvien velvollisuuksien olisi jatkuttava määräajan työsuhteen loppumisen jälkeenkin, mikäli se on tarkoitukseenmukaista (ks. [kohta 6.5](#)).

### Lisätiedot

Eettisillä ohjeilla voidaan ilmoittaa henkilöstön jäsenten tietoturvallisuutta koskevat vastuut, jotka liittyvät luottamuksellisuuteen, tietosuojaan, etiikkaan, organisaation tietojen ja niihin liittyvien omaisuuserien asianmukaiseen käyttöön sekä organisaation edellyttämiin hyvämaineisiin käytäntöihin.

Organisaation ulkopuolisen osapuolen, johon toimittajan henkilöstö kuuluu, voidaan edellyttää osallistuvan vuokratyöjärjestelyihin vuokratyöntekijän puolesta.

Jos organisaatio ei ole juridinen henkilö eikä sillä ole työntekijöitä, voidaan harkita tämän hallintakeinon ohjeiden mukaisia sopimusjärjestelyjä.

### 6.3 Tietoturvatietoisuus, -opastus ja -koulutus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ecosysteemi

#### Hallintakeino

Organisaation ja tärkeimpien sidosryhmien henkilöstön olisi saatava tietoturvaopastusta ja -koulutusta, ja heidän tietojaan organisaation tietoturvapolitiikan, kohdennettujen toimintaperiaatteiden ja menettelyjen muutoksista olisi päivitettyä säännöllisesti, sinä laajuudessa kuin se on heidän toimenkuvaltaa kannalta merkityksellistä.

#### Tarkoitus

Varmistetaan, että henkilöstö ja tärkeimmät sidosryhmät ovat tietoisia tietoturvavastuistaan ja täyttävät ne.

#### Ohjeistus

##### Yleistä

Tietoturvatietoisuus, -opastus ja -koulutus olisi toteutettava linjassa organisaation tietoturvapolitiikkojen, kohdennettujen toimintaperiaatteiden ja tietoturvallisuutta koskevien menettelyjen kanssa ottaen huomioon organisaation suojaavat tiedot sekä tiedon suojaamista varten toteutetut tietoturvallisuuden hallintakeinot.

Tietoturvaopastusta ja -koulutusta olisi järjestettävä säännöllisesti. Uudelle henkilöstölle sekä tietoturvallisuutta koskevilta vaatimuksiltaan merkittävästi poikkeavaan uuteen tehtävään tai rooliin vaihtavalle henkilöstölle voidaan kohdentaa perehdyttäävää tietoisuusopastausta ja koulutusta.

Henkilöstön ymmärrys olisi arvioitava tietoisuuteen, opetuksen tai koulutukseen liittyvän toiminnan lopuksi, jotta voidaan varmistaa tietämystavoitteiden saavuttaminen sekä tietoisuus-, opastus- ja koulutusohjelman vaikuttavuus.

##### Tietoisuus

Tietoturvallisuuteen liittyvän koulutusohjelman tarkoituksena olisi tehdä henkilöstön jäsenille selväksi heidän tietoturvavastuunsa sekä keinot, joilla kyseiset vastuu täytetään.

Koulutusohjelman suunnittelussa olisi otettava huomioon henkilöstön roolit organisaatiossa, mukaan lukien sisäinen ja ulkoinen henkilöstö (esim. ulkoset konsulttit, toimittajan henkilöstö). Koulutusohjelman toiminnot olisi aikataulutettava – mieluiten säännöllisiksi – siten, että toiminnot toistuvat ja uudet henkilöstön jäsenet osallistuvat niihin. Se olisi rakennettava myös tietoturvahäiriöistä opittujen asioiden pohjalle.

Koulutusohjelman olisi sisällettävä tietoisuutta parantavia toimia fyysisien tai virtuaalisten kanavien kautta, kuten kampanjoita, ohjelehtiä, julisteita, uutiskirjeitä, verkkosivustoja, tietoiskuja, esittelyjä, verkko-opiskelukokonaisuuksia ja sähköposteja.

Tietoturvatietoisuuden olisi katettava yleisiä näkökohtia, kuten

- johdon sitoutuminen koko organisaation kattavaan tietoturvallisuuteen
- sovellettaviin tietoturvasääntöihin ja -velvoitteisiin liittyvät tuntemis- ja vaatimustenmukaisuistarpeet, ottaen huomioon turvallisuuspolitiikka ja kohdennetut toimintaperiaatteet, standardit, lait, asetukset, viranomaismääräykset ja sopimukset

- c) henkilökohtainen vastuu omista tekemisistä ja tekemättä jättämisistä sekä yleiset vastut organisaation tai sidosryhmien omistaman tiedon turvaamisesta ja suojaamisesta
- d) yleiset tietoturvamenettelyt (kuten tietoturvatahtumista raportointi [6.8]) ja perustason hallintakeinot (kuten salasanat turvallisuus [5.17])
- e) yhteydenottopisteet ja resurssit, joista saa lisätietoa ja neuvoja tietoturva-asioista, mukaan lukien tietoturvatielaisuutta koskevat lisämateriaalit.

### Opetus ja koulutus

Organisaation olisi tunnistettava, valmisteltava ja toteutettava soveltuva koulutussuunnitelma niille teknisille ryhmille, joiden roolit edellyttää tiettyjä taitoja ja osaamista. Teknisillä ryhmillä olisi oltava taidot laitteiden, järjestelmien, sovellusten ja palveluiden vaaditun turvallisuustason konfigurointiin ja ylläpitämiseen. Jos ilmenee puuttuvia taitoja, organisaation olisi ryhdyttää toimeen niiden hankkimiseksi.

Opetus- ja koulutusohjelman toteuttamisessa olisi harkittava erilaisia muotoja (esim. luennot tai itseopiskelu, asiantuntijoiden tai konsulttien antama mentorointi [perehdytys], tutustuminen eri tehtäviin henkilöstön muiden jäsenien avustuksella, vaaditut taidot osaavien henkilöiden palkkaaminen ja konsulttien palkkaaminen). Siinä voidaan käyttää erilaisia opetusmenetelmiä, kuten luokkahuoneessa tapahtuvaa koulutusta, etäopetusta, verkkopohjaista koulutusta, itseopiskelua ja muita vaihtoehtoja. Teknisen henkilöstön olisi pidettävä tietämyksensä ajan tasalla tilaamalla uutiskirjeitä ja lehtiä tai käymällä konferensseissa ja tapahtumissa, jotka on tarkoitettu teknisen ja ammatillisen osaamisen parantamiseen.

### Lisätiedot

Koulutusohjelmaa koostettaessa olisi tärkeää keskittyä mitä- ja miten-kysymyksien lisäksi myös miksi-kysymykseen, kun se on mahdollista. On tärkeää, että henkilöstön jäsenet ymmärtävät tietoturvan tarkoituksen ja mahdolliset heidän käytöksestäni organisaatiolle aiheutuvat positiiviset tai negatiiviset vaikutukset.

Tietoturvatielaisuus, -opastus ja -koulutus voivat olla osa muita toimintoja tai ne voidaan toteuttaa yhdessä niiden kanssa esimerkiksi osana yleistä tietojenhallinnan, tietotekniikan, tietoturvallisuuden, tietosuojan tai turvallisuuden koulutusta.

## 6.4 Kurinpitoprosessi [\(EN\)](#)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi

### Hallintakeino

Organisaatiolla olisi oltava muodollinen ja tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, kun henkilöstön tai sidosryhmän edustaja on syyllistynyt tietoturvapolitiikan rikkomukseen.

### Tarkoitus

Varmistetaan, että henkilöstö ja muut olennaiset sidosryhmät ymmärtävät tietoturvapolitiikan rikkomusten seuraukset, jotta voidaan ehkäistä rikkomuksia ja käsitellä asianmukaisesti henkilöstöä tai sidosryhmiä, jotka ovat syyllistyneet rikkomukseen.

### Ohjeistus

Kurinpitoprosessia ei saisi aloittaa ennen kuin on todennettu, että tietoturvapolitiikan rikkomus on tapahtunut (ks. [kohta 5.28](#)).

Muodollisen kurinpitoprosessin olisi tarjottava asteittainen vaste, jossa otetaan huomioon tiettyjä tekijöitä, kuten

- a) rikkomuksen ja sen seurausten luonne (kuka, mitä, missä ja miten) ja vakavuus
- b) se, tehtiinkö rikkomus tahallaan tai tahattomasti
- c) se, oliko kyseessä ensimmäinen rikkomus
- d) se, oliko rikkomukseen syyllistynyt saanut asianmukaisen koulutuksen.

Vasteessa olisi otettava huomioon asiaankuuluvat laki, asetukset, viranomaisten, sopimusten ja liiketoiminnan vaatimukset sekä tarpeen mukaan muita tekijöitä. Kurinpitoprosessin olisi toimittava myös pelotteena, jonka ansiosta henkilöstö ja muut olennaiset sidosryhmät eivät riko tietoturvapolitiikkaa, kohdennettuja toimintaperiaatteita ja tietoturvaan liittyviä menettelyjä. Tahalliset tietoturvapolitiikan rikkomuksen voivat vaatia välittömiä toimia.

### Lisätiedot

Kurinpitoprosessin kohteiden henkilöllisyyttä olisi mahdollisuksien mukaan suojeleva asianmukaisten vaatimusten mukaisesti.

Kun henkilöt osoittavat erinomaista tietoturvallisuuteen liittyvää toimintaa, heitä voidaan palkita, mikä edistää tietoturvaa ja kannustaa hyviin käytäntöihin.

## 6.5 Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus #Omaisuudenhallinta	#Hallintotapa_ja_ecosysteemi

### Hallintakeino

Olisi määritettävä tietoturvavastut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä olisi viestittävä olennaisille henkilöille ja sidosryhmileille, ja niiden noudattaminen olisi varmistettava.

### Tarkoitus

Suojataan organisaation etuja osana työsuhteen tai sopimuksen päättymis- tai muutosprosessia.

### Ohjeistus

Työsuhteen päättymisen tai muutoksen hallintaprosessissa olisi määriteltävä, minkä tietoturvavastuiden ja -velvollisuuksien olisi pysyttävä voimassa työsuhteen päättymisen tai muun muutoksen jälkeen. Näihin voivat sisältyä tietojen, aineettoman omaisuuden ja muun saadun tietämyksen luottamuksellisuus sekä mahdollisiin salassapitositoumuksiin sisältyvät vastuut (ks. [kohta 6.6](#)). Vastut ja velvollisuudet, jotka ovat yhä voimassa työsuhteen tai sopimuksen päättymisen jälkeen, olisi sisällytettävä henkilön työsopimuksen tai muun sopimuksen ehtoihin (ks. [kohta 6.2](#)). Myös muut sopimukset, jotka jatkuvat määrätyn ajan työsuhteen loppumisen jälkeenkin, voivat sisältää tietoturvavastuita.

Vastuiden tai työsuhteiden muutoksia olisi hallittava kuten nykyisten vastuiden tai työsuhteiden päättymistä, mutta yhdistäen siihen uusien vastuiden ja työsuhteiden käynnistäminen.

Lähtevällä tai työroolia muuttavalla henkilöllä olevat tietoturvaroolit ja -vastut olisi tunnistettava ja siirrettävä toiselle henkilölle.

Olisi laadittava prosessi, jolla viestitään muutoksista ja toimintatavoista henkilöstölle, muille sidosryhmileille ja (esim. asiakkaiden ja toimittajien) olennaisille yhteyshenkilölle.

Työsuhteen päätämis- tai muutosprosessia olisi myös sovellettava ulkoiseen henkilöstöön (eli toimittajiin), kun työsuhteen päättyminen kohdistuu organisaatiolle tehtävään työhön tai sitä koskevaan sopimukseen tai kun työntkuva organisaatiossa muuttuu.

### Lisätiedot

Monissa organisaatioissa henkilöstöhallinto on vastuussa työsuhteen päättymisprosessista kokonaisuutena ja työskentelee yhdessä lähevän henkilön esimiehen kanssa, jotta se kykenee hallitsemaan asiaankuuluvien menettelyjen tietoturvallisuusnäkökohtia. Jos kyseessä on organisaation ulkopuolisen osapuolen (esim. toimittajan) kautta tullut työntekijä, olisi ulkopuolisen osapuolen tehtävä työsuhteen päättäminen organisaation ja ulkopuolisen osapuolen keskinäisen sopimuksen mukaisesti.

## 6.6 Salassapito- ja vaitiolositoumukset (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Henkilöstöturvallisuus #Tietojen_suojaaminen #Toimittajasuhteet	#Hallintotapa_ja_ecosysteemi

### Hallintakeino

Organisaation tiedonsuojaustarpeita kuvaavat salassapito- ja vaitiolositoumukset olisi yksilöitäävä, dokumentoitava ja katselmoitava säännöllisesti, ja niihin olisi saatava henkilöstön ja muiden olennaisten sidosryhmien hyväksyntä.

### Tarkoitus

Ylläpidetään henkilöstön ja ulkoisten osapuolen käytössä olevien tietojen luottamuksellisuutta.

### Ohjeistus

Salassapito- tai vaitiolositoumuksissa olisi käsiteltävä luottamuksellisen tiedon suojaamista käyttäen juridisesti täytäntöönpanokelpoisia ehtoja. Salassapito- tai vaitiolositoumuksia tehdään sidosryhmien ja organisaation henkilöstön kanssa. Sitoumuksissa olevat ehdot olisi määritettävä organisaation tietoturvavaatimusten perusteella ja ottamalla huomioon käsiteltävien tietojen tyyppi, niiden luokitustaso, käyttö ja muiden osapuolten luvallinen pääsy niihin. Yksilötäessä salassapito- tai vaitiolositoumuksia koskevia vaatimuksia olisi otettava huomioon seuraavat tekijät:

- a) suojattavan tiedon määrittely (esim. luottamuksellinen tieto)
- b) sitoumuksen oletettu kesto mukaan lukien tapaukset, joissa luottamuksellisuutta saatetaan joutua jatkamaan toistaiseksi tai kunnes tieto muuttuu julkiseksi
- c) edellytetty toimenpiteet, kun sopimus päättyy
- d) osapuolten vastuut ja toimenpiteet, jotta vältetään luvaton tiedon paljastaminen
- e) tiedon, liikesalaisuuksien ja aineettoman omaisuuden omistajuus ja se, miten tämä liittyy luottamuksellisen tiedon suojaamiseen
- f) luottamuksellisen tiedon sallittu käyttö ja osapuolen oikeudet käyttää tietoa
- g) oikeus tarkastaa ja valvoa tehtäviä, joihin liittyy erittäin arkaluonteisia asioita koskevaa luottamuksellista tietoa
- h) prosessi, jolla ilmoitetaan ja raportoidaan luvattomasta paljastumisesta tai luottamuksellisen tiedon vuotamisesta
- i) ehdot, joilla tieto palautetaan tai tuhotaan sitoumuksen päättymessä
- j) odotetut toimenpiteet, joihin ryhdytään, jos sitoumusta rikotaan.

Organisaation olisi varmistettava, että salassapito- ja vaitiolositoumukset noudattavat lainkäyttöalueidensa lakeja (ks. [kohdat 5.31, 5.32, 5.33 ja 5.34](#)).

Salassapito- ja vaitiolositoumuksia koskevia vaatimuksia olisi katselmoitava säännöllisin aikavälein ja aina silloin, kun tapahtuu näihin vaatimuksiin vaikuttavia muutoksia.

## Lisätietoa

Salassapito- ja vaitiolosopimukset suojaavat organisaation tietoa ja viestivät allekirjoittaneille heidän vastuunsa suojata, käyttää ja paljastaa tietoa vastuullisella ja luovallisella tavalla.

## 6.7 Etätyöskentely (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen #Fyysinen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Tilanteisiin, joissa henkilöstö työskentelee etänä, olisi toteutettava turvallisuusratkaisut, joilla suojataan organisaation tilojen ulkopuolella käytettyjä, käsiteltyjä tai varastoituja tietoja.

### Tarkoitus

Varmistetaan tietojen turvallisuus, kun henkilöstö työskentelee etänä.

### Ohjeistus

Etätyöskentelyksi katsotaan kaikki organisaation henkilöstön työskentely, joka tapahtuu organisaation toimitilojen ulkopuolella ja jossa käytetään tietoja joko tulosteina tai sähköisessä muodossa tieto- ja viestintätekniisten laitteiden välaineiden avulla. Etätyöskentely-ympäristöjä voidaan kutsua esim. "etätyöksi", "joustavaksi työskentelyksi" ja "virtuaalityöksi".

HUOM. Kaikkia tässä ohjeistuksessa annettuja suosituksia ei välttämättä voida soveltaa eri lankäyttöalueiden paikallisista laeista ja viranomaismääräyksistä johtuen.

Etätyön sallivien organisaatioiden olisi laadittava etätyöskentelyä koskevat kohdennetut toimintaperiaatteet, joissa määritellään etätyötä koskevat ehdot ja rajoitukset. Seuraavat asiat olisi otettava huomioon, kun ne katsotaan soveltuviksi:

- a) etätyöpaikan olemassa oleva tai ehdotettu fyysinen turvallisuus ottaen huomioon sijainnin ja paikallisen ympäristön fyysinen turvallisuus, mukaan lukien eri lankäyttöalueet, joilla henkilöstö sijaitsee
- b) etätyöskentelypaikan fyysisistä ympäristöä koskevat säännöt ja turvallisuusmekanismit, kuten lukittavat kaapit, sijaintien välinen turvallinen kuljettaminen sekä etäkäyttöä, puhdasta työpöytää, tietojen ja niihin liittyvien omaisuuserien tulostamista ja hävittämistä koskevat säännöt ja tietoturvatapahtumista raportointi (ks. [kohta 6.8](#))
- c) odotetut fyysiset etätyöskentely-ympäristöt
- d) tietoliikenteen turvallisuusvaatimukset ottaen huomioon organisaation järjestelmien etäkäyttötarve ja arkaluonteisuus sekä käytettävän ja tietoliikenneyhteyden yli siirrettävän tiedon arkaluonteisuus ja järjestelmien ja sovellusten arkaluonteisuus
- e) etäkäyttö, kuten pääsy virtuaalityöpöydälle, joka tukee tiedon käsittelyä ja tallentamista henkilökohtaisissa laitteissa

- f) muiden etäyöskentelypaikan jakavien ihmisten (esimerkiksi perheenjäsenten ja ystävien) luvattoman käytön tiedolle ja resursseille aiheuttama uhka
- g) muiden julkisilla paikoilla olevien ihmisten luvattoman käytön tiedolle ja resursseille aiheuttama uhka
- h) kotiverkon ja julkisten verkkojen käyttöä ja langattomien verkkopalvelujen konfiguraatioita koskevat vaatimukset ja rajoitukset
- i) turvallisuustoimien, kuten palomuurien ja haittaohjelmien torjunnan, käyttö
- j) turvalliset mekanismit järjestelmien käyttöönottoon ja käynnistämiseen etänä
- k) turvalliset mekanismit todentamiseen ja pääsyoikeuksien käyttöönottoon ottamalla huomioon yksivaiheisten todentamismekanismien haavoittuvuus, kun on sallittua ottaa etäyhteys organisaation verkoon.

Tarkasteltavien ohjeiden ja toimien olisi sisällettävä

- a) sopivien laitteiden ja säilytyskalusteiden järjestäminen etäyötä varten, jos organisaation valvonnan ulkopuolella olevien henkilökohtaisten laitteiden käyttö ei ole sallittua
- b) sallittavan työn ja käytettävän tiedon luokituksen määrittely ja sellaisten sisäisten järjestelmien ja palvelujen määrittely, joihin pääsy on hyväksytty etäyöskentelijälle
- c) koulutuksen tarjoaminen etänä työskenteleville sekä tukihenkilöstölle, minkä pitäisi sisältää se, kuinka liiketoiminta toteutetaan turvallisesti etäyössä
- d) soveltuvienviestintävälaineiden tarjoaminen mukaan lukien menetelmät etäyhteyden suojaamiseen, kuten vaatimus laitteen näytön lukitsemisesta ja toimettomuusajastimet, laitteen sijainnin aktivoiminen ja sekä etäyhennystoimintojen asentaminen
- e) fyysisen turvallisuuden
- f) perheen ja vieraiden pääsyä laitteistoon ja tietoihin koskevat säännöt ja ohjeet
- g) laitteisto- ja ohjelmistohankinnat sekä niiden tuki ja ylläpito
- h) vakuutusten hankkiminen
- i) varmuuskopointia ja liiketoiminnan jatkuvuutta koskevat menettelyohjeet
- j) tapahtumien ja turvallisuuden seuranta
- k) valtuksien ja pääsyoikeuksien peruuttaminen ja laitteiden palauttaminen etäyöskentelyn päätyessä.

## Lisätiedot

Ei lisätietoja.

## 6.8 Tietoturvatapahtumista raportointi (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto	#Tietoturva-tapahtumien_hallinta	#Puolustus

## Hallintakeino

Organisaation olisi tarjottava henkilöstölle mekanismi havaittujen tai epäiltyjen tietoturvatapahtumien välittömään raportointiin asianmukaisten kanavien kautta.

## Tarkoitus

Tuetaan henkilöstön tunnistettavissa olevien tietoturvatapahtumien välitöntä, johdonmukaista ja vaikuttavaa raportointia.

## Ohjeistus

Kaikkien henkilöstön jäsenten ja käyttäjien olisi oltava tietoisia velvollisuudestaan raportoida tietoturvatapahtumista mahdollisimman pian, jotta kyettää minimoimaan tai estämään tietoturvahäiriöiden vaikutukset. Heidän olisi myös tunnettava tietoturvatapahtumien raportointimenettely ja se yhteydenottopiste, johon tapahtumat olisi raportoitava. Raportointimekanismi olisi oltava mahdollisimman yksinkertainen sekä helposti saatavissa ja käytettävissä oleva. Tietoturvatapahtumia ovat mm. häiriötilanteet, murrot ja haavoittuvuudet.

Tietoturvatapahtumien raportointiin liittyen olisi otettava huomioon mm. seuraavat asiat:

- a) tehottomat tietoturvallisuuden hallintakeinot
- b) tietojen luottamuksellisuutta, eheyttä tai saatavuutta koskevien odotusten rikkominen
- c) ihmilliset virheet
- d) poikkeamat tietoturvapolitiikasta, kohdennetuista toimintaperiaatteista tai soveltuista standardeista
- e) fyysisen turvallisuusratkaisujen murrot
- f) järjestelmään tehtävät muutokset, jotka eivät ole menneet muutoksenhallintaprosessin kautta
- g) ohjelmistoja tai laitteistoja toimintahäiriöt tai muu poikkeava käyttäytyminen
- h) pääsyrikkomukset
- i) haavoittuvuudet
- j) epäillyt haittaohjelmatartunnat.

Henkilöstöä ja käyttäjiä olisi neuvottava olemaan yritymättä todentaa epäiltyjä tietoturvahaavoittuvuuksia. Haavoittuvuuksien testaaminen voitaisiin tulkita mahdolliseksi järjestelmän väärinkäytöksi ja se voi myös vahingoittaa tietojärjestelmää tai -palvelua, ja se voi korruptoida tai sotkea sähköisiä todisteita. Tästä voi aiheutua lakisäteinen vahinkovastuu testauksen tehneelle henkilölle.

## Lisätiedot

Lisätietoja löytyy standardisarjasta ISO/IEC 27035.

## 7 Fyysiset hallintakeinot (EN)

### 7.1 Fyysiset turva-alueet (EN)

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus	#Suojaaminen

## Hallintakeino

Turva-alueet olisi määriteltävä, ja niitä olisi käytettävä, mikäli tiedon ja siihen liittyvien omaisuuserien suojaaminen edellyttää turva-alueita

## Tarkoitus

Estetään luvaton tunkeutuminen organisaation tietoihin ja muihin niihin liittyviin omaisuuseriin sekä niiden vahingoittuminen ja toiminnan häiriintyminen.

## Ohjeistus

Seuraavat fyysisiä turva-alueita koskevat ohjeet olisi otettava huomioon ja toteutettava asianmukaisissa paikoissa:

- Turva-alueiden sijainnin ja rajojen (ulkokuoren) ja rakenteiden lujuuden määrittelemisen turva-alueella käsiteltävä tiedon ja muiden omaisuuserien tietoturvavaatimusten perusteella.
- Tietojenkäsittelypalveluita sisältävien rakennusten ja toimipaikkojen fyysisen turva-alueiden rakenteellinen eheys (eli turva-alueessa ei saisi olla aukkoja eikä helposti murrettavia kohtia). Toimipaikan ulkoseinien, perustusten, kattojen (ulko- ja sisä-) ja lattioiden olisi oltava yhtenäistä rakennetta ja kaikki ulko-ovet olisi suojattava asianmukaisesti luvattomalta kululta hallintamekanismien avulla (esim. rakenteelliset esteet, hälytimet, lukot). Ovet ja ikkunat olisi lukittava, kun niitä ei valvota, ja etenkin alakerroksissa oleviin ikkunoihin olisi harkittava ulkopuolista suojausta, kuten myös ilmastoinnin ilmanvaihtoaukkoihin.
- Kaikkien turva-alueen rajalla olevien palo-ovien varustaminen hälyttimillä, niiden valvonta ja testaaminen. Palo-ovien ja seinien olisi annettava standardien ja viranomaismääräyksien mukainen paloturvallisuussuoja. Hälyttimien olisi toimittava myös sähkökatkon aikana (*fail safe*).

## Lisätiedot

Fyysinen suojaus voidaan saavuttaa luomalla yksi tai useampi fyysinen este organisaation tilojen ja tietojenkäsittelypalvelujen tilojen ympärille.

Turva-alue voi olla lukittava toimisto tai useita huoneita, joita ympäröi pysyvä ja yhtenäinen sisäinen fyysinen este. Kunkin turvavyöhykkeen sisäpuolelle voi olla tarpeen luoda lisäestetä ja -vyöhykkeitä valvomaan eri alueiden välistä kulkua niiden erilaisten turvallisuusvaatimusten mukaan. Organisaation olisi harkittava fyysisiä turvallisuusratkaisuja, joita voidaan vahvistaa, kun uhkatalanne kärjistyy.

## 7.2 Kulunvalvonta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus #Identiteetti_-ja_käyttövaltuushallinta	#Suojaaminen

## Hallintakeino

Turva-alueet olisi suojattava asianmukaisella kulunvalvonnalla ja sisäänpäyntineillä.

## Tarkoitus

Varmistetaan, että organisaation tietoja ja niihin liittyviä omaisuuseriä käytetään vain luvallisesti.

## Ohjeistus

### Yleistä

Sisäänpäyntien, kuten tavaralogistiikan lastausalueita, sekä muita pisteytä, joiden kautta luvattomat henkilöt saattavat päästää tiloihin, olisi valvottava, ja ne olisi mahdollisuksien mukaan eristettävä tietojenkäsittelypalveluista, jotta niihin ei pääse luvatta.

Seuraavia ohjeita olisi noudatettava:

- a) Toimipaikkaan ja rakennuksiin pääsy rajoitetaan ainoastaan hyväksyttylle henkilöstölle. Fyysisen alueiden pääsyoikeuksien hallintaprosessin olisi sisällettävä valtuutuksien myöntäminen, säännöllinen katselointi, päivittäminen ja poistaminen (ks. [kohta 5.18](#)).
  - b) Kaiken kulun merkitseminen käyttöpäiväkirjaan tai vieraskirjaan tai sähköisen kulunvalvonnan järjestäminen niin, että kaikki kulut alueella kirjataan, ja että kirjausketju on suojattu oikeudettomilta muutoksilta. Kaikki lokitiedot sekä (ks. [kohta 5.33](#)) ja luottamuksellisten tunnistautumistietojen suojaaminen olisi järjestettävä.
  - c) Pääsynhallinta koskevien prosessien ja teknisten mekanismien suunnittelu ja toteuttaminen alueille, joissa tietoa käsitellään tai tallennetaan. Tunnistusmekanismeja ovat esim. kulkukortit, biometriikka ja kaksivaiheinen tunnistautuminen, kuten kulkukortti yhdistettyä salaiseen tunnuslukuun. Kaikkein tärkeimmillä alueilla olisi harkittava kaksinkertaisten turvaovien käyttöä.
  - d) Fyysisistä pääsyä tiloihin tai rakennukseen voidaan hallita henkilöstön valvoman vieraiden vastaanoton tai muiden keinojen avulla.
  - e) Henkilöstön ja muiden henkilöiden mukanaan tuomien tavaroiden tarkistaminen sekä saapuessa että poistuessa.
- HUOM. Paikalliset lait ja viranomaismääräykset voivat koskea henkilökohtaisten tavaroiden tarkistamista.
- f) Kaikkia henkilöstön jäseniä ja muita rakennuksessa olevia henkilöitä olisi vaadittava käyttämään näkyvää tunnistetta. Kaikkia olisi myös vaadittava ilmoittamaan välittömästi turvahenkilökunnalle, mikäli he tapaavat vierailijoita ilman saattajaa tai henkilön ilman näkyvää tunnistetta. Selkeästi toisistaan erottuvat kulkutunnisteet helpottavat pysyvien työntekijöiden, ulkoisten toimittajien ja vierailijoiden erottamisessa toisistaan.
  - g) Toimittajan henkilöstölle olisi myönnnettävä ainoastaan välttämättömät pääsyoikeudet turva-alueille ja tietojenkäsittelypalveluihin. Kulkuoikeuksien myöntämisestä vastaavan henkilön olisi hyväksyttävä nämä pääsyoikeudet, ja niitä olisi valvottava.
  - h) Kulkuoikeuksien turvallisuuteen olisi kiinnitettävä erityishuomiota rakennuksissa, joissa on useamman kuin yhden organisaation omaisuutta.
  - i) Fyysisen turvallisuusratkaisujen suunnitteleminen siten, että niitä voidaan tiukentaa, kun fyysisen häiriötilanteiden todennäköisyys kasvaa.
  - j) Muiden kuin jatkuvassa käytössä olevien kulkaukkujen, kuten hätäpoistumisteiden suojaaminen luvattomalta pääsyltä tiloihin.
  - k) Avaintehallintaprosessin toteuttaminen, jotta voidaan varmistaa fyysisen avainten ja tunnistautumistietojen (esim. lukkojen avauskoodien, toimistojen, huoneiden ja toimitilojen kulunvalvonnan ja tunkeutumisenestojärjestelmien PIN-koodien sekä avainturvakaappien PIN-koodien) hallinta, jotta käytössä on avainten luovutusten ja palautusten kirjaamisen loki tai avainten vuosittainen auditointi ja jotta pääsyä fyysisiin avaimiin tai tunnistautumistietoihin hallitaan ([kohdassa 5.17](#) on tunnistautumistietoja koskevia lisätietoja).

### Vierailijat

Seuraavia ohjeita olisi noudatettava:

- a) Vierailijoiden henkilöllisyydet olisi todennettava.
- b) Vierailijoiden saapumisen ja poistumisen päivämäärät ja kellonajat olisi kirjattava.
- c) Vierailijoille olisi sallittava pääsy vain tarkasti määriteltyjä, luvallisia tarkoituksesta varten ja heitä olisi ohjeistettava aluetta koskevista turvallisuusasioista ja toiminnasta palo- ja muissa hätätilanteissa.
- d) Kaikkia vierailijoita olisi valvottava, ellei näille ole myönnetty nimenomaista poikkeusta olla yksin.

### Lastausalueet ja saapuvat materiaalit

Seuraavia ohjeita olisi noudatettava:

- a) Pääsy lastausalueille rakennuksen ulkopuolelta olisi rajoitettava tunnistettuihin ja luvan omaaviin henkilöihin.
- b) Lastausalueet olisi suunniteltava siten, että kuormat voidaan lastata ja purkaa kuljetushenkilöstön pääsemättä luvatta rakennuksen muihin osiin.
- c) Lastausalueiden ulko-ovien olisi sulkeuduttava, kun lastausalueelta kulkuoikeusrajoitetuille alueille johtavat sisäovet avataan.
- d) Saapuvat tavaratoimitukset olisi tarkastettava ja tutkittava räjähteiden, kemikaalien tai muiden vaarallisten aineiden varalta ennen kuin ne siirretään eteenpäin toimitus- ja kuormausalueiltä.
- e) Saapuvat toimitukset olisi rekisteröitävä sovitusti (ks. [kohdat 5.9](#) ja [7.10](#)) niiden saapuessa toimipaikalle
- f) Saapuvan ja lähtevän tavaran käsittelyn eriyttäminen mahdollisuksien mukaan.
- g) Saapuvien toimitusten tarkastaminen, ettei niihin ole kajottu. Jos tästä havaitaan, olisi siitä ilmoitettava välittömästi turvahenkilökunnalle.

### Lisätiedot

Ei lisätietoja.

## 7.3 Toimistojen, tilojen ja laitteistojen suojaus ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysisen_turvallisuus #Omaisuudenhallinta	#Suojaaminen

### Hallintakeino

Toimistojen, tilojen ja laitteistojen fyysisen turvallisuus olisi suunniteltava ja toteutettava.

### Tarkoitus

Estetään luvaton fyysisen tunkeutuminen toimistoissa, huoneissa ja toimitiloissa oleviin organisaation tietoihin ja muihin niihin liittyviin omaisuuseriin sekä niiden vahingoittuminen ja toiminnan häiriointyminen.

### Ohjeistus

Toimistojen, tilojen ja laitteistojen suojauksessa olisi otettava huomioon seuraavat ohjeet:

- a) Korkeimman turvatason toimitilat olisi sijoitettava niin, etteivät satunnaiset henkilöt pääse niihin.
- b) Rakennusten olisi mahdollisuksien mukaan oltava huomiota herättämättömiä ja annettava mahdollisimman vähän tietoa niiden käyttötarkoituksesta, eikä rakennuksen ulko- tai sisäpuolella saisi olla ilmeisiä merkkejä tietojenkäsittelypalvelujen olemassaolosta.
- c) Toimitilat olisi toteutettava siten, etteivät luottamukselliset tiedot tai toiminnot ole näkyvissä tai kuultavissa ulkopuolelta. Myös sähkömagneettisen hajasäteilyn suojausta olisi harkittava, jos se katsotaan tarpeelliseksi
- d) Olisi varmistettava, että henkilöhakemistoja, sisäisiä puhelinluetteloita ja sisäverkossa olevia karttoja, joista ilmenee luottamuksellisten tietojenkäsittelypalvelujen sijaintitiedot, ei aseteta oikeudettomien henkilöiden saataville.

## Lisätiedot

Ei lisätietoja.

## 7.4 Fyysisen turvallisuuden valvonta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Fyysinen_turvallisuus	#Suosaaminen #Puolustus

### Hallintakeino

Toimitiloja olisi valvottava jatkuvasti luvattoman fyysisen pääsyn varalta.

### Tarkoitus

Havaitaan ja estetään luvaton fyysisen pääsy.

### Ohjeistus

Toimitiloja olisi valvottava valvontatoimilla, joita voivat olla esim. vartijat, rikosilmoitinlaitteistot, videovalvontajärjestelmät, kuten valvontakamerat, ja fyysisen turvallisuuden integroitu hallintajärjestelmä, jota hallitaan joko sisäisesti tai jota palveluntuottaja hallitsee.

Pääsyä kriittisiä järjestelmiä sisältäviin rakennuksiin olisi valvottava jatkuvasti, jotta voidaan havaita luvaton pääsy tai epäilyttävä toiminta

- Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.  
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulun käytöön.
- a) asentamalla videovalvontajärjestelmiä, kuten valvontakamerat, kuvaamaan ja tallentamaan kulkuaukkoja arkuunteisille alueille ja organisaation toimitilojen läheisyyteen
  - b) asentamalla sovellettavien standardien mukaisesti ja testaamalla säännöllisesti kosketus-, ääni- tai liikeantureita, jotka laukaisevat rikosilmoitinlaitteiston, kuten
    - 1) kontaktiin perustuvat hälytimet, jotka antavat hälytyksen, kun kontakti syntyy tai katkeaa (esim. ikkunassa, ovessa tai esineen alla)
    - 2) infrapunateknologiaan perustuvat liikkeentunnistimet, jotka antavat hälytyksen, kun jokin liikkuu niiden havaintoalueella
    - 3) lasin rikkoutumisesta syntyvän äänen havaitsevat anturit, jotka voivat antaa hälytyksen turvallisuushenkilöstölle
  - c) varustamalla kaikki ulko-ovet ja alimpien kerrostien ikkunat näillä hälyttimillä. Tyhjillään olevilla alueilla hälyttimien olisi oltava jatkuvasti päällä. Myös muut alueet (esim. tietojenkäsittely- ja tietoliikennelaitehuoneet) olisi suojahtava.

Valvontajärjestelmien suunnittelu olisi pidettävä luottamuksellisena, koska sen paljastuminen voi mahdollistaa huomaamatottomat murrot.

Valvontajärjestelmät olisi suojahtava luvattomalta käytöltä, jotta voidaan estää valvontatietojen, kuten videosyötteiden, luvaton käyttö tai järjestelmien etäkuljeminen.

Hälytysjärjestelmän ohjauspaneeli olisi sijoitettava hälytslaitteistolla suojaalle alueelle. Mikäli laitteella voidaan manuaalisesti tehdä hälytys, olisi se sijoitettava niin, että hälytyksen tekijän on turvallista poistua. Ohjauspaneelin ja anturien olisi oltava murrolta suojahtuja. Järjestelmä olisi testattava säännöllisesti, jotta voidaan varmistaa, että se toimii suunnitellusti etenkin, jos siinä on paristokäyttöisiä komponentteja.

Seuranta- ja tallennuslaitteita olisi käytettävä lakien ja viranomaismääräysten mukaisesti mukaan lukien tietosuoja ja henkilötietojen suojaamista koskeva lainsäädäntö. Tämä koskee etenkin henkilöstön seurantaa ja tallennettujen videoiden säilytsaikoja.

## Lisätiedot

Ei lisätietoja.

## 7.5 Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus	#Suojaaminen

### Hallintakeino

Olisi suunniteltava ja toteutettava suojaus fyysisiä ja ympäristön aiheuttamia uhkia, kuten luonnonkatastrofeja ja muita infrastruktuuriin kohdistuvia tahallisia tai tahattomia fyysisiä uhkia, vastaan.

### Tarkoitus

Estetään tai lievennetään fyysisien ja ympäristön aiheuttamien uhkien aiheuttamien tapahtumien seuraauksia.

### Ohjeistus

Riskien arvioinnit, joilla tunnistetaan fyysisien ja ympäristön aiheuttamien uhkien seuraukset, olisi tehtävä ennen kuin tärkeät toiminnot aloitetaan fyysisellä toimipaikalla sekä säännöllisin aikavälein. Olisi toteutettava tarpeelliset turvallisuusratkaisut ja uhkiin kohdistuvia muutoksia olisi seurattava. Olisi hankittava asiantuntijaneuvoja siitä, miten hallitaan fyysisien ja ympäristön aiheuttamien uhkien, kuten tulipalojen, tulvien, maanjäristysten, räjähdysten, mellakoiden ja muiden luonnollisten tai ihmisen aiheuttamien katastrofien, aiheuttamia riskejä.

Fyysisien toimitilojen sijainnissa ja rakentamisessa olisi otettava huomioon

- paikalliset maastonmuodot, kuten korkeus, vesistöt ja maanjäristysvyöhykkeet
- kaupunkiympäristöön liittyvät uhkat, kuten poliittista levottomuutta, rikollista toimintaa tai terroristi-iskuja houkuttelevat sijainnit.

Riskien arvioinnin tulosten perusteella olisi tunnistettava tärkeimmät fyysiset ja ympäristön aiheuttamat uhkat ja harkittava soveltuivia hallintakeinoja. Esimerkkejä:

- Tuli: Tulipalon havaitsevat järjestelmät asennetaan ja konfiguroidaan siten, että ne laukaisevat hälytyksen palon varhaisessa vaiheessa ja käynnistävät palonsammatusjärjestelmät, jotta voidaan estää tallennusvälineisiin ja niihin liittyviin tiedonkäsittelyjärjestelmiin kohdistuvat palovahingot. Palonsammatus olisi tehtävä ympäristön kannalta soveltuimmalla sammatusaineella (esim. kaasu suljetuissa tiloissa).
- Vesivahingot: Vesivahingot niiden varhaisessa vaiheessa havaitsevat järjestelmät asennetaan tallennusvälineitä tai tietojenkäsittelyjärjestelmiä sisältävien tilojen lattian alapuolelle. Vesipumppuja tai vastaavia ratkaisuja olisi oltava helposti saatavilla tulvimisen varalta.
- Virtapiikit: Otetaan käyttöön palvelin- ja asiakaspulosten tietojärjestelmiä virtapiikeiltä ja multta sähköhäiriöiltä suojaavat järjestelmät, jotta voidaan minimoida tällaisten tapahtumien seuraukset.
- Räjähteet ja aseet: Tehdään satunnaistarkastuksia räjähteiden tai aseiden varalta henkilöstölle, ajoneuvoille ja tavaroille, joita saapuu arkaluonteiseen tietojenkäsittelypalveluun.

### Lisätiedot

Kassakaapit ja muut turvalliset säilytystilat voivat myös suojata niissä säilytettyä tietoa onnettamuksilta, kuten tulipalolta, maanjäristykseltä, vesivahingolta tai räjähdykseltä.

Organisaatiot voivat toteuttaa rikosten ehkäisyä myös rakennetun ympäristön suunnittelulla. Hallintakeinot voidaan suunnitella suojaamaan tiloja ja vähentämään kaupunkiympäristössä tyypillisiä uhkia. Esimerkiksi kulkuesteiden ja puomien sijasta käytetyt patsaat tai vesialtaat toimivat sekä maisemointina että fyysisenä esteenä.

## 7.6 Turva-alueilla työskentely (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus	#Suojaaminen

### Hallintakeino

Olisi suunniteltava ja toteutettava menettelyt, joiden mukaisesti turva-alueilla työskennellään.

### Tarkoitus

Suojellaan turva-alueilla olevia tietoja ja niihin liittyviä omaisuuseriä kyseisillä alueilla työskentelevän henkilöstön aiheuttamalta vahingoittumiselta tai luvattomalta häirinnältä.

### Ohjeistus

Turva-alueilla työskentelyn turvallisuustoimien olisi koskettava koko henkilöstöä ja katettava kaikki turva-alueella tapahtuvat toiminnot.

Seuraavia ohjeita olisi noudatettava:

- Henkilöstön olisi oltava tietoinen turva-alueiden olemassaolosta tai toiminnasta siltä osin kuin se on tarpeen.
- Valvomatonta työskentelyä turva-alueilla olisi vältettävä turvallisuussyyistä ja jotta vähennetään tahallisen vahingollisen toiminnan mahdollisuksia.
- Turva-alueet, jotka ovat tyhjillään, olisi lukittava ja ne olisi tarkastettava säännöllisesti.
- Valokuva- tai videokameroiden tai äänitallentimien tai muiden tallennuslaitteistojen, kuten käyttäjän päätelaitteissa olevien kameroiden, käyttöä ei saisi sallia ilman lupaa.
- Käyttäjien päätelaitteiden turva-alueilla tapahtuvan kuljettamisen ja käytön hallinta.
- Palo- ja muussa hätätilanteessa noudatettavien menettelyiden asettaminen selkeästi näkyviin tai saataville.

### Lisätiedot

Ei lisätietoja.

## 7.7 Puhdas pöytä ja puhdas näyttö (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Fyysinen_turvallisuus	#Suojaaminen

### Hallintakeino

Olisi määriteltävä ja täytäntöönpanava papereita ja siirrettäviä tallennusvälineitä koskevat puhtaan pöydän säänöt sekä tietojenkäsittelypalveluja koskevat puhtaan näytön säänöt.

## Tarkoitus

Lievennetään pöydillä, näytöillä ja muissa saavutettavissa olevissa sijainneissa oleviin tietoihin kohdistuvia luvattoman käytön, menettämisen ja vahingoittamisen riskiä.

## Ohjeistus

Organisaation olisi laadittava puhdasta pöytää ja puhdasta näyttöä koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille olennaisille sidosryhmille.

Seuraavia ohjeita olisi noudatettava:

- a) Arkalouonteista tai kriittistä, esim. paperilla tai sähköisillä tallennusvälineillä olevaa, liiketoimintatietoa olisi säilytettävä lukitussa paikassa (mieluimmin kassakaapissa, kaapissa tai muussa lukittavassa kalusteessa), kun sitä ei tarvita. Tämä koskee erityisesti sitä, kun toimisto on tyhjänä.
- b) Käyttäjien päätelaitteita olisi suojahtava näppäinlukoilla tai muilla turvallisuusratkaisuilla, kun pääteleitteet eivät ole käytössä tai ne on jätetty valvomatta.
- c) Ilman valvontaa jäävät käyttäjien päätelaitteet olisi jätettävä siten, että niistä on kirjauduttu ulos tai ne on suojattu näytön ja näppäimistön lukitusmekanismilla, joka avataan niin, että käyttäjä tunnistetaan. Kaikkiin tietokoneisiin ja järjestelmiin olisi konfiguroitava aikakatkaisu tai automaattinen uloskirjautuminen.
- d) Käyttäjät olisi velvoitettava noutamaan tulosteensa välittömästi. Olisi syytä harkita tunnistautumistoiminnolla toimivien tulostimien käyttöä siten, että vain itse tulostaja voi saada tulosteensa ja vain ollessaan tulostimen luona.
- e) Arkalouonteista tietoa sisältävät asiakirjat ja siirrettävät tallennusvälineet olisi varastoitava turvallisesti ja tarpeellomiksi käyneet asiakirjat tai tallennusvälineet olisi hävitettävä turvallisella tavalla.
- f) Olisi laadittava näytölle tulevia ilmoituksia koskevat säännöt ja ohjeet (esim. uusista sähköpostiviesteistä tai muista viesteistä kertovat ilmoitukset olisi mahdollisuksien mukaan pantava pois päältä esitysten aikana, näyttöä jaettaessa tai julkisilla alueilla työskenneltäessä) ja viestittävä niistä.
- g) Arkalouoneiset tai kriittiset tiedot olisi poistettava valkotauluilta ja muun tyyppisiltä esityspinnoilta, kun tietoja ei enää tarvita.

Organisaatiolla olisi oltava menettelyt toimitiloista luopumiseen mukaan lukien lopputarkastus, jossa varmistetaan, ettei tiloihin jää mitään organisaation omaisuutta (esim. varmistetaan, ettei asiakirjoja ole tippunut vaikkapa kaapin taakse).

## Lisätiedot

Ei lisätietoja.

## 7.8 Laitteiden sijoitus ja suojaus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus #Omaisuudenhallinta	#Suojaaminen

## Hallintakeino

Laitteet olisi sijoitettava turvallisesti, ja niitä olisi suojahtava.

## Tarkoitus

Lievennetään fyysisten ja ympäristöstä aiheutuvien uhkien sekä luvattomasta käytöstä ja vahingoittumisesta aiheutuvaa riskiä.

## Ohjeistus

Laitteistojen suojaamisessa olisi otettava huomioon seuraavat ohjeet:

- a) Laitteet olisi sijoitettava siten, että turha pääsy työskentelyalueille estyy ja vältytään luvattomalta käytöltä.
- b) Arkaluonteista tietoa käsitlevät tietojenkäsittelypalvelut olisi sijoitettava huolellisesti siten, että vähennetään sen riskiä, että luvattomat henkilöt näkevät tietoa käytön aikana.
- c) Olisi otettava käyttöön hallintakeinoja, joilla pidetään mahdollisten fyysisten ja ympäristöstä aiheutuvien uhkien riski mahdollisimman pienenä (esim. varkaudet, tulipalo, räjähheet, savu, vesi ( tai vedensaannin häiriö), pöly, tärinä, kemialliset aineet, sähkönsaannin häiriö, tietoliikennehäirintä, sähkömagneettinen säteily ja vandalismi).
- d) Tietojenkäsittelypalvelujen läheisyydessä syömisenstä, juomisenstä ja tupakoinnista olisi laadittava ohjeet.
- e) Olisi tehtävä olosuhdevalvontaa, jotta haitallisesti tietojenkäsittelylaitteistojen toimintaan vaikuttava lämpötila ja kosteus kyötään havaitsemaan.
- f) Kaikki rakennukset ja kaikki saapuvat sähköjohdot ja viestikaapelit olisi suojahtava salamaa vastaan.
- g) Teollisuusympäristön laitteiden erityissuojausta, esimerkiksi näppäinkalvojen tarvetta, olisi harkittava.
- h) Luottamuksellista tietoa käsitlevät laitteet olisi suojahtava siten, että sähkömagneettisesta hajasäteilystä johtuva tietovuotoriski pidetään mahdollisimman pienenä.
- i) Organisaation hallinnassa olevien tietojenkäsittelypalvelujen olisi oltava fyysisesti erillään niistä, joita organisaatio ei hallinnoi.

## Lisätiedot

Ei lisätietoja.

## 7.9 Toimitilojen ulkopuolelle viedyn omaisuuden turvallisuus ([EN](#))

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus #Omaisuudenhallinta	#Suojaaminen

## Hallintakeino

Toimitilojen ulkopuolella olevaa omaisuutta olisi suojahtava.

## Tarkoitus

Estetään toimitilojen ulkopuolella olevan omaisuuden katoaminen, vahingoittuminen, varastaminen tai muunlainen vaarantuminen sekä organisaation toimintojen keskeytyminen.

## Ohjeistus

Kaikkia toimitilojen ulkopuolella käytettäviä laitteita, joissa säilytetään tai käsitellään tietoa (esim. mobiililaitteet), mukaan lukien organisaation omistamat laitteet sekä organisaation toiminnassa

käytettävät yksityisomisteiset laitteet (*bring your own device [BYOD]* eli käytetään omia laitteita) olisi tarpeen suojata. Johdon olisi hyväksyttävä näiden laitteiden käyttö.

Toimitilojen ulkopuolella käytettävien laitteiden, joissa säilytetään tai käsitellään tietoa, suojaamisessa olisi noudatettava seuraavia ohjeita:

- Toimitilojen ulkopuolelle vietyjä laitteita ja tallennusvälineitä ei jätetä valvomatta julkisiin tai turvattomiin paikkoihin.
- Laitteiden suojausta koskevia valmistajan ohjeita olisi noudatettava kaiken aikaa, esim. vahvoilta sähkömagneettisilta kentiltä, vedeltä, kuumuudelta, kosteudelta ja pölyltä suojaaminen.
- Kun toimitilojen ulkopuolella olevia laitteita siirretään eri yksilöiden tai sidosryhmien välillä, olisi ylläpidettävä lokia, jossa määritellään laitteen omistajuusketju ja joka sisältää tiedot ainakin laitteistoista vastaavien nimistä ja organisaatioista. Tiedot, joita ei ole tarpeen siirtää omaisuuserät mukana, olisi poistettava turvallisesti ennen siirtoa.
- Tarvittaessa ja mahdollisuksien mukaan kaikkien tietovälineiden siirtämiseen organisaation toimitiloista olisi hankittava lupa ja kaikista siirroista olisi pidettävä kirja, jotta voidaan ylläpitää kirjausketjua (ks. [kohta 5.14](#)).
- Laitteet (esim. mobiililaitteet tai kannettavat tietokoneet) olisi suojattava siltä, että tietoja on mahdollista nähdä esim. joukkoliikennevälitteessä. Tähän liittyvät riskit olisi otettava huomioon.
- Laitteille olisi tehtävä sijainnin seuranta ja mahdollistettava etätyhjennys.

Pysyvästi organisaation toimitilojen ulkopuolelle asennettuihin laitteisiin (kuten antenneihin tai pankkiautomaatteihin) voi kohdistua suurempi vaurioitumisen, varkauden tai salakuuntelun riski. Nämä riskit voivat vaihdella huomattavasti laitteiden sijainnin mukaan. Ne olisi siksi otettava huomioon suositeltavia hallintakeinoja arvioitaessa. Toimitilojen ulkopuolelle sijoitettavien laitteiden suojaamisessa olisi noudatettava seuraavia ohjeita:

- fysisen turvallisuuden valvonta (ks. [kohta 7.4](#))
- suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan (ks. [kohta 7.5](#))
- fyyysiseltä pääsyltä ja luvattomalta muuttamiselta suojaavat hallintakeinot
- kulkuoikeudet tiloihin.

## Lisätiedot

Lisätietoa tietojen tallennusvälineitä ja käsitellytlaiteita sekä käyttäjien päätelaitteita koskevista muista näkökohdista löytyy [kohdista 8.1](#) ja [6.7](#).

## 7.10 Tallennusvälineet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus #Omaisuudenhallinta	#Suojaaminen

### Hallintakeino

Tallennusvälineitä olisi hallittava koko niiden elinkaaren ajan aina hankinnasta, käyttöön, kuljettamiseen ja hävittämiseen organisaation luokitteluperiaatteiden ja käsitellyvaatimusten mukaisesti.

### Tarkoitus

Estetään tallennusvälineillä olevien tietojen luvaton paljastuminen, muuttuminen, poistaminen tai tuhoutuminen.

## Ohjeistus

### Siirrettävät tallennusvälineet

Siirrettävien tallennusvälineiden hallinnassa olisi noudatettava seuraavia ohjeita:

- a) Olisi laadittava siirrettäviä tallennusvälineitä koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikkia siirrettäviä tallennusvälineitä käyttäville tai käsitleville tahoille.
- b) Tarvittaessa ja mahdollisuksien mukaan kaikkien tallennusvälineiden siirtämiseen pois organisaatiosta olisi hankittava lupa ja kaikista siirroista olisi pidettävä kirja, jotta voidaan ylläpitää kirjausketjua.
- c) Kaikkia tallennusvälineitä olisi säilytettävä turvallisessa ja suojuissa ympäristössä niillä olevan tiedon turvaluokituksen, mukaisesti ja suojuilla niitä ympäristöstä aiheutuvilta uhkilta (kuten kuumuudelta, vedeltä, ilmankosteudelta, sähkökentiltä tai vanhenemiselta) valmistajan ohjeiden mukaisesti.
- d) Jos tiedon luottamuksellisuutta ja eheyttä pidetään tärkeinä näkökohtina, siirrettävillä tallennusvälineillä olevat henkilötiedot olisi suojahtava salaustekeikoiden avulla.
- e) Jotta tieto ei muutu käytökelvottomaksi sen tallennusmedian ajan kuluessa tapahtuvan heikkenemisen myötä, olisi tiedon luettavuus säilytettävä siirtämällä se toiselle fyysiselle tallennusmedialle.
- f) Arvokkaasta tiedosta olisi säilytettävä useampia kopioita erillisillä tallennusvälineillä yhtäaikaisen tiedon vahingoittumisen tai katoamisen riskin pienentämiseksi.
- g) Siirrettävien tallennusvälineiden rekisterointiä olisi harkittava, jotta voidaan rajoittaa tietohävikin mahdollisuutta.
- h) Siirrettävien tallennusvälineiden porttien (esim. SD-korttipaikkojen ja USB-porttien) käyttö olisi sallittava vain silloin, kun niiden käyttöön on organisaatioon liittyvä peruste.
- i) Kun on tarve käyttää siirrettäviä tallennusvälineitä, olisi tiedon siirtämistä tällaisille tallennusvälineille valvottava.
- j) Tieto voi fyysisen kuljetuksen aikana altistua luvattomalle käytölle, väärinkäytölle tai vääristymiselle esimerkiksi silloin, kun tallennusvälineitä lähetetään posti- tai lähettilpalvelujen kautta.

Tässä hallintakeinossa tallennusvälineiksi lasketaan myös paperiset asiakirjat. Kun fyysisiä tallennusvälineitä siirretään, olisi noudatettava [kohdassa 5.14](#) esitettyjä turvallisustointia.

### Laitteiden turvallinen kierrättäminen ja käytöstä poistaminen

Tallennusvälineiden turvallista hävittämistä tai kierrättämistä varten olisi laadittava muodolliset menettelyt, jotta riski siitä, että luottamuksellista tietoa paljastuu luvattomille tahoille, pysyy mahdollisimman pienenä. Luottamuksellista tietoa sisältävien tallennusvälineiden turvallisen hävittämisen tai kierrättämisen menettelyjen olisi oltava oikeassa suhteessa tiedon arkaluonteisuuteen. Seuraavat seikat olisi otettava huomioon:

- a) Jos luottamuksellista tietoa sisältäviä tallennusvälineitä on tarpeen kierrättää uuteen käyttöön organisaation sisällä, olisi tiedot poistettava tai tallennusväline alustettava turvallisesti ennen uudelleenkäyttöä (ks. [kohta 8.10](#)).
- b) Luottamuksellista tietoa sisältävät tallennusvälineet olisi hävitettävä turvallisesti, kun niitä ei enää tarvita (esim. tuhoamalla, silppuamalla tai poistamalla sisältö turvallisesti).
- c) Turvallista hävittämistä edellyttävien tallennusvälineiden tunnistamiseen olisi oltava menettelyt.
- d) Monilla organisaatioilla on tallennusvälineiden keräys- ja hävityspalvelut, mutta soveltuva ulkoinen toimittaja olisi valittava tarkasti hallintakeinojen ja kokemuksen perusteella.

- e) Arkaluonteisten kohteiden hävittäminen olisi mahdollisuksien mukaan kirjattava, jotta kyetään ylläpitämään kirjausketjua.
- f) Kun tallennusvälineitä kerätään hävittämistä varten, olisi kiinnitettävä huomiota tiedon kasautumisen vaikutukseen. Sen seurauksena suuresta määristä tietoa, joka ei ole arkaluonteista, saattaa tulla arkaluonteista.

Vaurioituneille tallennusvälineille, jotka sisältävät arkaluonteista tietoa, olisi tehtävä riskien arvointi. Näin voidaan määrittää, pitäisikö välineet tuhota fyysisesti sen sijaan, että ne korjattaisiin tai poistettaisiin käytöstä (ks. [kohta 7.14](#)).

#### Lisätiedot

Kun tallennusvälineellä oleva luottamuksellinen tieto on salaamatonta, olisi kyseiselle tallennusvälineelle harkittava ylimääräistä fyysisen suojaksen kerrosta.

### 7.11 Tukipalvelut (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Eheys #Saatavuus	#Suojaus #Havainto	#Fyysinen_turvallisuus	#Suojaaminen

#### Hallintakeino

Tietojenkäsittelypalvelut olisi suojattava sähkökatkoilta ja multa tukipalveluiden vikojen aiheuttamilta häiriöiltä.

#### Tarkoitus

Estetään tietojen ja niihin liittyvien omaisuuserien menettäminen, vahingoittuminen tai vaarantuminen sekä tukipalveluiden vikaantumisista ja häiriöstä johtuva organisaation toimintojen keskeytyminen.

#### Ohjeistus

Organisaatioiden tietojenkäsittelypalveluiden toiminta on riippuvalista peruspalveluista (kuten sähköstä, tietoliikenteestä, vedenjakelusta, viemäröinnistä, lämmityksestä, tuuletuksesta ja ilmastoinnista). Tästä syystä organisaation olisi

- a) varmistettava, että peruspalveluita tukevat laitteistot on konfiguroitu ja että niitä käytetään ja ylläpidetään valmistajan olennaisten määritysten mukaisesti
- b) varmistettava, että tukipalvelut arvioidaan säännöllisesti, jotta voidaan varmistaa, että niiden kapasiteetti kattaa liiketoiminnan kasvun ja että ne toimivat yhdessä muiden peruspalvelujen kanssa
- c) varmistettava, että yleishyödylliset palvelut tarkastetaan ja testataan säännöllisesti, jotta voidaan varmistaa, että ne toimivat kunnolla
- d) tarvittaessa toteutettava hälytysmekanismit, jotka havaitsevat peruspalveluiden toimintahäiriöt
- e) tarvittaessa varmistettava, että peruspalveluilla on useampia eri fyysisiä reittejä kulkevia syöttölinjoja
- f) varmistettava, että peruspalveluita tukevat laitteistot ovat tietojenkäsittelypalveluista erillisessä verkossa, jos ne on kytketty verkoon
- g) varmistettava, että peruspalveluita tukevat laitteistot on yhdistetty internettiin vain tarvittaessa ja vain suojustusti.

Olisi hankittava hätävalaistus ja -viestintävälineet. Sähkon, veden, kaasun tai muiden peruspalveluiden hätäkatkaisinten ja -venttiilien olisi sijaittava lähellä hätäuloskäyntejä tai laitetiloja. Hätätilannekontaktien yhteystiedot olisi kirjattava ja niiden olisi oltava henkilöstön saatavilla katkoksen aikana.

## Lisätiedot

Tietoliikenneverkon vikasietoisuutta voidaan parantaa entisestään hankkimalla peruspalvelut useamman reitin ja useamman palveluntuottajan kautta.

### 7.12 Kaapeloinnin turvallisuus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Saatavuus	#Suojaus	#Fyysisen_turvallisuus	#Suojaaminen

#### Hallintakeino

Sähkökaapelointi sekä tietoa siirtävä tai tietotekniikkapalveluita tukeva tietoliikennekaapelointi olisi suojattava salakuuntelulta, häirinnältä ja vahingoittumiselta.

#### Tarkoitus

Estetään tietojen ja niihin liittyvien omaisuuserien sähkö- ja tietoliikennekaapelinneista johtuva menettäminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toimintojen keskeytyminen.

#### Ohjeistus

Kaapeloinnin turvallisuudessa olisi otettava huomioon seuraavat ohjeet:

- Tietojenkäsittelypalveluiden sähkö- ja tietoliikennekaapelointien olisi mahdollisuksien mukaan oltava maan alla tai niitää olisi suojattava muilla keinoilla, kuten suojaamalla lattialla kulkevat kaapelit ja nostamalla ne kulkemaan pylväissä. Maan alla kulkevia kaapeleita olisi suojattava tahattomalta katkaisemiselta (esim. vahvennetuilla asennusputkilla tai sijainnin ilmaisemisella).
- Sähkökaapelit olisi eristettävä tietoliikennekaapeleista, jotta vältytään häiriöiltä.
- Arkaluonteisten ja kriittisten järjestelmien suojaussa olisi harkittava seuraavia hallintakeinoja:
  - vahvennettujen asennusputkien asentaminen ja lukitut huoneet tai kaapit ja hälyttimet tarkastus- ja päätekohtiin
  - kaapelien sähkömagneettinen suojaaminen
  - luvattomasti kaapeleihin liitettyjen laitteiden selvittäminen tietoteknisin keinoin tai fyysisellä tarkastuksella
  - valvottu pääsy asennuspaneeliin ja tietoliikenteen kytkentätiloihin (esim. mekaaniset avaimet tai PIN-tunnukset)
  - valokuitukaapelien käyttö.
- Kaapelien merkitseminen molemmissa päässä riittävillä lähtö- ja päätapaikan tiedoilla, jotta voidaan mahdollistaa kaapelin fyysinen tunnistaminen ja tarkastaminen.

Kaapelointiin liittyvien häiriötilanteista tai toimintahäiriöistä aiheutuvien riskien hallintaan olisi hyödynnettävä asiantuntijoiden neuvoja.

#### Lisätiedot

Toisinaan sähkö- ja tietoliikennekaapeloinnit ovat useamman samassa toimipaikassa sijaitseva organisaation jaettuja resursseja.

## 7.13 Laitteiden huolto (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvallisuus #Omaisuuden-hallinta	#Suojaaminen #Kriisinkestävyys

### Hallintakeino

Laitteita olisi huollettava asianmukaisesti, jotta tietojen saatavuus, eheys ja luottamuksellisuus voidaan varmistaa.

### Tarkoitus

Estetään tietojen ja niihin liittyvien omaisuuserien huollon puutteesta johtuva menettäminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toimintojen keskeytyminen.

### Ohjeistus

Laitteistoja huollettaessa olisi otettava huomioon seuraavat ohjeet:

- a) Laitteistoja olisi huollettava toimittajan suosittelemien aikavälein ja sen määrittelyjä noudattaen.
- b) Organisaation olisi toteutettava huolto-ohjelma ja valvottava sen noudattamista.
- c) Vain pätevän henkilöstön olisi tehtävä korjaukset ja huollot.
- d) Kaikista epäillyistä ja sattuneista vioista sekä ehkäisevistä ja korjaavista toimenpiteistä olisi pidettävä kirjaaa.
- e) Kun laitteistolle on suunniteltu tehtäväksi huolto, olisi toteutettava asianmukaiset hallintakeinot ottaen huomioon, tekeekö huollon paikan päällä oleva henkilöstö vai organisaation ulkopuolinens taho. Huoltohenkilöstön olisi allekirjoitettava salassapitosopimukset.
- f) Toimipaikassa huoltoa tekevää huoltohenkilöstöä olisi valvottava.
- g) Etähuollon käyttö olisi hyväksytävä ennakolta ja sen käyttöä olisi valvottava.
- h) Toimitilojen ulkopuolelle viedyn omaisuuden turvallisuutta (ks. [kohta 7.9](#)) koskeva hallintakeinoa olisi käytettävä, jos tietoa sisältäviä laitteita viedään huoltoa varten toimitilojen ulkopuolelle.
- i) Vakuutusten edellyttämät huollot olisi tehtävä.
- j) Laitteet olisi tarkastettava ennen huollon jälkeistä käyttöönnottoa, jotta voidaan varmistaa, ettei laitteita ole muutettu luvattomasti ja että ne toimivat kunnolla.
- k) Laitteiden turvallinen käytöstä poistamista ja kierrättämistä (ks. [kohta 7.14](#)) koskeva hallintakeinoa olisi käytettävä, jos laitteistoja joudutaan hävittämään.

### Lisätiedot

Laitteistoja ovat esim. tietojenkäsittelypalveluiden tekniset osat, katkoton tehonsyöttö (UPS) ja akut, sähkögeneraattorit, laturit ja muuntimet (taajuus, vaihto/tasavirta, jännite), fyysiset tunkeutumisen havaitsemisjärjestelmät ja -hälyttimet, savunilmaisimet, palonsammuttimet, ilmastointi ja hissit.

## 7.14 Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvalisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Fyysisen_turvallisuus #Omaisuudenhallinta	#Suojaaminen

### Hallintakeino

Laitteiden tallennettua tietoa sisältävät osat olisi tarkistettava, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmistot on poistettu tai tuhottu turvallisesti ennen laitteen käytöstä poistamista tai kierrättämistä.

### Tarkoitus

Estetään tietojen vuotaminen käytöstä poistettavista tai kierrätettävistä laitteista.

### Ohjeistus

Laitteet olisi tarkistettava ennen käytöstä poistamista tai kierrättämistä, jotta voidaan varmistaa, sisältävätkö ne tallennusvälineitä.

Luottamuksellista tai tekijänoikeuksien alaista tietoa sisältävät tallennusvälineet olisi tavanomaisen tiedon poistamisen sijasta tuhottava fyysisesti tai tieto olisi tuhottava, poistettava tai päälekirjoitettava käyttäen tekniikoita, jotka tekevät alkuperäisen tiedon palauttamisen mahdottomaksi. [Kohdassa 7.10](#) on tarkempaa ohjeistusta tallennusvälineiden turvallisesta hävittämisestä ja [kohdassa 8.10](#) tietojen poistamisesta.

Organisaation, omistajan, järjestelmän tai verkon tai laitteen sisältäneen tiedon ilmaisevat merkinnät olisi poistettava ennen käytöstä poistamista, koskien myös uudelleen myytäviä ja hyväntekeväisyteen lahjoitettavia laitteita.

Organisaation olisi harkittava turvallisuuden hallintalaitteiden, kuten kulunvalvonnan ja muiden valvontalaitteiden, poistamista leasingsopimuksen päätyessä tai kun toimipaikkaa vaihdettaessa. Tämä riippuu eri tekijöistä, kuten siitä

- edellytetäänkö leasingsopimussa, että toimipaikka palautetaan alkuperäiseen kuntoon
- että pyritään minimoimaan riski, että seuraavalle vuokralaiselle jää arkaluonteista tietoa sisältäviä järjestelmiä (esim. käyttäjäluetelot, video- tai kuvatiedostojen)
- voidaanko hallintakeinoja käyttää myös seuraavassa toimipaikassa.

### Lisätiedot

Vaurioituneille laitteistoille, jotka sisältävät tallennusvälineitä, voidaan joutua tekemään riskien arvionti. Näin voidaan määrittää, olisiko välineet tuhottava fyysisesti sen sijaan, että ne korjattaisiin tai poistettaisiin käytöstä. Tieto voi vaarantua, jos laitteet poistetaan käytöstä huolimattomasti tai kierrätetään varomattomasti.

Turvallisen levyn tyhjentämisen lisäksi koko levyn salaaminen vähentää luottamuksellisen tiedon paljastumisen riskiä, kun laitteet poistetaan käytöstä tai käytetään uudelleen, kunhan

- käytetty tietojen salaus on riittävän vahva ja kattaa koko levyn (mukaan lukien käytämätön varattu tila ja heittovaihtotiedostot)
- salausavaimet ovat riittävän pitkiä kestämään väsytyshyökkäyksen (*brute-force attack*)
- salausavaimet pidetään luottamuksellisina (esim. niitä ei koskaan tallenneta samalle levylle).

Salausta käsitellään tarkemmin [kohdassa 8.24](#).

Tallennusvälineen turvallinen ylikirjoittaminen saattaa vaihdella tallennusvälineen teknologiasta ja tallennusvälineessä olevien tietojen luokitustasosta riippuen. Ylikirjoittamistyökalut olisi katselmoitava, jotta voidaan varmistaa, että niitä voidaan käyttää tallennusvälineen teknologiaan.

Lisätietoja tallennusvälineiden puhdistamisesta löytyy standardista ISO/IEC 27040.

## 8 Teknologiset hallintakeinot (EN)

### 8.1 Käyttäjien päätelaitteet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvalli-suuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen	#Suojaaminen

#### Hallintakeino

Käyttäjien päätelaitteille tallennetut, niillä käsiteltävät tai niiden kautta käytettävät tiedot olisi suojattava.

#### Tarkoitus

Suojellaan tietoa riskeiltä, jotka ovat seurausta käyttäjien päätelaitteiden käytöstä.

#### Ohjeistus

##### Yleistä

Organisaation olisi laadittava käyttäjien päätelaitteiden turvallista konfigurointia ja käsitellyä koskevat kohdennetut toimintaperiaatteet ja viestittävä niistä kaikille olennaisille henkilöstön jäsenille ja sidosryhmille sekä otettava seuraavat asiat huomioon:

- a) sen tiedon tyyppi ja luokitustaso, jota käyttäjien päätelaitteilla voidaan käyttää, käsitellä, varastoida tai tukea
- b) käyttäjien päätelaitteiden rekisteröinti
- c) fyysisä suojaamista koskevat vaatimukset
- d) ohjelmistojen asentamisen rajoittaminen (esim. järjestelmän pääkäyttäjät etääsentavat)
- e) käyttäjien päätelaitteilla olevia ohjelmistoja (esim. ohjelmistoversioita) ja päivitysten asentamista (esim. aktiivinen automaattinen päivittäminen) koskevat vaatimukset
- f) tietopalveluihin, julkisiin verkkoihin tai mihin tahansa muihin toimitilojen ulkopuolisiiin verkkoihin yhdistämistä koskevat säännöt (esim. vaatimus henkilökohtaisen palomuurin käytöstä)
- g) pääsynhallinta
- h) tallennusvälineiden salaus
- i) haittaohjelmilta suojaaminen
- j) etänä tehty käytöstä poistaminen, tietojen poistaminen tai -lukitseminen
- k) varmuuskopointi
- l) verkkopalveluiden ja verkkosovellusten käyttö
- m) loppukäyttäjien käyttäytymisen analysointi (ks. [kohta 8.16](#))

- n) siirrettävien laitteiden, kuten siirrettävien muistilaitteiden, käyttö sekä mahdollisuus fyysisen porttien (esim. USB-porttien) käytöstä poistamiseen
- o) ositustoimintojen käyttö, jos käyttäjien päätelaitteet tukevat sitä, koska siten pystytään turvallisesti erottamaan organisaation tiedot ja niihin liittyvät omaisuuserät (kuten ohjelmistot) laitteella olevista muista tiedoista ja niihin liittyvistä omaisuuseristä.

Olisi tarkasteltava myös sitä, ovatko jotkin tiedot niin arkaluonteisia, että niitä voidaan ainoastaan tarkastella käyttäjien päätelaitteilla mutta ei tallentaa niille. Näissä tapauksissa laiteeseen voidaan tarvita teknisiä lisävarmistuksia, kuten sen varmistaminen, että tiedostojen lataaminen verkkoyhteydettömään työskentelyyn on poistettu käytöstä ja että paikallisten tallennusvälineiden, kuten SD-korttien, käyttö on estetty.

Tämän hallintakeinon suosituksia olisi mahdollisuksien mukaan täytäntöönpanava konfiguraationhallinnan (ks. [kohta 8.9](#)) tai automatisoitujen työkalujen avulla.

#### Käyttäjän vastuu

Kaikki käyttäjät olisi saatettava tietoisiksi turvallisuusvaatimuksista ja menettelyistä, joilla suojataan käyttäjien päätelaitteita, samoin kuin velvollisuudestaan pitää yllä turvallisuustoimia. Käyttäjiä olisi ohjattava

- a) kirjautumaan ulos aktiivisista istunnoista tai sammuttamaan palvelut, kun niitä ei enää tarvita
- b) suojaamaan päätelaitteitaan luvattomalta käytöltä fyysisillä hallintakeinoilla (esim. näppäinlukoilla tai erikoislukoilla) ja loogisilla hallintakeinoilla (esim. salasanaan perustuvalla pääsyllä), kun niitä ei käytetä, sekä olemaan jättämättä tärkeitä, arkaluonteisia tai kriittisiä liiketoimintatietoja sisältäviä laitteita ilman valvontaa
- c) käytämään laitteita erityisen huolellisesti julkisilla paikoilla, avoimissa toimistoissa, tapaamispalstoissa ja muissa suojaamattomissa paikoissa (esim. arkaluonteisten tietojen lukemisen välttäminen, jos tietoja voidaan lukea käyttäjän selän takaa, katselusuojien käyttö)
- d) suojaamaan päätelaitteitaan fyysisesti varkauksilta (esim. autoissa ja muissa liikennevälineissä, hotellihuoneissa, kokouskeskuksissa ja tapaamispalstoissa).

Käyttäjien päätelaitteiden varkautta tai katoamista varten olisi laadittava erityinen menettely, jossa otetaan huomioon lakeihin, asetuksiin, sopimuksiin (esim. vakuutuksiin) liittyvät ja organisaation omat turvallisuusvaatimukset.

#### Henkilökohtaisten laitteiden käyttö

Jos organisaatio sallii henkilökohtaisten laitteiden käytön (*bring your own device [BYOD]* eli omien laitteiden käytön), tässä hallintakeinossa annettujen ohjeiden lisäksi olisi otettava huomioon

- a) laitteiden henkilökohtaisen ja työkäytön erottamisen, mukaan lukien sellaisen ohjelmiston käyttö, joka tukee kyseisenlaista erottelua ja suojaaa henkilökohtaisella laitteella olevia liiketoimintatietoja
- b) sallia pääsy liiketoimintatietoihin vasta sen jälkeen, kun käyttäjät ovat ilmaisseet ymmärtävänsä vastuunsa (fyysinen suojaaminen, ohjelmistojen päivitys jne.), jossa he luopuvat liiketoimintatietojen omistajuudesta ja hyväksyvät organisaation suorittaman tiedon etäpyyhkimisen, jos laite varastetaan tai häviää tai kun käyttäjällä ei ole enää oikeutta käyttää palvelua; näissä tilanteissa myös henkilötietojen suojaamista koskevat lait olisi otettava huomioon
- c) kohdennetut toimintaperiaatteet ja menettelyt ehkäisemään henkilökohtaisella laitteistolla kehitetyn aineettoman omaisuuden oikeuksia koskevat kiistat
- d) pääsy henkilökohtaisiin laitteisiin (laitteen turvallisuuden varmentamiseksi tai tutkinnan yhteydessä), minkä lainsäädäntö saattaa estää
- e) ohjelmistolisen sisopimukset, joiden mukaan organisaatiot saattavat olla vastuussa asiakasohjelmistolisen sisestä, jotka ovat henkilöstön jäsenten tai ulkopuolisten osapuolten käyttäjien henkilökohtaisesti omistamissa käyttäjien päätelaitteissa.

### Langattoman yhteydet

Organisaation olisi luotava menettelyt

- laitteiden langattomien yhteyksien konfigurointiin (esim. haavoittuvien protokollien estäminen)
- asianmukaisen kaistanleveyden langattomien tai langallisten yhteyksien käyttö kohdennettujen toimintaperiaatteiden mukaisesti (esim. koska tarvitaan varmuuskopointia tai ohjelmistopäivityksiä).

### Lisätiedot

Käyttäjien päätelaitteilla olevien tietojen suojaamisen hallintakeinot riippuvat siitä, käytetäänkö käyttäjän päätelaitetta vain organisaation turvallisissa tiloissa ja sen turvallisivat verkoyhteyksin vai kohdistuuko siihen suurempi fyysisiin seikkoihin tai verkkoihin liittyvä uhka organisaation ulkopuolella.

Käyttäjien päätelaitteiden langattomat yhteydet ovat samantapaisia kuin muut verkoyhteydet, mutta niissä on tärkeitä eroja, jotka olisi otettava huomioon hallintakeinoja yksilöitääessä. Etenkin käyttäjien päätelaitteisiin tallennettujen tietojen varmuuskopointi saattaa toisinaan epäonnistua, koska verkon kaistanleveys on rajoitettu tai koska käyttäjien päätelaitteet eivät välttämättä ole yhteydessä verkkoon, kun varmuuskopointi olisi tarkoitus tehdä.

Joidenkin USB-porttien, kuten USB-C-porttien, käyttöä ei ole mahdollista estää, koska sitä käytetään muihin tarkoituksiin (esim. virransyöttö ja näytösignaali).

## 8.2 Ylläpito-oikeudet (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti- ja käyttövaltuushallinta	#Suojaaminen

### Hallintakeino

Ylläpito-oikeuksien jakamista ja käyttöä olisi rajoitettava ja hallittava.

### Tarkoitus

Varmistetaan, että vain luvallisille käyttäjille, ohjelmistokomponenteille ja palveluille on myönnetty ylläpito-oikeudet.

### Ohjeistus

Ylläpito-oikeuksien jakamista olisi hallittava valtuutusprosessilla pääsynhallintaa koskevien asianmukaisten kohdennettujen toimintaperiaatteiden mukaisesti (ks. [kohta 5.15](#)). Seuraavat seikat olisi otettava huomioon:

- Olisi yksilöitvä käyttäjät, jotka tarvitsevat ylläpito-oikeudet kuhunkin järjestelmään tai prosessiin (esim. käyttöjärjestelmiin, tietokannanhallintajärjestelmiin ja sovelluksiin).
- Ylläpito-oikeudet olisi myönnettävä käyttäjille tarpeen mukaan ja tapauskohtaisesti pääsynhallintaa (ks. [kohta 5.15](#)) koskevien kohdennettujen toimintaperiaatteiden mukaisesti (eli vain henkilölle, joilla on tarvittava pätevyys tehdä tehtävät, jotka vaativat ylläpito-oikeudet, ja nällekin vain toiminnallisten rooliensa vaatimat vähimmäisoikeudet).
- Valtuutusprosessia olisi ylläpidettävä (eli sen määrittäminen, kuka voi hyväksyä ylläpito-oikeuksien myöntämisen tai ylläpito-oikeuksien antamisen vasta, kun valtuutusprosessi on viety loppuun), ja kaikki myönnetyt ylläpito-oikeudet olisi kirjattava.
- Ylläpito-oikeuksien päättymistä koskevat vaatimukset olisi määriteltävä ja toteutettava.
- Olisi toteuttava toimet, joilla varmistetaan, että käyttäjät ovat tietoisia omista ylläpito-oikeuksistaan sekä siitä, milloin he toimivat ylläpitotilassa. Mahdollisia toimia ovat esim. määriteltyjen käyttäjäidentiteettien, käyttöliittymän asetusten tai jopa tiettyjen laitteistojen käyttö.

- f) Ylläpito-oikeuksien tunnistautumista koskevat vaatimukset voivat olla tiukempia kuin normaaleja pääsyoikeuksia koskevat vaatimukset. Ennen ylläpito-oikeuksien käyttöön saatetaan vaatia uudelleentunnistautuminen tai vahvempi tunnistautuminen.
- g) Ylläpito-oikeuksien käyttäjät olisi katselmoitava säännöllisesti ja aina organisaation muutosten jälkeen, jotta voidaan varmistaa, että heidän tehtävänsä, roolinsa, vastuunsa ja pätevyysensä oikeuttavat yhä ylläpito-oikeuksien käyttämisen (ks. [kohta 5.18](#)).
- h) Olisi laadittava säännöt, joilla vältetään geneeristen ylläpitotunnusten (kuten 'root') käyttö järjestelmien konfiguraatiomahdollisuuden huomioiden. Tällaisten tunnusten tunnistautumistietoja olisi hallittava ja suojatava (ks. [kohta 5.17](#)).
- i) Olisi myönnettävä tilapäisiä ylläpito-oikeuksia hyväksytyjen muutosten tai toimintojen (esim. huoltotoimintojen tai jonkin kriittisen muutoksen) suorittamisen ajaksi ennenmin kuin pysyviä ylläpito-oikeuksia. Tätä kutsutaan usein lasirikkomenettelyksi, ja usein se tehdään automatisoidulla ylläpito-oikeuksien hallinnan välineillä.
- j) Kaikki järjestelmän käytökerrat ylläpito-oikeuksilla olisi kirjattava auditointitarkoituksesta varten.
- k) Ylläpito-oikeuksin varustettuja identiteettejä ei saisi jakaa ja yhdistää useammille henkilöille, vaan olisi myönnettävä kullekin henkilölle erillinen identiteetti, mikä mahdollistaa kohdennettujen ylläpito-oikeuksien myöntämisen. Identiteeteistä voidaan muodostaa ryhmiä (esim. pääkäyttäjät), mikä yksinkertaistaa ylläpito-oikeuksien hallintaa.
- l) Ylläpito-oikeuksin varustettuja tunnuksia pitäisi käyttää vain ylläpitotehtäviin, muihin kuin päivittäisiin yleisiin tehtäviin (eli ei sähköpostin tarkistamiseen tai verkon selailuun, vaan niitä varten käyttäjillä olisi oltava erilliset verkkoidentiteetit).

## Lisätiedot

Ylläpito-oikeudet ovat tunnuksille, roolille tai prosessille myönnetyjä pääsyoikeuksia, jotka mahdollistavat sellaisten tehtävien tekemisen, joita normaalit käyttäjät tai prosessit eivät pysty tekemään. Järjestelmävastaavien ja pääkäyttäjien roolit vaativat yleensä ylläpito-oikeudet.

Pääkäyttäjän ylläpito-oikeuksien (minkä tahansa tietojärjestelmän ominaisuuden tai palvelun, joka sallii käyttäjän ohittavan järjestelmän tai sovelluksen hallintakeinot) asian käyttö on merkittävä tekijä järjestelmää koskevien häiriötilanteiden tai tietomurtojen takana.

Lisätietoa pääsynhallinnasta sekä tieto- ja viestintäteknisiä teknologiresursseja koskevasta pääsyn turvallisesta hallinnasta löytyy standardista ISO/IEC 29146.

## 8.3 Tietoihin pääsyn rajoittaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttöövaltuushallinta	#Suojaaminen

## Hallintakeino

Pääsyä tietoihin ja muihin niihin liittyviin omaisuuseriin olisi rajoitettava pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden mukaisesti.

## Tarkoitus

Varmistetaan pelkkä luvallinen pääsy tietoihin ja muihin niihin liittyviin omaisuuseriin sekä estetään luvaton pääsy niihin.

## Ohjeistus

Pääsyä tietoihin ja muihin niihin liittyviin omaisuuseriin olisi rajoitettava kohdennettujen toimintaperiaatteiden mukaisesti. Pääsyrajoitusvaatimusten tueksi olisi harkittava seuraavia asioita:

- a) Tuntemattomille käyttäjäidentiteeteille tai anonymeille käyttäjille ei sallita pääsyä arkaluonteisiin tietoihin. Julkinen tai anonymi pääsy olisi mahdollistettava vain sellaisiin varastointipaikkoihin, joissa ei säilytetä arkaluonteisia tietoja.
- b) Toteutetaan konfiguraatiomekanismit, joiden avulla hallitaan pääsyä järjestelmissä, sovelluksissa ja palveluissa oleviin tietoihin.
- c) Hallitaan sitä, mihin tietoihin kullakin käyttäjällä on pääsy.
- d) Hallitaan sitä, millä identiteeteillä tai identiteettijoukoilla on mitkäkin oikeudet, kuten luku-, kirjoitus-, poisto- ja suorittamisoikeudet.
- e) Toteutetaan fyysinen ja ohjelmallinen pääsynhallinta, jolla eriytetään arkaluonteiset sovellukset, sovellustiedot tai järjestelmät.

Organisaatiolle arvokkaiden arkaluonteisten tietojen suojaaksi olisi harkittava tarkempia, dynaamisia pääsynhallintateknikoita ja -prosesseja, kun organisaatio

- a) tarvitsee tarkemman hallinnan siihen, kenellä on pääsy tällaiseen tietoon, millä ajanjaksolla ja millä tavoin
- b) haluaa jakaa tällaista tietoa organisaation ulkopuolisille ihmisiille mutta säilyttää hallinnan siihen, kuka pääsee tietoihin käsiksi
- c) haluaa hallita dynaamisesti ja reaalialkaisesti tällaisten tietojen käyttöä ja jakelua
- d) haluaa suojella tällaista tietoa luvattomalta muuttamiselta, kopioimiselta ja jakelulta (myös tulostamiselta)
- e) haluaa valvoa tietojen käyttöä
- f) haluaa tallentaa kaikki tällaisiin tietoihin tehtävät muutokset siltä varalta, että muutoksia on tarpeen tutkia tulevaisuudessa.

Tietoja olisi suojatta dynaamisilla pääsynhallintateknikoilla koko niiden elinkaaren ajan (eli luotaessa, käsittelyssä, varastoitaessa, siirrettäessä ja hävitettäessä). Tämä sisältää

- a) dynaamista pääsynhallintaa koskevien sääntöjen laatimisen tarkempien käyttötapausten pohjalta tarkastellen
  - 1) pääsyoikeuksien myöntämistä identiteetin, laitteen, sijainnin tai sovelluksen perusteella
  - 2) luokitteluperiaatteiden hyödyntämistä sen määrittämisessä, mitä tietoja on suojattava dynaamisilla pääsynhallintateknikoilla
- b) käyttöä, valvontaa ja raportointia koskevien prosessien tukevan teknisen infrastruktuurin luomisen.

Dynaamisten pääsynhallintajärjestelmien olisi suojattava tietoja

- a) edellyttämällä tunnistautumista, asianmukaisia oikeuksia tai lupaa tietoihin pääsyn
- b) rajoittamalla pääsy esim. tiettyyn ajanjaksoon (esim. tietyn päivän jälkeen tai tiettyyn päivään asti)
- c) käytämällä salaustekniikoita

- d) määrittelemällä tietoja koskevat tulostusluvat
- e) tallentamalla tietojen käyttäjät ja käyttötavat
- f) tekemällä hälytyksen, jos tietojen väärinkäytöryityksiä havaitaan.

### Lisätiedot

Dynaamisilla pääsynhallintatekniikoilla ja muilla tietojen dynaamisilla suojausteknologioilla voidaan tukea tietojen suojaamista jopa silloin, kun tietoa jaetaan sen luoneen tahon ulkopuolelle, jolloin perinteistä pääsynhallintaa ei voida toteuttaa. Niitä voidaan soveltaa asiakirjoihin, sähköposteihin tai muihin tieto sisältäviin tiedostoihin, jotta voidaan rajoittaa sitä, kenellä on pääsy sisältöön ja miten. Se voi olla eri tarkkuustasoilla ja sitä voidaan mukauttaa tietojen elinkaareen aikana.

Dynaamiset pääsynhallintatekniikat eivät korvaa perinteistä pääsynhallintaa (esim. pääsynhallintalistojen käytöä), mutta se voi lisätä siihen ominaisuuksia, jotka voivat koskea ehdollisuutta, reaalialaista arvointia, tietojen oikea-aikaista pelkistämistä ja muita parannuksia, jotka voivat olla hyödyllisiä kaikkein arkaluonteisimpien tietojen kannalta. Se tarjoaa keinon hallita pääsyä organisaation ympäristön ulkopuolella. Häiriöihin reagoimista voidaan tukea dynaamisilla pääsynhallinnan tekniikoilla, sillä lupia voidaan muokata ja kumota milloin tahansa.

Lisätietoja pääsynhallinnan puitteista löytyy standardista ISO/IEC 29146.

## 8.4 Pääsy lähdekoodiin (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttövaltuushallinta #Sovelluksen_turvallisuus #Turvallinen_konfigurointi	#Suojaaminen

### Hallintakeino

Lähdekoodien, kehittämistyökalujen ja ohjelmistokirjastojen luku- ja kirjoitusoikeuksia olisi hallittava asianmukaisesti.

### Tarkoitus

Estetään luvattomien toiminnallisuuskseen luominen, vältetään tahattomat ja ilkivaltaiset muutokset sekä ylläpidetään arvokkaan aineettoman omaisuuden luottamuksellisuutta.

### Ohjeistus

Pääsyä lähdekoodeihin ja niihin liittyviin tietoihin (kuten suunnitelmiin, spesifikaatioihin, todennussuunnitelmiin ja kelpuutussuunnitelmiin) ja kehitystyökaluihin (esim. käänäjiin, kokoajiin, integrointityökaluihin, testialustoihin ja -ympäristöihin) olisi hallittava tiukasti.

Lähdekoodin hallinta voidaan toteuttaa tallentamalla koodi valvotusti ja keskitetysti, mieluiten lähdekoodien hallintajärjestelmiin.

Lähdekoodien luku- ja kirjoitusoikeudet voivat vaihdella henkilöstön roolien perusteella. Esimerkiksi lähdekoodiin voidaan myöntää lukuoikeuksia laajastikin organisaation sisällä, mutta kirjoitusoikeudet myönnestää vain työntekijöille henkilöstön jäsenille tai nimetyille omistajille. Jos useampi kehittäjä organisaation sisällä käyttää samoja koodikomponentteja, olisi toteutettava lukuoikeudet keskitettyyn koodivarastoon. Lisäksi, jos organisaatiossa käytetään avoimen lähdekoodin tai kolmansien osapuolien koodikomponentteja, voidaan lukuoikeuksia näihin koodivarastoihin myöntää laajasti. Kirjoitusoikeuksien myöntämisen olisi yhä oltava rajotettua.

Lähdekirjastoihin pääsyä olisi hallittava ottaen huomioon seuraavat ohjeet tietokoneohjelmien turmeltumisen mahdollisuuden pienentämiseksi:

- Pääsyä ohjelmien lähdekoodeihin ja ohjelmien lähdekirjastoihin olisi hallittava laadittujen menettelyjen mukaisesti.
- Luku- ja kirjoitusoikeuksia lähdekoodiin olisi myönnnettävä liiketoimintatarpeiden perusteella, ja niitä olisi hallittava muuttamisen tai väärinkäytön riskien varalta laadittujen menettelyjen mukaisesti.
- Lähdekoodien ja niihin liittyvien tietojen päivitys ja lähdekoodiin pääsyn myöntäminen olisi tehtävä muutostenhallintamenettelyn (ks. [kohta 8.32](#)) mukaisesti ja vasta sen jälkeen, kun asianmukainen valtuutus on saatu.
- Kehittäjille ei mahdolisteta suoraa pääsyä lähdekoodivarastoon, vaan pääsy toteutetaan kehittämistyökalujen kautta. Niillä hallitaan lähdekoodia koskevia toimintoja ja valtuuksia.
- Ohjelman listausohjeita olisi säilytettävä turvallisessa ympäristössä, jossa luku- ja kirjoitusoikeuksia olisi hallittava ja myönnnettävä asianmukaisesti.
- Olisi ylläpidettävä lähdekoodin kaikkia käyttökertoja ja muutoksia koskeva tapahtumalokia.

Jos ohjelman lähdekoodi on tarkoitus julkistaa, olisi harkittava lisähallintakeinoja, joista on apua sen eheyden varmistamisessa (esim. digitaalinen allekirjoitus).

## Lisätiedot

Jos pääsyä lähdekoodiin ei hallita kunnolla, luvattomat henkilöt saattavat päästää muokkaamaan lähdekoodia tai saada haltuunsa kehitysympäristössä olevaa tietoa (esim. tuotantotietoja tai konfiguraatiotietoja).

## 8.5 Turvallinen todentaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_-ja_käyttövaltuushallinta	#Suojaaminen

### Hallintakeino

Olisi toteutettava turvallisen pääsyn teknologiat ja menettelyt, jotka perustuvat tietoja koskeviin pääsyrajoituksiin ja pääsynhallintaa koskeviin kohdennettuihin toimintaperiaatteisiin.

### Tarkoitus

Varmistetaan, että käyttäjä tai taho on turvallisesti todennettu, kun sille myönnetään pääsy järjestelmiin, sovelluksiin ja palveluihin.

### Ohjeistus

Olisi valittava asianmukainen todennusmenettely, jolla voidaan varmistaa käyttäjän, ohjelmiston, viestien ja muiden tahojen vätetty identiteetti.

Käyttäjän todennuksen vahvuuden olisi oltava riittävä ottaen huomioon käsiteltäväissä olevan tiedon luokitus. Jos tarvitaan vahvaa tunnistusta ja henkilöllisyyden todennusta, olisi käytettävä jotain muuta todennusmenetelmää kuin salasanoja, kuten digitaalisia varmenteita, sirukortteja, tunnistevälineitä tai biometrisiä keinoja.

Tunnistautumistietojen tukena olisi käytettävä useampia todentamistekijöitä, kun kyse on pääsystä kriittisiin tietojärjestelmiin (eli ns. monivaiheinen tunnistautuminen). Useamman todentamistekijän, kuten mitä tietää, mitä on hallussa ja fyysiset ominaisuudet (*you know, what you have, what you are*), yhdistelmä pienentää luvattoman pääsyn mahdollisuutta. Monivaiheiden tunnistautuminen voidaan yhdistää muihin

tekniikoihin ja vaatia lisätekijöitä tietyissä tilanteissa, ennalta määriteltyjen sääntöjen ja tekijöiden perusteella, kuten käyttö epätavallisesta sijainnista, epätavalliselta laitteelta tai epätavalliseen aikaan.

Biometrista todentamista koskevat tiedot olisi hylättävä, jos ne paljastuvat. Biometrinen todennus voi olla mahdotonta myös käyttöön liittyvistä syistä (esim. kosteus tai vanheneminen). Tästä syystä biometrisen todennuksen tukena olisi oltava vähintään yksi vaihtoehtoinen todentamistekniikka.

Järjestelmän tai sovelluksen kirjautumismenettely olisi suunniteltava siten, että riski luvattomaan pääsyyn on mahdollisimman pieni. Kirjautumismenettelyjen ja -teknologoiden toteuttamisessa olisi otettava huomioon seuraavat asiat:

- a) Järjestelmä ei saisi näyttää arkaluonteisia järjestelmä- tai sovellustietoja ennen kirjautumista, jotta luvatonta käyttäjää ei autettaisi tarpeettomasti.
- b) Järjestelmän olisi näytettävä yleinen varoitus siitä, että järjestelmä, sovellus tai palvelu on tarkoitettu vain luvallisille käyttäjille.
- c) Järjestelmä ei saisi näyttää luvattomia käyttäjiä auttavia apuviestejä kirjautumisprosessin aikana (esim. virhetilanteessa järjestelmän ei pidä kertoa, mikä osa tiedoista on oikein tai väärin).
- d) Järjestelmän olisi osoitettava kirjautumistiedot kelvollisiksi vasta, kun kaikki tiedot on syötetty.
- e) Järjestelmän olisi oltava suojattu käyttäjäniimiin ja salasanoihin kohdistuvilta väsytyshyökkäyksiltä (*brute-force attack*) (esim. käytettävä täysin automaattista julkista Turingin testiä, jolla on tarkoitus erottaa tietokoneet ja ihmiset toisistaan [CAPTCHA-testi], vaadittava salasanalla vaihtamista, jos virheellisiä yrityksiä on tietty määrä, tai estettävä käyttäjä virheiden enimmäismäärän täyttyttyä).
- f) Järjestelmän olisi kirjattava epäonnistuneet ja onnistuneet kirjautumisyritykset.
- g) Järjestelmän olisi annettava hälytys, jos se havaitsee kirjautumisen hallintakeinojen mahdollisen tai onnistuneen murtoyrityksen (esim. lähetämällä hälytys käyttäjälle ja organisaation pääkäyttäjille, kun väärä salasana on annettu riittävän monta kertaa).
- h) Järjestelmän olisi onnistuneen kirjautumisen jälkeen lähetettävä seuraavat tiedot erillistä kanavaa pitkin:
  - 1) edellisen onnistuneen kirjautumisen päivämäärä ja kellonaika
  - 2) edellisen onnistuneen kirjautumisen jälkeisten mahdollisten epäonnistuneiden yritysten yksityiskohdat.
- i) Järjestelmä ei saisi näyttää salasanaa salaamattomana, kun sitä syötetään. Joissain tapauksissa voidaan vaatia tämän toiminnallisuuden kytkemistä pois, jotta käyttäjän kirjautumista voidaan helpottaa (esim. saavutettavuuteen liittyen tai jotta vältytään käyttäjien estämislöytöihin).
- j) Järjestelmä ei saisi lähetää salasanoja selväkieliteksttinä verkon kautta, jotta verkossa olevat "nuuskintaohjelmat" eivät saisi niitä siepattua.
- k) Järjestelmän olisi katkaistava käyttämättömät istunnnot määritellyn toimettonuusajan jälkeen etenkin korkean riskin sijainneista, kuten julkisista tai ulkopuolisista alueista, jotka ovat organisaation turvallisuuden hallinnan ulkopuolella, tai käyttäjien päätelaitteista.
- l) Järjestelmän olisi rajoittettava yhteysaikojen kestoja, jotta saadaan ylimääräistä suojaa korkean riskin sovelluksiin ja pienennetään aikaikkunaa, jona luvaton pääsy on mahdollinen.

## Lisätiedot

Lisätietoja tahojen todentamisen varmistamisesta löytyy standardista ISO/IEC 29115.

## 8.6 Kapasiteetinhallinta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Eheys #Saatavuus	#Tunnistus #Suojaus #Havainto	#Jatkuvuus	#Hallintotapa_ ja_ekosysteemi #Suojaaminen

### Hallintakeino

Resurssien käyttöä olisi seurattava, ja se olisi mukautettava senhetkisten ja odotettujen kapasiteettivaatimusten mukaisesti.

### Tarkoitus

Varmistetaan tietojenkäsittelypalveluiden, henkilöresurssien, toimistojen ja muiden toimitilojen kapasiteetin riittävyys.

### Ohjeistus

Tietojenkäsittelypalveluita, henkilöresursseja, toimistoja ja muita toimitiloja koskevat kapasiteettivaatimukset olisi yksilöitäävä ottaen huomioon kyseisten järjestelmien ja prosessien kriittisyyys liiketoiminnan kannalta.

Järjestelmän säättämisellä ja seurannalla olisi varmistettava järjestelmien saatavuus ja tehokkuus sekä tarvittaessa parannettava niitä.

Organisaation olisi tehtävä järjestelmien ja palveluiden stressitestausta, jotta voidaan varmistaa, että saatavilla on huippukuormituksen vaatimukset täyttävä kapasiteetti.

Havaitsevilla hallintakeinoilla olisi havaittava ongelmat ajoissa.

Tulevien kapasiteettivaatimusten ennakoinnissa olisi otettava huomioon uudet liiketoiminta- ja järjestelmävaatimukset samoin kuin tietojenkäsittelykapasiteetin nykyinen ja ennakoitu tuleva tarve.

Sellaisiin resursseihin, joilla on pitkät toimitusajat tai korkeat kustannukset, olisi kiinnitetään erityistä huomiota. Tämän vuoksi esimiesten tai palvelujen tai tuotteiden omistajien olisi tarkkailtava tärkeimpien järjestelmäresurssien käytötä.

Esimiesten olisi tällä perusteella havaittava järjestelmän tai palveluiden turvallisuutta mahdollisesti uhkaavat resurssirajoitukset ja riippuvuus avainhenkilöistä sekä suunniteltava asianmukaiset toimet.

Riittävän kapasiteetin takaaminen voidaan saavuttaa lisäämällä kapasiteettia tai vähentämällä kapasiteetin tarvetta. Kapasiteetin lisäämisessä olisi otettava huomioon seuraavat asiat:

- uuden henkilöstön palkkaaminen
- uusien toimitilojen tai muiden tilojen hankkiminen
- tehokkaampien käsittelyjärjestelmien, muistien ja tallennustilan hankkiminen
- pilvilaskennan hyödyntäminen, koska siinä on sisäänrakennetusti otettu huomioon kapasiteettia koskevat kysymykset. Pilvilaskenta on joustavaa ja skaalattavaa, mikä mahdolistaan tiettyjen sovellusten ja palvelujen käytössä olevien resurssien tarpeenmukaisen ja nopean lisäämisen ja vähentämisen.

Organisaation resurssitarpeiden vähentämisessä olisi otettava huomioon seuraavat asiat:

- vanhentuneiden tietojen poistaminen (tallennustila)
- tulostekopioiden hävittäminen, kun niiden säilytsaika on täynnä (hyllytila)
- sovellusten, järjestelmien, tietokantojen tai ympäristöjen käytöstä poistaminen

- d) eräajoprosessien ja -aikataulujen optimointi
- e) sovellusten koodien tai tietokantakyselyjen optimointi
- f) kaistanleveyden epääminen tai rajoittaminen paljon resursseja kuluttavilta palveluilta, jos nämä palvelut eivät ole kriittisiä (esim. videoiden suoratoisto).

Tehtävän kannalta kriittisille järjestelmille olisi harkittava dokumentoidun kapasiteetin hallintasuunnitelman laatimista.

### Lisätietoa

Lisätietoja pilvilaskennan joustavuudesta ja skaalattavuudesta löytyy teknisestä raportista ISO/IEC 23167.

## 8.7 Haittaohjelmilta suojaaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-omaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyytet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Järjestelmän_ ja_verkon_turvallisuus #Tietojen_suojaaminen	#Suojaaminen #Puolustus

### Hallintakeino

Haittaohjelmilta suojaaminen olisi toteutettava, ja sitä olisi tuettava käyttäjien haittaohjelmia koskevan tietoisuuden parantamisella.

### Tarkoitus

Varmistetaan, että tiedot ja niihin liittyvät omaisuuserät on suojattu asianmukaisesti haittaohjelmilta.

### Ohjeistus

Haittaohjelmilta suojaamisen olisi perustuttava haittaohjelmien havaitsemis- ja korjausohjelmistoihin, tietoturvatietoisuuteen, järjestelmiin pääsyn riittävään valvontaan ja tehokkaaseen muutosten hallintaan. Yleensä kuitenkaan haittaohjelmien havaitsemis- ja korjausohjelmistot eivät yksinään riitä. Seuraavia ohjeita olisi noudatettava:

- a) Olisi toteutettava hallintakeinot, jotka estävät tai havaitsevat luvattomien ohjelmien käytön (esim. sallittujen ohjelmien luettelot) (ks. [kohdat 8.19](#) ja [8.32](#)).
- b) Olisi toteutettava hallintakeinot, jotka estävät tai havaitsevat tiedettyjen tai epäiltyjen haitallisten verkkosivustojen käytön (esim. estoluettelot).
- c) Olisi vähennettävä haavoittuvuuksia, joita haittaohjelmat voivat hyödyntää (esim. teknisten haavoittuvuuksien hallinnan avulla, ks. [kohdat 8.8](#) ja [8.19](#)).
- d) Järjestelmien ja etenkin kriittisiä liiketoimintaprosesseja tukevien järjestelmien ohjelmistot ja aineistosisältö olisi katselmoitava automaatisesti säännöllisesti. Luvattomia tiedostoja tai muutoksia olisi etsittävä.
- e) Olisi laadittava suojaustoimet suojaamaan riskeiltä, jotka syntyvät, kun tiedostoja ja ohjelmistoja hankitaan ulkopuolisista verkoista tai niiden kautta tai millä tahansa tietovälineellä.
- f) Haittaohjelmien havaitsemis- ja korjausohjelmistot olisi asennettava tietokoneiden ja sähköisten tallennusvälineiden tarkistamiseksi, ja niitä olisi päivitetä säännöllisesti. Olisi tehtävä säännöllisiä tarkistuksia, joissa tarkistetaan
  - 1) kaikki verkon tai sähköisten tallennusvälineiden kautta saapuneet tiedot haittaohjelmien varalta ennen käytöä

- 2) sähköpostien ja pikaviestien liitetiedostot ja lataukset haittaohjelmien varalta ennen käyttöä; tarkistus voidaan toteuttaa eri pisteissä (esim. sähköpostipalvelimilla, työasemilla) ja organisaation verkkoon saavuttaessa
- 3) verkkosivustot haittaohjelmien varalta, kun niille mennään.
- g) Haittaohjelmien havaitsemis- ja korjaustyökalujen sijainti olisi määritettävä riskien arvioinnin tulosten ja seuraavien asioiden perusteella:
- 1) Syvyyssuuntaisen turvallisuuden periaatteiden noudattaminen siellä, missä se on vaikuttavinta. Tämä voi tarkoittaa esim. haittaohjelmien havaitsemista verkon yhdyskäytävän kohdalla (eri sovellusprotokollissa, kuten sähköpostissa, tiedostonsiirrossa ja verkossa) sekä käyttäjien päätelaitteilla ja palvelimilla.
  - 2) Hyökkääjien väistötekniikat (esim. salattujen tiedostojen käyttö) haittaohjelmien toimittamiseen tai salausprotokollien käyttö haittaohjelmien siirtämiseen.
- h) Haittaohjelmien tuomiselta järjestelmään olisi suojauduttava huolellisesti ylläpito- ja hätätilannemenettelyjen aikana, koska näissä tilanteissa tavalliset haittaohjelmilta suojaavat hallintakeinot saatetaan ohittaa.
- i) Olisi toteutettava prosessi, jolla valtuutetaan tilapäisesti tai estetään pysyvästi, osa tai kaikki haittaohjelmilta suojaavat toimet, mukaan lukien poikkeusten hyväksyjät, perusteiden dokumentointi ja katselmoinnin päivämäärä. Tämä voi olla tarpeen, jos haittaohjelmilta suojautuminen aiheuttaa häiriön normaalitoimintaan.
- j) Olisi laadittava asianmukaiset liiketoiminnan jatkuvuussuunnitelmat haittaohjelmanhyökkäyksistä toipumista varten mukaan luettuna kaikki tarvittavat tiedostojen ja ohjelmistojen varmuuskopiointiin (sekä verkkovarmistus että muu varmistus) ja palauttamiseen liittyvät toimet (ks. [kohta 8.13](#)).
- k) Olisi eristettävä ympäristöt, joissa voi syntyä erittäin vahingollisia seuraauksia.
- l) Olisi määriteltävä menettelyohjeet ja vastuu järjestelmien suojaamiseen haittaohjelmilta, esim. koulutetaan henkilöstöä suojauskien käyttöön sekä haittaohjelmanhyökkäyksistä raportointiin ja niistä toipumiseen.
- m) Tarjotaan kaikille käyttäjille tietoisuutta tai koulutusta siitä, miten tunnistetaan ja mahdollisesti lievennetään haittaohjelmien saastuttamien sähköpostien, tiedostojen tai ohjelmien vastaanotosta, lähetämisenstä tai asentamisesta aiheutuvia ongelmia (ks. [kohta 6.3](#)) (luetelmaohdissa n) ja o) kerättyjä tietoja voidaan käyttää sen varmistamiseen, että tietoisuus ja koulutus ovat ajantasaisia).
- n) Olisi toteutettava menettelyt uusia haittaohjelmia koskevien tietojen säännölliseen keräämiseen, kuten postituslistojen ja aiheeseen liittyviä tietoja tarjoavien verkkosivustojen seuraaminen.
- o) Todennetaan, että haittaohjelmiin liittyvät tiedot, kuten varoitusviestit, ovat peräisin päteviltä ja luotettavilta tahoilta (esim. luotettava verkkosivustot tai haittaohjelmien havaitsemisohjelmistojen toimittajat) ja että ne ovat tarkkoja ja opastavia.

## Lisätiedot

Aina ei ole mahdollista asentaa haittaohjelmilta suojaavia ohjelmistoja kaikkiin järjestelmiin (esim. joihinkin teollisuuden ohjausjärjestelmiin). Jotkin haittaohjelmat tarttuttavat tietokoneiden käyttöjärjestelmiä ja laiteohjelmistoja siten, että yleiset haittaohjelmien hallintakeinot eivät kykene puhdistamaan järjestelmää ja voi olla pakko asentaa käyttöjärjestelmä tai toisinaan jopa tietokoneen laiteohjelmisto uudelleen, jotta kyötään palauttamaan turvallinen tila.

## 8.8 Teknisten haavoittuvuuksien hallinta ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Uhkien_ja_haavoittuvuuksien_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus

### Hallintakeino

Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista olisi hankittava tietoa. Organisaation altistuminen näille haavoittuvuuksille olisi arvioitava, ja niihin liittyviin riskeihin olisi vastattava asianmukaisilla toimenpiteillä.

### Tarkoitus

Estetään teknisten haavoittuvuuksien hyväksikäyttö.

### Ohjeistus

#### Teknisten haavoittuvuuksien tunnistaminen

Organisaatiolla olisi oltava tarkka omaisuuserien luettelo (ks. [kohdat 5.9–5.14](#)), jotta se kykee vaikuttavaan tekniseen haavoittuvuuksien hallintaan. Omaisuuserien luetteloon olisi sisällettävä ohjelmiston toimittaja, ohjelmiston nimi, versionumerot, käyttötilanne (esim. mitä ohjelmistoja on asennettuna mihinkin järjestelmään) ja ohjelmistosta organisaatiossa vastaavat henkilöt.

Teknisten haavoittuvuuksien hallinnassa organisaation olisi otettava huomioon seuraavat asiat:

- Organisaation olisi määriteltävä ja luotava teknisten haavoittuvuuksien hallintaan liittyvät roolit ja vastuut. Tähän sisältyy haavoittuvuuksien seuranta, haavoittuvuusriskien arvointi, päivittäminen, omaisuuserien seuranta ja mahdollisesti tarvittavat koordinointivastuu.
- Ohjelmistojen ja muiden teknologioiden kohdalla (perustuen omaisuuserien luetteloon, ks. [kohta 5.9](#)) olisi tunnistettava tietolähteet, joiden avulla tunnistetaan olennaiset tekniset haavoittuvuudet ja ylläpidetään niitä koskevaa tietoisuutta. Tietolähteiden luettelo olisi päivitettyä omaisuusluetteloon tehtävien muutosten perusteella tai kun löydetään uusia tai hyödyllisiä tietolähteitä.
- Tietojärjestelmien (ja niiden komponenttien) toimittajia olisi vaadittava varmistamaan, että käytössä on haavoittuvuuksien raportointi, käsittely ja julkistaminen, mukaan lukien soveltuissa sopimuksissa olevat vaatimukset (ks. [kohta 5.20](#)).
- Käytössä oleviin teknologioihin soveltuavia haavoittuvuuksien skannaustyökaluja olisi käytettävä, jotta tunnistetaan haavoittuvuudet ja kyetään todentamaan, onko haavoittuvuuksien korjaaminen onnistunut.
- Pätevien henkilöiden olisi tehtävä suunniteluja, dokumentoituja ja toistettavissa olevia tunkeutumistestejä tai haavoittuvuusarvionteja, jotta kyetään tukemaan haavoittuvuuksien tunnistamista. Näiden toimintojen tekemisessä olisi oltava varovainen, koska tällainen toiminta saattaa vaarantaa järjestelmän turvallisuuden.
- Kolmansien osapuolten tuottamien kirjastojen ja lähdekoodien haavoittuvuuksia olisi seurattava. Tämä olisi sisällytettyä turvalliseen ohjelointiin (ks. [kohta 8.28](#)).

Organisaation olisi luotava menettelyt ja kyvykkydet

- havaita haavoittuvuuksien olemassaolo tuotteissaan ja palveluissaan, myös näihin sisältyvissä ulkopuolisissa komponenteissa
- vastaanottaa haavoittuvuusraportteja sisäisistä ja ulkoisistä lähteistä.

Organisaatiolla olisi oltava julkinen yhteydenottopiste osana haavoittuvuuksien ilmoittamista koskevia kohdennettuja toimintaperiaatteita, jotta tutkijat ja muut toimijat kykenevät raportoimaan ongelmista.

Organisaation olisi laadittava haavoittuvuuksien raportointimenettelyt, verkkolomakkeet raportointia varten ja hyödynnettävä asianmukaista uhkatiedon seurantaa tai foorumeita, joilla jaetaan tietoja. Organisaation olisi myös harkittava virheiden löytämisen palkitsemisohjelmia (*bug bounty*), joissa tarjotaan palkintoja houkuttimena siitä, että organisaatioita autetaan paikallistamaan haavoittuvuuksia ja näin korjaamaan niitä. Organisaation olisi myös jaettava tietoa toimialan pätevien elinten tai muiden sidosryhmien kanssa.

#### Teknisten haavoittuvuuksien arviointi

Tunnistettujen teknisten haavoittuvuuksien arvioinnissa olisi otettava huomioon seuraavat asiat:

- a) Raportit olisi analysoitava ja todennettava, jotta voidaan määrittää, mitä vasteita ja korjaavia toimintoja tarvitaan.
- b) Kun mahdollinen tekninen haavoittuvuus on tunnistettu, olisi yksilöitää siihen liittyvät riskit ja tarvittavat toimenpiteet. Tällaisia toimenpiteitä voivat olla haavoittuvien järjestelmien paikkaus tai muiden hallintakeinojen käyttö.

#### Teknisten haavoittuvuuksien asianmukainen käsite

Ohjelmistopäivityksiä varten olisi toteutettava hallintaprosessi, jotta voidaan varmistaa, että viimeisimmät hyväksytyt korjaustiedostot ja sovelluspäivitykset on asennettu kaikkiin hyväksyttyihin ohjelmistoihin. Jos muutokset ovat tärkeitä, alkuperäinen ohjelmisto olisi säilyttävä ja muutokset olisi tehtävä selkeästi määriteltyyn kopioon. Muutokset olisi testattava ja dokumentoitava täydellisesti siten, että niitä voidaan tarvittaessa käyttää uudelleen, kun ohjelmistoa parannetaan myöhemmin. Riippumattoman arviontielimen olisi tarvittaessa testattava ja kelpuutettava muutokset.

Teknisten haavoittuvuuksien käsitellyssä olisi noudatettava seuraavia ohjeita:

- a) Tunnistettuihin mahdollisiin teknisiin haavoittuvuuksiin olisi vastattava asianmukaisin ja oikea-aikaisin toimenpitein. Olisi määriteltävä aikataulu, jonka puiteissa reagoidaan ilmoituksiin mahdollisista olenaisista teknisistä haavoittuvuuksista.
- b) Riippuen siitä, kuinka kiireellisesti teknistä haavoittuvuutta on tarpeen käsitellä, toimenpiteisiin olisi ryhdyttävä joko muutoksenhallinnan hallintakeinojen mukaisesti (ks. [kohta 8.32](#)) tai noudattaen tietoturvahäiriöihin vastaamisen menettelyä (ks. [kohta 5.26](#)).
- c) Olisi käytettävä vain luotettavista lähteistä (jotka voivat olla organisaation sisäisiä tai ulkoisia) peräisin olevia korjaustiedostoja.
- d) Korjaustiedostot olisi testattava ja arvioitava ennen niiden asentamista, jotta voidaan varmistaa, että ne toimivat ja etteivät ne aiheuta kestämättömiä sivuvaikutuksia (eli jos korjaustiedosto on saatavilla, olisi arvioitava sen asentamiseen liittyvät riskit eli haavoittuvuuden aiheuttamia riskejä olisi verrattava korjaustiedoston asentamisesta seuraaviin riskeihin).
- e) Hyvin riskialttiita järjestelmä olisi käsiteltävä ensimmäisenä.
- f) Olisi kehitettävä korjaus (yleensä ohjelmiston päivitys tai korjaustiedosto).
- g) Testauksella olisi varmistettava, että korjaus tai käsitteily on vaikuttavaa.
- h) Korjauksen aitouden varmentamiseen olisi oltava mekanismit.
- i) Jos korjausta ei ole saatavilla tai sitä ei voida asentaa, olisi harkittava muiden hallintakeinojen käyttöä, kuten
  - 1) ohjelmiston toimittajan tai muiden asianmukaisten lähteiden suosittelemien kiertoratkaisujen käyttöä
  - 2) haavoittuvuuksiin liittyvien palvelujen tai ominaisuuksien kytkemistä pois käytöstä
  - 3) pääsynhallintamekanismien, esim. palomuurien, mukauttamista tai lisäämistä verkon rajoille (ks. kohta [kohdat 8.20–8.22](#))

- 4) haavoittuvien järjestelmien, laitteiden tai sovellusten suojaamista hyökkäyksiltä asianmukaisille liikennesuodattimilla (tätä kutsutaan myös virtuaaliseksi päivittämiseksi).
- 5) valvontan lisäämistä, jotta havaitaan todelliset hyökkäykset
- 6) haavoittuvuudesta viestimistä.

Jos hankittujen ohjelmistojen toimittajat julkaisevat tietoa ohjelmistojensa turvallisuuspäivityksistä ja tarjoavat mahdollisuuden asentaa nämä päivitykset automaattisesti, organisaation olisi päättävä, käytetäänkö automaattisia päivityksiä.

#### Muut näkökohtat

Kaikista teknisten haavoittuvuuksien hallinnan tehdystä toimenpiteistä olisi pidettävä tapahtumalokia.

Teknisten haavoittuvuuksien hallintaprosessia olisi seurattava ja arvioitava säännöllisesti, jotta voidaan varmistaa sen tehokkuus ja vaikuttavuus.

Vaikuttavan teknisten haavoittuvuuksien hallintaprosessin olisi oltava yhtenevä häiriötilanteiden hallintatoimenpiteiden kanssa, viestittävä haavoittuvuuksia koskeva tietoa häiriövastetoiminnolle ja annettava tekniset menettelyt, jotka tehdään mahdollisessa häiriötilanteessa.

Kun organisaatio käyttää pilvipalvelua, jonka tuottaa kolmannen osapuolen pilvipalvelun tuottaja, pilvipalvelun tuottajan olisi varmistettava omien resurssien teknisten haavoittuvuuksien hallinta. Pilvipalvelun tuottajan vastuun teknisten haavoittuvuuksien hallinnasta olisi sisällyttävä pilvipalvelua koskevan sopimuksen, ja sen olisi sisällyttävä prosessit, joilla raportoidaan pilvipalvelun tuottajan teknisiin haavoittuvuuksiin kohdistamat toimenpiteet. Joissain pilvipalveluissa pilvipalvelun tuottajalla ja pilvipalvelun asiakalla on kummakin omat vastuunsa. Esimerkiksi pilvipalvelun asiakas on vastuussa omien pilvipalvelussa käytettävien omaisuuseriensä haavoittuvuuksien hallinnasta.

#### Lisätiedot

Teknisten haavoittuvuuksien hallintaa voidaan pitää muutoksenhallinnan alatoimintona, ja sellaisena se voi hyödyntää muutoksenhallintaprosesseja ja -menettelytä (ks. [kohta 8.32](#)).

On mahdollista, ettei päivitys välittämättä käsitlele ongelmaa riittävästi ja sillä on haitallisia sivuvaiktuksia. Joissakin tapauksissa myös päivityksen poistaminen asentamisen jälkeen saattaa olla vaikeaa.

Jos päivitysten riittävä testaus ei ole mahdollista esim. kustannusten tai puutteellisten resurssien vuoksi, voidaan harkita viivettä päivitysten asentamisessa, jotta voidaan arvioida siihen liittyvät riskit muiden käyttäjien raportoimien kokemusten perusteella. Standardin ISO/IEC 27031 noudattaminen voi olla hyödyllistä.

Kun ohjelmistokorjausia tai -päivityksiä vastaanotetaan, voi organisaatio harkita automaattista päivitysprosessia, jossa nämä päivitykset asennetaan vaikutuksille altistuneisiin järjestelmiin ja tuotteisiin ilman asiakkaan tai käyttäjän toimia. Jos automaattinen päivitysprosessi tarjotaan, se voi antaa asiakkaille ja käyttäjille mahdollisuuden sammuttaa automaattiset päivitykset tai hallita niiden asentamisen ajankohtaa.

Jos toimittaja tarjoaa automaattisen päivitysprosessin ja päivitykset voidaan asentaa vaikutuksille altistuneisiin järjestelmiin ja tuotteisiin ilman toimia, organisaatio määrittää, käytääkö se automaattista prosessia vai ei. Yksi syy olla käytämättä automaattista päivittämistä on säilyttää hallinta siitä, milloin päivitykset asennetaan. Esimerkiksi ohjelmistoa, joka on liiketoiminnan tehtävän käytössä, ei voida päivittää ennen kuin tehtävä on suoritettu loppuun.

Haavoittuvuuksien skannaamisen heikkous on siinä, että siinä ei välittämättä oteta täysin huomioon syvyysluokituista turvallisuutta: kahdella aina samassa järjestysessä tehtävällä vastatoimella voi olla haavoittuvuuksia, jotka peittyytävät yhteisvaikutuksen alle. Kahden vastatoimen yhdistelmä ei ole haavoittuva, vaikka haavoittuvuuksia saattaa raportoida, että molemmat osat ovat haavoittuvia. Organisaation olisi tähän syistä katselmoitava haavoittuvuusraportit huolellisesti ja harkittava niistä seuravia toimenpiteitä tarkkaan.

Monet organisaatiot toimittavat ohjelmistoja, järjestelmiä, tuotteita ja palveluja oman organisaationsa lisäksi myös sidosryhmille, kuten asiakkaille, yhteistyökumppaneille tai muille käyttäjille. Näillä ohjelmistoilla, järjestelmillä, tuotteilla ja palveluilla voi olla tietoturvallisuuteen liittyviä haavoittuvuuksia, jotka vaikuttavat käyttäjien turvallisuuteen.

Organisaatiot voivat julkaista korjauksia ja antaa käyttäjille tietoa haavoittuvuuksista (yleensä julkisena tiedotteena) sekä tarjota asianmukaista tietoa ohjelmistohaavoittuvuuksia kokoaville tietokantapalveluille.

Lisätietoja teknisten haavoittuvuuksien hallinnasta pilvilaskentaa käytettäessä löytyy standardista ISO/IEC 19086 ja standardisarjasta ISO/IEC 27017.

Lisätietoa haavoittuvuuusraporttien vastaanottamisesta ja haavoittuvuuustiedotteiden julkaisemisesta löytyy standardista ISO/IEC 29147. Lisätietoa raportoitujen haavoittuvuuksien käsittelyä ja ratkaisua koskevia lisätietoja löytyy standardista ISO/IEC 30111.

## 8.9 Konfiguraationhallinta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi	#Suojaaminen

### Hallintakeino

Laitteistojen, ohjelmistojen, palveluiden ja verkkojen konfiguraatiot, mukaan lukien turvallisuuskonfiguraatiot, olisi laadittava, dokumentoitava ja toteutettava, ja niitä olisi seurattava ja katselmoitava.

### Tarkoitus

Varmistetaan, että laitteistot, ohjelmistot, palvelut ja verkot toimivat oikein ja riittävän tiukoilla turvallisuusasetuksilla, eikä konfiguraatioon kohdistu luvattomia tai väärää muutoksia.

### Ohjeistus

#### Yleistä

Organisaation olisi määriteltävä ja toteutettava prosessit ja työkalut, joilla laitteistojen, ohjelmistojen, palveluiden (esim. pilvipalveluiden) ja verkkojen määritellyt konfiguraatiot (myös turvallisuuskonfiguraatiot) toteutetaan sekä uusille järjestelmäasennuksille että käytössä oleville järjestelmille.

Roolien, vastuiden ja menettelyjen olisi oltava käytössä, jotta kaikkia konfiguraatioihin tehtäviä muutoksia voidaan hallita riittävällä tasolla.

#### Vakiomallit

Laitteistojen, ohjelmistojen, palvelujen ja verkkojen turvalliseen konfigurointiin olisi määriteltävä vakiomallit, jotka

- perustuvat julkisesti saatavilla olevaan ohjeistukseen (esim. ennalta määritellyt mallit toimittajilta ja riippumattomilta turvallisuusorganisaatioilta)
- ottavat huomioon vaaditun suojaustason, jotta voidaan määrittää riittävä turvallisuustaso
- tukevat organisaation tietoturvapolitiikkaa, kohdennettuja toimintaperiaatteita, standardeja ja muita turvallisuusvaatimuksia
- ottavat huomioon turvallisuuskonfiguraatioiden toteutettavuuden ja sovellettavuuden organisaation toimintaympäristössä.

Nämä mallit olisi katselmoitava säännöllisesti, ja niitä olisi päivitetty aina, kun uusiin uhkiin tai haavoittuvuuksiin pitää reagoida tai kun uusia ohjelmisto- tai laitteistoversioita tulee saataville.

Laitteistojen, ohjelmistojen, palvelujen ja verkkojen turvalliseen konfiguroointiin tarkoitettujen vakiomallien laatimisessa olisi otettava huomioon seuraavat asiat:

- a) ylläpito-oikeuksilla varustettujen identiteettien lukumääärän minimointi
- b) tarpeettomien, käyttämättömien tai turvattomien identiteettien käytöstä poistaminen
- c) tarpeettomien toimintojen ja palveluiden käytöstä poistaminen tai rajoittaminen
- d) tehokkaisiin apuohjelmiin ja isäntäkoneen parametreihin pääsyn rajoittaminen
- e) kellojen synkronointi
- f) toimittajan oletustunnistautumistietojen, kuten oletussalasanojen, vaihtaminen välittömästi asennuksen jälkeen sekä muiden turvallisuuteen liittyvien tärkeiden oletusasetusten katselointi
- g) sellaisten aikakatkaisutoimintojen käyttö, jotka automaattisesti kirjaavat laitteet ulos määritellyn toimettonuusajan jälkeen
- h) todennetaan, että lisensointivaatimukset on täytetty (ks. [kohta 5.32](#)).

#### Konfiguraatioiden hallinta

Laitteistojen, ohjelmistojen, palveluiden ja verkkojen laaditut konfiguraatiot olisi tallennettava ja kaikista konfiguraatioihin tehtävistä muutoksista olisi ylläpidettävä tapahtumalokia. Näitä tallenteita olisi säilytettävä suojauduttua. Tämä voidaan saavuttaa monella tavalla, kuten konfiguraatiotietokannoilla tai konfiguraatiomalleilla.

Konfiguraatioihin tehtävien muutosten olisi noudatettava muutoksenhallintaprosessia (ks. [kohta 8.32](#)).

Konfiguraatioita koskevat tallenteen voivat sisältää tarpeen mukaan

- a) omaisuuserän omistajan tai yhteyshenkilön ajantasaiset tiedot
- b) konfiguraatioon tehdyn viimeisimmän muutoksen päivämäärän
- c) konfiguraatiomallin versiotiedon
- d) suhteet muiden omaisuuserien konfiguraatioihin.

#### Konfiguraatioiden valvonta

Konfiguraatioita olisi valvottava järjestelmän hallintatyökalujen kattavalla joukolla (esim. huoltotoiminnot, etätuki, yrityksen hallintatyökalut, varmuuskopiointi ja ohjelmiston palautus) ja katselmoitava säännöllisin aikavälein, jotta voidaan todentaa, että konfiguraatioiden asetukset ovat kunnossa sekä arvioida salasanojen vahvuutta ja tehtyjä toimenpiteitä. Todellisia konfiguraatioita voidaan verrata määriteltyihin tavoitemalleihin. Kaikkiin poikkeamiin olisi reagoitava joko määriteltyjen tavoitekonfiguraatioiden automaattisella toteuttamisella tai analysoimalla poikkeamaa manuaalisesti ja toteuttamalla siihen perustuva korjaava toimenpide.

#### Lisätiedot

Järjestelmien dokumentaatiossa kerrotaan usein yksityiskohtia laitteistojen ja ohjelmistojen konfiguroinnista.

Järjestelmien koventaminen on tyypillinen osa konfiguraationhallintaa.

Konfiguraationhallinta voidaan integroida omaisuudenhallinnan prosesseihin ja siihen liittyviin työkaluihin.

Automaatio tuottaa yleensä vaikuttavampaa turvallisuuskonfiguraatioiden hallintaa (esim. käytämällä *Infrastructure as Code*-tekologiaa).

Konfiguraatiomallit ja -tavoitteet voivat olla luottamuksellista tietoa, ja niitä olisi suojauduttava luvattomalta käytöltä sen mukaisesti.

## 8.10 Tietojen poistaminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Tietojen_suojaaminen #Lait_ja_vaatimusten-mukaisuus	#Suojaaminen

### Hallintakeino

Tietojärjestelmiin, laitteisiin tai mihin tahansa muuhun tallennusvälineeseen varastoidut tiedot olisi poistettava, kun niitä ei enää tarvita.

### Tarkoitus

Estetään arkaluonteisten tietojen tarpeeton paljastuminen sekä noudatetaan lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyviä vaatimuksia, jotka koskevat tietojen poistamista.

### Ohjeistus

#### Yleistä

Arkaluonteista tietoa ei saisi säilyttää pidempäään kuin tarpeellista, jotta lievennetään tarkoittamattoman paljastumisen riskiä.

Järjestelmissä, sovelluksissa ja palveluissa olevien tietojen poistamisessa olisi otettava seuraavat asiat huomioon:

- Poistamismenetelmä (esim. sähköinen ylikirjoitus tai salaustekninen poistaminen) olisi valittava liketoiminnallisten vaatimusten mukaisesti ottamalla huomioon myös olennaiset lait ja viranomaismääräykset.
- Poistamisten tulokset olisi tallennettava todistusaineistoksi.
- Kun tietojen poistamiseen käytetään siihen erikoistuneita palveluntuottajia, olisi näiltä toimijoilta saatava näyttö siitä, että tiedot on poistettu.

Kun kolmannet osapuolet säilyttävät tietoja organisaation puolesta, organisaation olisi harkittava tietojen poistamista koskevien vaatimusten sisällyttämistä kolmannen osapuolen kanssa tehtyihin sopimuksiin, jotta organisaatio kykenee toimeenpanemaan tietojen poistamisen tällaisten palveluiden päättämisen aikana.

#### Poistamismenetelmät

Kun arkaluonteisia tietoja ei enää tarvita, ne olisi poistettava organisaation tietojen säilyttämistä koskevien kohdennettujen toimintaperiaatteiden mukaisesti ja ottamalla huomioon olennaisten lakien ja viranomaisten vaatimukset. Poistaminen voidaan toteuttaa

- konfiguroimalla järjestelmät poistamaan tiedot turvallisesti, kun niitä ei enää tarvita (esim. tietojen säilyttämistä koskevien kohdennettujen toimintaperiaatteiden mukaisen ajan jälkeen tai käyttöynnön jälkeen)
- poistamalla vanhentuneet versiot, kopiot ja tilapäistiedostot aina, kun sellaisia havaitaan
- käyttämällä hyväksyttyjä ja turvallisia poisto-ohjelmistoja, joilla tiedot poistetaan pysyvästi, millä varmistetaan, ettei tietoja ole mahdollista palauttaa erityisillä palautustyökaluilla tai rikostechnisillä työkaluilla
- käyttämällä hyväksyttyjä ja sertifioitua turvallisia hävittämispalveluita.
- käyttämällä hävitettävän tallennusvälineen tyypin mukaista asianmukaista hävittämismekanismia (esim. kiintolevyjen ja muiden magneettisten tallennusvälineiden magnetoinnin poistaminen).

Kun käytetään pilvipalveluita, organisaation olisi todennettava, että pilvipalvelun tuottajan käyttämät poistamismenetelmät ovat hyväksyttäviä. Jos menetelmät ovat hyväksyttäviä, organisaation olisi selvitettyvä, olisiko organisaation käytettävä sitä itse vai pyydettävä pilvipalvelun tuottajaa poistamaan tiedot. Näiden poistamisprosessien olisi oltava automatisoituja kohdennettujen toimintaperiaatteiden mukaisesti, kun se on käytettävissä ja sovellettavissa. Poistettujen tietojen arkaluonteuudesta riippuen voidaan käyttää tapahtumalokeja, jotka seuraavat ja todentavat, että poistamisprosessi on tapahtunut.

Jotta arkaluonteisia tietoja ei pääse tahattomasti paljastumaan, kun laitteita palautetaan takaisin toimittajille, arkaluonteisia tietoja olisi suojahtava poistamalla tallennusvälineet (esim. kiintolevyt) ja muistit ennen kuin laitteet poistuvat organisaation toimitiloista.

Kun otetaan huomioon, että tietojen turvallinen poistaminen joistakin laitteista (esim. älypuhelimista) voidaan toteuttaa vain tuhoamalla kyseinen laite tai käytämällä siihen ohjelmoitua toimintoja (esim. "palauta tehdasasetukset), olisi organisaation valittava asianmukaiset menetelmät sen mukaisesti, minkä luokituksen tietoja kyseisissä laitteissa käsitellään.

[Kohdassa 7.14](#) kuvailtuja hallintatoimenpiteitä olisi sovellettava tallennusvälineiden fyysiseen tuhoamiseen ja samanaikaiseen tietojen poistamiseen.

Tietojen poistamista koskeva virallinen tallenne on hyödyllinen, kun analysoidaan mahdollisen tietovuototapahtuman syytä.

## Lisätiedot

Lisätietoa tietojen poistamisesta pilvipalveluista löytyy standardista ISO/IEC 27017.

Lisätietoja henkilötietojen poistamisesta löytyy standardista ISO/IEC 27555.

## 8.11 Tietojen peittäminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Tietojen_suojaaminen	#Suojaaminen

### Hallintakeino

Tietojen peittämistä olisi käytettävä organisaation pääsynhallintaa koskevien ja muiden asiaan liittyvien kohdennettujen toimintaperiaatteiden sekä liiketoiminnallisten vaatimusten mukaisesti ottaen huomioon olennainen lainsäädäntö.

### Tarkoitus

Estetään arkaluonteisten tietojen, kuten henkilötietojen, paljastuminen sekä noudatetaan lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyviä vaatimuksia.

### Ohjeistus

Kun huolena on arkaluonteisten tietojen (kuten henkilötietojen) suojaaminen, organisaation olisi harkittava tällaisten tietojen piilottamista erilaisten tekniikkoiden, kuten tietojen peittämisen, pseudonymisoinnin tai anonymisoinnin, avulla.

Pseudonymisointi- tai anonymisointiteknikoilla voidaan piilottaa henkilötiedot, naamioida rekisteröityjen todelliset henkilöllisydet tai muut arkaluonteiset tiedot sekä katkaista yhteys henkilötietojen ja rekisteröidyn välillä tai linkki muihin arkaluonteisiin tietoihin.

Pseudonymisointi- tai anonymisointiteknikoita käytettäessä olisi todennettava, että tiedot on pseudonymisoitu tai anonymisoitu riittävällä tavalla. Ollakseen vaikuttavaa tietojen anonymisoinnissa olisi otettava huomioon kaikki arkaluonteisten tietojen osa-alueet. Jos kaikkia osa-alueita ei toteuteta kunnolla, henkilö voidaan yhä tunnistaa, vaikka suoran tunnistamisen mahdollistava tieto olisikin anonymisoitu, koska käytössä on myös muuta tietoa, joka mahdollistaa henkilön epäsuoran tunnistamisen.

Tietojen peittämisen muita tekniikoita ovat

- a) salaus (luvallisilla käyttäjillä on avain)
- b) merkkien nollaus tai poistaminen (luvattomat käyttäjät eivät näe viestejä kokonaisuudessaan)
- c) numeroiden ja päivämäärien variointi
- d) korvaaminen (arvon muuttaminen toiseksi arkaluonteisen tiedon naamioimistarkoituksessa)
- e) arvojen korvaaminen tiivisteillä.

Tietojen peittämistekniikoiden toteuttamisessa olisi otettava huomioon seuraavat asiat:

- a) Kaikille käyttäjille ei myönnetä pääsyä kaikkeen tietoon, vaan hakutoiminnot ja naamioinnit suunnitellaan siten, että ne näyttävät käyttäjälle vain vaaditun vähimmäismäärän tietoa.
- b) On tilanteita, jolloin osan tiettyyn tallennejoukkoon kuuluvien tallenteiden tiedoista ei kuuluisi olla käyttäjän nähtävissä. Näissä tapauksissa olisi suunniteltava ja toteutettava tietojen peittämisen mekanismi (esim. jos potilaas haluaa, että sairaalahenkilökunta ei näe kaikkia hänen tietojaan edes hätätilanteessa, henkilökunnalle näytetään osittain peitettyt tiedot ja tietoihin pääsevät käsiksi vain tietyt roolit, jos tiedoissa on joitain hoidon kannalta hyödyllistä tietoa).
- c) Kun tietoja peitetään, olisi rekisteröidyllle annettava mahdollisuus vaatia, etteivät käyttäjät voi nähdä sitä, että tietoja on peitetty (peittämisen peittäminen; tästä käytetään terveydenhoitolaitoksissa, jos potilaas ei halua henkilökunnan näkevän, että arkaluonteisia tietoja, kuten raskauksia tai verikokeiden tuloksia, on peitetty).
- d) Kaikki laki ja viranomaisten vaatimukset olisi otettava huomioon (esim. maksukorttien tietojen peittäminen tietojen käsittelyn tai varastoinnin aikana).

Tietojen peittämistä, pseudonymisointia tai anonymisointia käytettäessä olisi otettava huomioon seuraavat asiat:

- a) Tietojen peittämisen, pseudonymisoinnin tai anonymisoinnin vahvuustaso olisi valittava käsitletyjen tietojen käytön perusteella.
- b) Käsitletyihin tietoihin olisi sovellettava pääsynhallinta.
- c) Käsitletyjen tietojen käytöstä tai sen rajoittamisesta olisi sovittava.
- d) Käsitellyn tietojen yhdistäminen muihin tietoihin rekisteröidyn tunnistamista varten olisi kielletävä.
- e) Käsitellyjen tietojen vastaanottamisesta ja luovuttamisesta olisi pidettävä kirja.

## Lisätiedot

Anonymisointi muuttaa henkilötietoja peruuttamattomasti siten, ettei rekisteröityä voida enää tunnistaa suoraan tai epäsuorasti.

Pseudonymisointi korvaa yksilöivät tiedot salanimillä. Tieto pseudonymisoinnin algoritmista (toisinaan nimellä "lisätiedot") mahdollistaa rekisteröidyn tunnistamisen ainakin jollain tasolla. Tällaiset "lisätiedot" olisikin tästä syystä pidettävä erillään ja suojauduttuna.

Vaikka pseudonymisointi onkin heikompi vaihtoehto kuin anonymisointi, pseudonymisoidut tietojoukot voivat olla hyödyllisempiä tilastotutkimusten kannalta.

Tietojen peittäminen on joukko tekniikoita, joilla salataan, korvataan tai peitetään arkaluonteisia tietokohteita. Tietojen peittäminen voi olla staattista (kun tietokohde on peitetty alkuperäisessä tietokannassa), dynaamista (tietoja suojataan reaalialkaisesti automatisoinnin ja sääntöjen avulla) tai lennossa tapahtuvaltaa (tiedot peitetään sovelluksen muistissa).

Henkilötiedot voidaan anonymoida tiivistysfunktioiden avulla. Enumeraatiohyökkäysten estämiseksi tiivistysfunktiot olisi aina yhdistettävä suolafunktioon.

Resurssitunnisteisiin ja niiden attribuutteihin (esim. tiedostojen nimiin, URL-osoitteisiin) ei saisi sisällyttää henkilötietoja tai ne olisi vähintään anonymisoitava asianmukaisesti.

Henkilötietojen suojaamista koskevia lisätietoja löytyy standardista ISO/IEC 27018.

Lisätietoa tunnistamisyhteyksien poistamistekniikoista löytyy standardista ISO/IEC 20889.

## 8.12 Tietovuotojen estäminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Luottamuksellisuus	#Suojaus #Havainto	#Tietojen_suojaaminen	#Suojaaminen #Puolustus

### Hallintakeino

Tietovuotojen estämistoimia olisi sovellettava järjestelmiin, verkkoihin ja muihin laitteisiin, joissa käsitellään, varastoidaan tai siirretään arkaluonteisia tietoja.

### Tarkoitus

Havaitaan ja estetään henkilöiden tai järjestelmien tekemä tietojen luvaton paljastaminen ja kerääminen.

### Ohjeistus

Tietovuotoriskien lieventämiseksi organisaation olisi tarkasteltava seuraavia asioita:

- Tiedot yksilöidään ja luokitellaan niiden vuotamisen estämiseksi (esim. henkilötiedot, hintamallit ja tuotetiedot).
- Tietovuotojen kanavia valvotaan (esim. sähköposti, tiedostonsiirto, mobiililaitteet ja siirrettävä tallennusvälineet).
- Tietojen vuotaminen pyritään estämään omilla toimilla (esim. arkaluonteisia tietoja sisältävien sähköpostiviestien karanteeniin laittaminen).

Tietovuotojen estotyökaluilla olisi

- yksilötävä arkaluonteiset tiedot, joihin kohdistuu luvattoman paljastamisen riski, ja valvottava niitä (esim. käyttäjän järjestelmässä oleva rakenteeton tietoaineisto)
- havaittava arkaluonteisten tietojen paljastamiset (esim. kun tietoja ladataan ei-luotetun kolmannen osapuolen pilvipalveluun tai lähetetään sähköpostilla)
- estettävä käyttäjätoiminnot tai verkkosiirrot, jotka paljastavat arkaluonteisia tietoja (esim. estetään tietokantakohteiden kopioiminen laskutaulukkoon).

Organisaation olisi määritettävä, onko tarpeen rajoittaa käyttäjien kykyä kopioida ja liimata tai ladata tietoa organisaation ulkopuolisille palveluihin, laitteisiin ja tallennusvälineisiin. Jos rajoittaminen on tarpeen, organisaation olisi otettava käyttöön teknologioita, kuten tietovuotojen estotyökaluja, tai konfiguroitava olemassa olevia työkaluja, jotta käyttäjät pystyvät käyttämään ja muokkaamaan tietoja etäyhteyden avulla, mutta samalla estetään tietojen leikkaaminen ja liimaaminen organisaation hallinnan ulkopuolelle.

Jos tietoja on vietävä organisaation ulkopuolelle, tietojen omistajalle olisi annettava mahdollisuus hyväksyä viesti ja asettaa käyttäjät vastuullisiksi toimistaan.

Kuvakaappausten ja valokuvien ottaminen näytöstä olisi estettävä käyttöehojen, koulutuksen ja auditoinnin avulla.

Kun tietoja varmuuskopioidaan, olisi varmistettava, että arkaluonteisia tietoja suojataan eri toimenpitein, kuten varmuuskopion sisältävän tallennuslaitteen salauksella, pääsynhallinnalla ja fyysisellä suojauksella.

Tietovuotojen estämistä olisi myös tarkasteltava suojausseura vastapuolen tiedustelutoimia vastaan, jottei organisaation tai yhteiskunnan kannalta kriittistä luottamuksellista tai salaista (esim. geopoliittista, ihmisiä koskevaa, talouteen liittyviä, kaupallisia, tieteellisiä tai muun tyypissä) tietoa päädy väärin käsiin. Tietovuotojen estämiseen tähtäävät toimenpiteet olisi suunniteltava siten, että ne pyrkivät hämäämään vastapuolen päätöksentekoa, esim. korvaamalla oikeat tiedot väärillä. Tätä olisi tehtävä joko yksittäisinä toimenpiteinä tai vasteena kilpailijan tiedustelutoimiin. Esimerkkejä tällaisista toimenpiteistä ovat sosiaalinen tiedustelu tai ns. hunajapurkkiyhökkäykset.

## Lisätiedot

Tietovuotojen estämistyökalut on suunniteltu tunnistamaan tietoja, seuraamaan tietojen käyttöä ja liikkumista sekä tekemään toimenpiteitä, joilla estetään tietojen vuotaminen (esim. huomautetaan käyttäjille riskialttiista käytöksestä ja estämällä tietojen siirto siirrettäviin tallennusvälineisiin).

Tietovuotojen estämiseen liittyy luontaisesti henkilöstön viestinnän ja verkkokäytäytymisen seuraaminen sekä tähän liittyen ulkoisten tahojen viestien seuraaminen. Tästä syntyy juridisia kysymyksiä, jotka olisi selvitetävä ennen tietovuotojen estötöökalujen käyttöönnottoa. Yksityisyysystä, tietosuoja, työsuheteita, tietojen sieppaamista ja televiestintää koskevia lakeja on paljon, ja niistä osaa sovelletaan tietovuotojen estämiseen liittyvään tietojen käsittelyyn ja seurantaan.

Tietovuotojen estämistä voidaan tukea standardoiduilla turvallisuuksilla hallintakeinoilla, kuten pääsynhallintaa ja turvallista asiakirjojen hallintaa koskevissa kohdennetuilla toimintaperiaatteilla (ks. [kohdat 5.12 ja 5.15](#)).

## 8.13 Tietojen varmuuskopiointi (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Korjaava	#Eheys #Saatavuus	#Palautus	#Jatkuvuus	#Suojaaminen

### Hallintakeino

Tiedoista, ohjelmistoista ja järjestelmistä olisi otettava varmuuskopiot ja ne olisi testattava säännöllisesti varmuuskopointia koskevien kohdennettujen toimintaperiaatteiden mukaisesti.

### Tarkoitus

Mahdollistetaan toipuminen tietojen tai järjestelmien menetyksestä.

### Ohjeistus

Olisi laadittava varmuuskopointia koskevat kohdennetut toimintaperiaatteet, joilla täytetään organisaation tietojen säilyttämistä ja tietoturvallisuutta koskevat vaatimukset.

Olisi otettava riittävät varmuuskopiot, jotta voidaan varmistaa, että kaikki tärkeät tiedot ja ohjelmat voidaan palauttaa tallennusvälineen häiriötilanteen, vikaantumisen tai menetyksen jälkeen.

Olisi laadittava suunnitelmat siihen, miten organisaation varmuuskopioi tietoja, ohjelmistoja ja järjestelmiä, sekä toteutettava tämä suunnitelma, jotta voidaan noudattaa varmuuskopointia koskevia kohdennettuja toimintaperiaatteita.

Varmuuskopointisuunnitelman suunnittelussa olisi otettava seuraavat ohjeet huomioon:

- Varmuuskopioista ja dokumentoiduista palautusmenettelyistä tuotetaan tarkat ja täydelliset tallenteet.
- Varmuuskopioiden laajuudessa (esim. täydelliset tai eroavuusvarmistus) ja ottovälissä otetaan huomioon organisaation liiketoiminnalliset vaatimukset (esim. palautustavoite, ks. [kohta 5.30](#)), asiaan liittyviä tietoja koskevat turvallisuusvaatimukset sekä tietojen kriittisyyys organisaation toiminnan jatkumisen kannalta.
- Varmuuskopiot varastoidaan erillään olevaan turvalliseen ja suojaatun paikkaan, joka on riittävän kaukana vältykseen pääkäytöpaikalla tapahtuvan katastrofin aiheuttamalta vahingolta.

- d) Varmuuskopioiden tiedot suojataan sekä fyysisesti että ympäristöuhilta (ks. [kohdat 7](#) ja [8.1](#)) pääkäyttöpaikalla noudatettavan vaatimustason mukaisesti.
- e) Varmuuskopioiden tallennusvälineet testataan säännöllisesti, jotta varmistuttaisiin siitä, että niihin voidaan luottaa hätätilanteessa. Varmuuskopioidun tiedon palautustestaus toteutetaan määritellyllä testijärjestelmällä, eikä ylikirjoittamalla alkuperäistä tietoa, sillä varmuuskopointi- tai palautusprosessin epäonnistuminen voisi aiheuttaa korjaamatonta vahinkoa tai hävikkää.
- f) Varmuuskopioita suojataan tunnistettujen riskien mukaisella salauksella (esim. jos luottamuksellisuus on tärkeää).
- g) Varmistetaan, että tahaton tietojen häviäminen havaitaan ennen seuraavan varmuuskopion ottamista.

Toimintaohjeiden avulla olisi seurattava varmuuskopioiden toteuttamista ja niissä olisi varauduttava aikataulutettujen varmuuskopioiden epäonnistumiseen, jotta voidaan varmistaa varmuuskopioiden kattavuus varmuuskopointia koskevien kohdennettujen toimintaperiaatteiden mukaisesti.

Yksittäisiä järjestelmiä ja palveluita koskevat varmuuskopointitoimet olisi testattava säännöllisesti, jotta voidaan varmistaa, että ne täytävät häiriötilannevastetta ja liiketoiminnan jatkuvuussuunnitelmaa koskevat tavoitteet (ks. [kohta 5.30](#)). Tämä olisi yhdistettävä palauttamismenetelyjen testaukseen, ja se olisi tarkistettava suhteessa liiketoiminnan jatkuvuussuunnitelmassa vaadittuun palauttamisaikaan. Kriittisissä järjestelmissä ja palveluissa varmuuskopointitoimien olisi katettava kaikki järjestelmän tiedot, sovellukset ja aineistot, joita tarvitaan järjestelmän täydelliseen palauttamiseen katastrofin sattuessa.

Kun organisaatio käyttää pilvipalvelua, organisaation pilvipalvelussa olevista tiedoista, sovelluksista ja järjestelmistä olisi otettava varmuuskopiot. Organisaation olisi määritettävä, täytyvätkö varmuuskopointia koskevat vaatimukset ja millä tavoin, kun käytetään pilvipalvelun osana tarjottua tietojen varmuuskopointipalvelua.

Oleellisten liiketoimintatietojen säilytysaika olisi määritettävä ottaen huomioon mahdolliset vaatimukset säilyttää arkistokopiot. Organisaation olisi tarkasteltava sitä, miten tiedot poistetaan (ks. [kohta 8.10](#)) varmuuskopointiin käytetyiltä tallennusvälineiltä, kun tietojen säilytysaika on kulunut. Tässä olisi otettava huomioon lait ja viranomaismääräykset.

## Lisätiedot

Lisätietoa varastoinnin turvallisuudesta ja säilytysajoista löytyy standardista ISO/IEC 27040.

## 8.14 Tietojenkäsittelypalvelujen vikasietoisuus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Saatavuus	#Suojaus	#Jatkuvuus #Omaisuudenhallinta	#Suojaaminen #Krisinkestävyys

## Hallintakeino

Tietojenkäsittelypalvelut olisi toteutettava niin vikasietoisina, että saatavuusvaatimukset täytyvät.

## Tarkoitus

Varmistetaan tietojenkäsittelypalvelujen jatkuva toiminta.

## Ohjeistus

Organisaation olisi yksilöitvä liiketoimintojen ja tietojärjestelmien saatavuutta koskevat vaatimukset. Organisaation olisi suunniteltava ja otettava käyttöön järjestelmäarkkitehtuuri, jossa on riittävästi vikasietoisuutta tämän vaatimuksen täyttämiseen.

Vikasietoisuus voidaan toteuttaa tietojenkäsittelypalveluiden toisintamisella osittain tai kokonaisuudessaan (eli varaosilla tai kahdella täydellisellä kokonaisuudella). Organisaation olisi suunniteltava ja toteutettava menettelyt varalla olevien komponenttien ja käsittelypalveluiden

käynnistämiseen. Menettelyistä olisi selvittävä, ovatko nämä komponentit ja käsitellytoiminnot aina pääällä vai käynnistyvätkö ne vain hätätilanteissa joko automaattisesti tai manuaalisesti. Varalla olevien komponenttien ja tietojenkäsittelypalveluiden olisi varmistettava sama turvallisuustaso kuin varsinaistenkin palveluiden.

Käytössä olisi oltava mekanismit, joilla organisaatiolle hälytetään mahdollisiin vikatilanteisiin tietojenkäsittelypalveluissa, tarjotaan mahdollisuus toteuttaa suunnitellut menettelyt ja mahdolistetaan jatkuva saatavuus tietojenkäsittelypalveluiden korjausten tai korvaamisen aikana.

Varajärjestelmien toteuttamisessa organisaation olisi tarkasteltava seuraavia asioita:

- a) Solmitaan sopimuksia kahden tai useamman verkkojen ja kriittisten tietojenkäsittelypalveluiden toimittajien, kuten internetsalvelutarjoajien, kanssa.
- b) Käytetään eriytettyjä verkkoa.
- c) Käytetään kahta maantieteellisesti eriytettyä datakeskusta, joissa on peilatut järjestelmät.
- d) Käytetään fyysisesti kahdennettuja virransyöttöjä ja virtalähteitä.
- e) Käytetään useita rinnakkaisia ohjelmistoinstansseja, joiden välillä on automaattinen kuormanjako (saman datakeskuksen tai eri datakeskusten välillä).
- f) Järjestelmissä käytetään kahdennettuja komponentteja (esim. suoritin, kiintolevy, muistit) tai verkkoa (esim. palomuurit, reitittimet, kytkimet).

Toiminnoiltaan kahdennetut tietojärjestelmät olisi mahdollisuksien mukaan testattava, ja se olisi suositeltavaa tehdä tuotantokäytössä, jotta voidaan varmistaa, että vian ilmetessä siirtyminen komponentista toiseen toimii tarkoitettuksi.

### Lisätiedot

Vikasietoisuudella ja liiketoiminnan jatkuvuutta koskevalla tieto- ja viestintäteknisellä valmiudella on vahva keskinäinen suhde (ks. [kohta 5.30](#)), etenkin kun edellytetään lyhyitä palautumisaikoja. Monet vikasietoustoimet voivat olla osa tieto- ja viestintäteknisen jatkuvuuden strategioita ja ratkaisuja.

Toiminnoiltaan päälekkäisten komponenttien toteuttaminen voi synnyttää riskejä, jotka koskevat tiedon ja tietojärjestelmien eheyttä (esim. tietojen kopiointiprosessi kahdennettuihin komponentteihin voi synnyttää virheitä) tai luottamuksellisuutta (esim. kahdennettujen komponenttien heikot turvallisuuden hallintakeinot voivat johtaa tietojen vaarantumiseen), mikä on otettava huomioon tietojärjestelmäsuunniteltaessa.

Tietojenkäsittelypalveluiden vikasietoisuus ei yleensä kata sovellusten sisällä tapahtuvista vikaantumisista johtuvia sovellusten käyttökatkoksiakin.

Julkisen pilvipalvelun avulla on mahdollista ylläpitää useita tietojenkäsittelypalvelujen käytössä olevia versioita, jotka sijaitsevat useammissa fyysisissä sijainneissa ja joissa on toimintojen automaattinen siirto vikaantumistilanteissa ja kuormanjako.

Joitain vikasietoisuutta lisääviä ja automaattisten toimintojen siirron pilvipalveluissa mahdolistavia teknologioita ja tekniikoita käsitellään teknisessä spesifikaatiossa ISO/IEC TS 23167.

### 8.15 Lokkirjaukset (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto	#Tietoturvatapahtumien_hallinta	#Suojaaminen #Puolustus

## Hallintakeino

Olisi luotava tapahtumaloakeja, joihin tallennetaan toiminnot, poikkeamat, vikaantumiset ja muut olennaiset tapahtumat. Nämä lokit olisi säilytettävä, ja niitä olisi suojattava ja analysoitava.

## Tarkoitus

Tallennetaan tapahtumat, luodaan todistusaineisto, varmistetaan lokitietojen eheys, estetään luvaton pääsy, tunnistetaan tietoturvatapahtumat, jotka voivat johtaa tietoturvahäiriöihin, ja tuetaan mahdollisia tutkimuksia.

## Ohjeistus

### Yleistä

Organisaation olisi määritettävä tapahtumalokien tarkoitus, mitä tietoja niihin kerätään ja kirjataan sekä lokitietojen suojaamista ja käsittelyä koskevat lokikohtaiset vaatimukset. Nämä vaatimukset olisi dokumentoitava lokikirjauksia koskeviin kohdennettuihin toimintaperiaatteisiin.

Tapahtumaloakeihin olisi sisällytettävä seuraavat asiat kullekin tapahtumalla tarpeen mukaan:

- a) käyttäjätunnukset
- b) järjestelmän toiminnot
- c) tärkeiden tapahtumien päivämäärät, kellonajat ja yksityiskohdat (esim. sisään- ja uloskirjautumiset)
- d) laitteen tunniste, järjestelmän tunniste ja sijainti
- e) verkko-osoitteet ja käytännöt.

Seuraavien tapahtumien kirjaamista olisi harkittava:

- a) onnistuneet ja epäonnistuneet yritykset päästää järjestelmään
- b) onnistuneet ja epäonnistuneet yritykset päästää tietoihin tai muihin resursseihin
- c) järjestelmäkonfiguraation muutokset
- d) ylläpito-oikeuksien käyttö
- e) apuohjelmien ja sovellusten käyttö
- f) tarkastellut tiedot ja pääsyn tyyppi sekä mahdollinen tärkeiden tiedostojen poistaminen
- g) pääsynhallintajärjestelmän hälytykset
- h) suojausjärjestelmien, kuten viristorjunnan ja tunkeutumisen havaitsemisjärjestelmien, kytkeminen päälle ja pois
- i) identiteettien luominen, muokkaus tai poistaminen
- j) käyttäjien sovelluksissa tekemät transaktiot. Joissain tapauksissa sovellukset ovat kolmannen osapuolen toimittamia tai operoimia palveluita tai tuotteita.

Kaikilla järjestelmillä on tärkeää olla synkronoidut aikalähteet (ks. [kohta 8.17](#)), koska tämä mahdollistaa eri järjestelmien lokitietojen korreloinnin häiriötilanteiden analysointiin, niistä hälyttämiseen ja niiden tutkimiseen.

### Tapahtumalokien suojaaminen

Edes ylläpito-oikeuksin varustetuilla käyttäjillä ei saisi olla lupaa poistaa tai kytkeä pois lokeja omista tekemisistään. Muuten käyttäjät voivat manipuloida suorassa hallinnassaan olevien tietojenkäsittelypalveluiden lokeja. Lokeja on tärkeää suojata ja katselmoida, jotta ylläpito-oikeuksin varustettujen käyttäjien vastuu kyetään säilyttämään.

Hallintakeinojen olisi pyrittävä suojaamaan lokitietojen luvattomilta muutoksilta ja lokitietopalvelun toimintahäiriöiltä, joita voivat olla

- a) tallennettavien sanomatyyppien muutokset
- b) lokitiedostojen muokkaaminen tai poistaminen
- c) tapahtumien tallentamisen epäonnistuminen tai aiempien tallennettujen tapahtumien ylikirjoittaminen, jos lokitiedoston sisältävä tallennusväline on täynnä.

Tapahtumalokien suojaamiseen olisi harkittava seuraavia tekniikoita: salaustiivisteet, tallenteiden tekeminen tiedostoina, joihin voi vain lisätä tietoa tai lukea jo siellä olevaa tietoa, tallentaminen julkisen avoimuuden tiedostoon.

Joidenkin tapahtumalokien arkistoimista voidaan edellyttää osana tallenteiden säilyttämisen politiikkaa tai todisteiden keräämisen ja säilyttämisen vaatimuksia (ks. [kohta 5.28](#)).

Jos organisaation on lähetettävä järjestelmien tai sovellusten lokitiedostoja toimittajalle virheiden poistoa tai ongelmanratkaisua varten, lokitiedostot olisi mahdollisuksien mukaan puhdistettava tietojen peittämistekniikoilla (ks. [kohta 8.11](#)) henkilötiedoista, kuten käyttäjänimistä, IP-osoitteista, isäntäkoneen tunnisteista tai organisaation nimestä, ennen kuin tiedot lähetetään toimittajalle.

Tapahtumalokit voivat sisältää arkaluonteista tietoa ja henkilötietoja. Olisi noudatettava asianmukaisia tietosuojatoimenpiteitä (ks. [kohta 5.34](#)).

#### Lokien analysointi

Lokien analysoinnin olisi katettava tietoturvatapahtumien analysointi ja tulkinta, jotta siitä on apua epätavallisen tai pahantahtoisen toiminnan tai käyttäytymisen tunnistamisessa, sillä ne voivat viitata tietojen vaarantumiseen.

Tapahtumien analysoinnissa olisi otettava huomioon seuraavat asiat:

- a) analyysin tekeviltä asiantuntijoilta vaaditut taidot
- b) lokien analysointimenettelyjen määrittäminen
- c) kultakin turvallisuteen liittyvältä tapahtumalta vaaditut attribuutit
- d) ennalta määritettyihin sääntöihin perustuva poikkeamien tunnistaminen (turvallisuteen liittyvien tietojen ja tapahtumien hallinta tai palomuureja koskevat säännöt, tunkeutumisen havaitsemisjärjestelmät tai haittaohjelmien merkit)
- e) tiedossa olevat käyttäytymismallit ja normaali verkkoliikenne verrattuna poikkeavaan toimintaan ja käytökseen (käyttäjien ja tahojen käyttäytymisen analysointi)
- f) kehityssuuntien tai -mallien analysoinnista saadut tulokset (esim. tietojen analysoinnin tulokset, massadatan käyttötekniikat ja erikoistuneet analysointityökalut)
- g) saatavilla oleva uhkatiedon seuranta.

Lokien analysointia olisi tuettava määritellyillä valvontatoiminoilla, jotta siitä on apua poikkeavan käyttäytymisen tunnistamisessa ja analysoinnissa. Tällaisia toimintoja ovat

- a) suojauttuihin resursseihin kohdistuneiden onnistuneiden ja epäonnistuneiden käyttöyritysten katselointi (esim. DNS-palvelimet, verkkoportaalit ja tiedostojenjakopalvelut)
- b) DNS-lokien tarkistaminen, jotta kyötään tunnistamaan ulospäin otetut verkkoyhteydet pahantahtoisiiin palvelimiin, kuten bottiverkkojen komentopalvelimiin
- c) palveluntuottajilta saatujen käyttöraporttien (esim. laskujen tai palveluraporttien) tarkastelu järjestelmissä ja verkoissa tapahtuneen poikkeavan käytön havaitsemiseksi (esim. katselmoimalla toimintamalleja)

- d) fyysisen seurannan, kuten saapumisen ja poistumisen, tapahtumalokien sisällyttäminen, jotta varmistetaan tarkempi havaitseminen ja häiriötilanteiden analysointi
- e) lokien korrelointi, jotta mahdollistetaan tehokas ja erittäin tarkka analysointi.

Epäillyt ja todelliset tietoturvahäiriöt olisi tunnistettava (esim. haittaohjelmatartunta tai palomuurien murtoyritykset), ja niitä olisi tutkittava tarkemmin (esim. osana tietoturvahäiriöiden hallintaprosessia, ks. [kohta 5.25](#)).

## Lisätiedot

Järjestelmälokit sisältävät usein runsaasti tietoa, josta suuri osa on tietoturvallisuuden tarkkailun kannalta epäolennaista. Jotta tietoturvallisuuden tarkkailun kannalta merkittäväät tapahtumat saadaan tunnistettua, olisi harkittava tarkoituksemukaisten apuohjelmien tai tarkastustyökalujen käyttöä tiedostojen läpikäymisessä.

Tapahtumien kirjaaminen muodostaa perustan automaattisille valvontajärjestelmille (ks. [kohta 8.16](#)), jotka kykenevät tuottamaan yhdistettyjä järjestelmän turvallisuutta koskevia raportteja ja hälytyksiä.

Turvallisuuteen liittyvien tietojen ja tapahtumien hallintatyökaluilla tai vastaavilla palveluilla voidaan tallentaa, korreloida, normalisoida ja analysoida lokitietoja sekä luoda hälytyksiä. Turvallisuuteen liittyvien tietojen ja tapahtumien hallinta vaatii yleensä tarkkaa konfigurointia, jotta sen hyödyt voidaan optimoida. Tarkasteltaviin konfiguraatioihin sisältyvät asianmukaisten lokilähteiden tunnistaminen ja valinta, sääntöjen hienosäätö ja testaus sekä käyttötapausten kehittäminen.

Julkisia läpinäkyvyystiedostoja käytetään lokien tallentamisessa esimerkiksi sertifikaatteihin liittyvissä läpinäkyvyysjärjestelmissä. Tällaiset tiedostot voivat tarjota ylimääräisen havaitsemismekanismin, joka on hyödyllinen lokien luvattoman muuttamisen estämisessä.

Pilviympäristöissä lokien hallintavastutut voivat jakautua pilvipalvelun tuottajaan ja pilvipalvelun asiakkaan välille. Nämä vastut vaihtelevat käytetyn pilvipalvelun tyypistä riippuen. Lisähjelmosta löytyy standardista ISO/IEC 27017.

## 8.16 Valvontatoiminnot ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Havaitseva	#Luottamuksellisuus	#Havainto #Vaste	#Tietoturva-tapahtumien_hallinta	#Puolustus
#Korjaava	#Eheys #Saatavuus			

### Hallintakeino

Verkkoja, järjestelmiä ja sovelluksia olisi valvottava poikkeavan käyttäytymisen varalta, ja mahdollisia tietoturvahäiriöitä olisi arvioitava asianmukaisin toimenpitein.

### Tarkoitus

Havaitaan poikkeava käyttäytyminen ja mahdolliset tietoturvahäiriöt.

### Ohjeistus

Valvonnan laajuus ja taso olisi määritettävä liiketoiminnallisten ja tietoturvallisuutta koskevien vaatimusten perusteella ottaen huomioon olennaiset lait ja viranomaismääräykset. Valvonnan tallenteita olisi ylläpidettävä määritelty säilytsaika.

Seuraavien asioiden valvonnan sisällyttämistä valvontajärjestelmään olisi harkittava:

- a) verkon, järjestelmän ja sovelluksen sisään- ja ulospäin suuntautuva liikenne
- b) pääsy järjestelmiin, palvelimiin, verkkolaitteisiin, valvontajärjestelmiin, kriittisiin sovelluksiin jne.
- c) kriittisen tai pääkäyttäjätason järjestelmän ja verkon konfiguraatiotiedostot

- d) turvallisuustyökalujen tapahtumalokit (esim. virustorjunta, tietomurtohälytin, tunkeutumisenestojärjestelmä, verkkosuodattimet, palomuurit, tietovuotojen estäminen)
- e) järjestelmän ja verkon käyttöön liittyvät tapahtumalokit
- f) varmistetaan, että suoritettavaa ohjelmistokoodia on sallittua ajaa järjestelmässä ja että sitä ei ole luvattomasti muutettu (esim. käänämällä sitä uudelleen, jotta siihen voidaan lisätä haittakoodia)
- g) resurssien (esim. suoritin, kiintolevy, muisti, kaistanleveys) käyttö ja suorituskyky.

Organisaation olisi laadittava normaalin käyttäytymisen vertailukohta ja tarkasteltava poikkeamia siihen nähden. Vertailukohdan laatimisessa olisi otettava huomioon

- a) järjestelmien käytön katselointi sekä normaalialikana että huippuaikana
- b) kunkin käyttäjän tai käyttäjäryhmän yleiset käyttöajat, -sijainnit ja -taajuus.

Valvontajärjestelmä olisi konfiguroitava suhteessa laadittuun vertailukohtaan, jotta kyetään tunnistamaan poikkeava käyttäytyminen, kuten

- a) prosessien tai sovellusten suunnittelematon sammuttaminen
- b) haittaohjelmiin yleisesti liitettyt toiminnot tai haitallisista IP-osoitteista tai verkkoalueista (kuten bottiverkkojen komentopalvelimista) peräisin oleva liikenne
- c) tunnetut hyökkäysprofiilit (esim. palvelun esto tai puskurin ylivuoto)
- d) järjestelmän poikkeava käyttö (esim. näppäilyjen tallentaminen, prosessien väliin ajaminen ja poikkeamat normaalimenettelyistä)
- e) pullonkaulat ja ylikuormitukset (esim. verkkojonotus, latenssitasot ja verkon viivevaihtelu)
- f) järjestelmien tai tietojen luvaton käyttö (onnistunut tai yritys)
- g) liiketoimintasovellusten, -järjestelmien ja verkkojen luvaton skannaus
- h) suojaattuihin resursseihin kohdistuneet onnistuneet ja epäonnistuneet käyttöyritykset (esim. DNS-palvelimet, verkkoportaalit ja tiedostojärjestelmät)
- i) järjestelmän ja käyttäjän poikkeava käyttäytyminen odotettuun käyttäytymiseen verrattuna.

Valvonnan olisi oltava jatkuvaa ja se olisi toteutettava valvontatyökalulla. Valvonnan olisi oltava reaaliaikaista tai se olisi toteutettava säännöllisin aikavälein organisaation tarpeiden ja kyvykkyyksien mukaisesti. Valvonnan työkalujen olisi sisällettävä kyky käsittellä suuria tietomääriä, mukautua jatkuvasti muuttuvaan uhkaympäristöön ja mahdollistaa reaaliaikaiset ilmoitukset. Työkalujen olisi myös pystyttävä tunnistamaan tietyt merkit sekä tietojen, verkon tai sovelluksen käyttäytymismallit.

Automatisoitu valvontaohjelmisto olisi konfiguroitava tuottamaan hälytykset (esim. hallintakonsoleiden, sähköpostiviestien tai pikaviestien kautta) ennalta määritellyjen kynnyssarvojen perusteella. Hälytysjärjestelmät olisi hienosäädetävä ja kalibroitava organisaation vertailukohtaan, jotta vältytään vääriltä positiivisilta. Henkilöstön olisi oltava sitoutunutta reagoimaan hälytyksiin ja sen olisi oltava riittävästi koulutettua tulkitsemaan oikein mahdolliset häiriötilanteet. Käytössä olisi oltava päallekkäisiä järjestelmiä ja prosesseja, jotta hälytysilmoitukset otetaan vastaan ja niihin reagoidaan.

Poikkeavista tapahtumista olisi viestittävä olennaisille sidosryhmileille, jotta seuraavia toimintoja voidaan parantaa: auditointi, turvallisuuden arvointi, haavoittuvuuksien tarkkailu ja seuranta (ks. [kohta 5.25](#)). Käytössä olisi oltava menettelyt, joilla reagoidaan valvontajärjestelmästä saatuihin positiivisiin indikaattoreihin viivyttellemättä, jotta voidaan minimoida tietoturvallisuuteen kohdistuvien haitallisten tapahtumien (ks. [kohta 5.26](#)) vaikutukset. Olisi laadittava myös menettelyt väärrien positiivisten tunnistamiseen ja käsittelyyn sisältäen myös valvontajärjestelmän hienosäätämisen, jotta väärrien positiivisten määrää kyetään vähentämään.

## Lisätiedot

Turvallisuuden valvontaa voidaan tehostaa

- a) hyödyntämällä uhkatiedon seurannan järjestelmiä (ks. [kohta 5.7](#))
- b) hyödyntämällä koneoppimisen ja tekoälyn kyvykkyyksiä
- c) käyttämällä esto- ja lupalistoja
- d) toteuttamalla joukko teknisiä turvallisuusarvointeja (esim. haavoittuvuuksien arvointi, tunkeutumistestaus, kyberhyökkäysten simulaatiot ja kybervasteiden harjoitukset), joiden tuloksien avulla kyetään määrittämään vertailukohdat ja hyväksyttävä käyttäytyminen
- e) käyttämällä suorituskyvyn valvontajärjestelmiä, joista on apua poikkeavan käyttäytymisen määrittelemisessä ja havaitsemisessa
- f) hyödyntämällä lokeja yhdessä valvontajärjestelmien kanssa.

Valvontatoiminnot suoritetaan yleensä erikoistuneilla ohjelmistoilla, kuten tietomurtohälyttimeillä. Näihin voidaan konfiguroida vertailukohdat järjestelmän ja verkon normaalille, hyväksyttävälle ja odotetulle käytölle.

Poikkeavan viestinnän valvonnalla pystytään tunnistamaan bottiverkot (eli joukko laitteita, jotka ovat bottiverkon omistajan pahantahtoisessa hallinnassa ja joilla yleensä tehdään hajautettuja palvelunestohyökkäyksiä muiden organisaatioiden tietokoneiden kimppuun). Jos tietokone on ulkoisen laitteen hallinnassa, tartunnan saaneen laitteen ja isäntälaitteen välillä on viestintää. Organisaation olisi tästä syystä käytettävä teknologiaita, joilla valvotaan poikkeavaa viestintää, sekä tehtävä tarvittavat toimenpiteet.

## 8.17 Kellojen synkronointi (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Havaitseva	#Eheys	#Suojaus #Havainto	#Tietoturvatapahtumien_hallinta	#Suojaaminen #Puolustus

### Hallintakeino

Organisaatiossa käytettävien tietojenkäsittelyjärjestelmien kellojen olisi oltava synkronoituja hyväksyttävien aikalähteiden kanssa.

### Tarkoitus

Mahdollistetaan turvallisuuteen liittyvien tapahtumien ja muiden tallennettujen tietojen korrelointi ja analysointi sekä tietoturvahäiriöiden tutkinnan tukeminen.

### Ohjeistus

Ajan esittämistä, luotettavaa synkronointia ja tarkkuutta koskevat sisäiset ja ulkopuoliset vaatimukset olisi dokumentoitava ja toteutettava. Nämä vaatimukset voivat olla peräisin laeista, asetuksista, viranomaismääräyksistä, sopimuksista, standardeista ja sisäisen valvonnan tarpeista. Organisaatiossa käytettävä vertailuaika olisi määriteltävä, ja sitä olisi käytettävä kaikissa järjestelmissä, myös rakennusten hallintajärjestelmissä, saapumis- ja poistumisjärjestelmissä sekä muissa tutkintaa mahdollisesti avustavissa järjestelmissä.

Kansallisen atomikellon radioaikalähetykseen tai GPS-järjestelmään liitettyä kelloa olisi käytettävä lokijärjestelmien pääkellona. Nämä varmistetaan yhdenmukainen ja luotettava päivämäärien ja kellonaikojen lähde ja voidaan varmistaa tarkat aikaleimat. Määriteltyjä käytäntöjä, kuten verkkoaikeayteksykäytäntöä (NTP) tai tarkka-aikakäytäntöä (PTP), olisi käytettävä kaikkien verkotettujen järjestelmien pitämisessä synkronoituna pääkellon kanssa.

Organisaatio voi käyttää kahta ulkoista aikalähettä samaan aikaan parantaakseen sisäisten kellojen luotettavuutta ja hallitakseen asianmukaisesti vaihtelua.

Kellojen synkronointi voi olla haastavaa useampien pilvipalveluiden välillä tai kun käytetään sekä pilvipalvelua että sisäisiä palveluita. Näissä tapauksissa kummankin palvelun kelloa olisi seurattava ja niiden välinen ero olisi kirjattava ylös, jotta voidaan lieventää aikojen erosta johtuvia riskejä.

## Lisätiedot

Tietokoneiden kellonajan oikea asetus on tärkeä, sillä sen avulla pyritään takaamaan tutkimuksiin tai todisteeksi oikeus- tai kurinpitotapauksissa mahdollisesti tarvittavien tapahtumalokien täsmällisyys. Epätarkat tapahtumalokit voivat vaikuttaa tällaisia tutkimuksia tai vahingoittaa tällaisten todisteiden uskottavuutta.

## 8.18 Ylläpito- ja hallintasovellukset (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ ja_verkon_turvallisus #Turvallinen_konfigurointi #Sovelluksen_turvallisus	#Suojaaminen

### Hallintakeino

Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käyttöä olisi rajoitettava, ja niitä olisi hallittava tarkasti.

### Tarkoitus

Varmistetaan, että apuohjelmien käyttö ei heikennä tietoturvallisuteen liittyvien järjestelmien ja sovellusten hallintakeinojen toimintaa.

### Ohjeistus

Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käytössä olisi otettava huomioon seuraavat ohjeet:

- a) apuohjelmien käytön rajoittaminen niin harvalle luotettavalle, luvalliselle käyttäjälle kuin käytännössä mahdollista (ks. [kohta 8.2](#))
- b) tunnistamis-, todennus- ja oikeuksien myöntämismenetelyjen käyttö apuohjelmissa, mukaan lukien apuohjelmaa käyttävän henkilön ainutkertainen tunnistus
- c) apuohjelmien valtuustasojen määrittelemisen ja dokumentointi
- d) apuohjelmien tilapäiskäytön myöntäminen
- e) apuohjelmien asettaminen sellaisten käyttäjien ulottumattomiin, joilla on pääsy tehtävien eriyttämistä edellyttävissä järjestelmissä oleviin sovelluksiin.
- f) kaikkien tarpeettomien apuohjelmien poistaminen tai niiden käytön estäminen
- g) vähintään apuohjelmien looginen erottaminen sovellusohjelmista, sekä mahdolisuuksien mukaan näiden ohjelmien verkkoviestinnän erottaminen sovellusten aiheuttamasta liikenteestä
- h) apuohjelmien käytettävyyden rajoittaminen (esim. luvallisen muutoksen keston ajaksi)
- i) apuohjelmien kaiken käytön kirjaaminen.

## Lisätiedot

Useimmissa tietojärjestelmissä on yksi tai useampi apuohjelma, jolla voi olla mahdollista ohittaa järjestelmän tai sovelluksen hallintakeinot, esim. diagnostiikka, päivittäminen, virustorjunta, levyjen eheyttäjä, virheenkorjaimet, varmuuskopiointi- ja verkkotyökalut.

## 8.19 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi #Sovelluksen_turvallisuus	#Suojaaminen

### Hallintakeino

Olisi toteutettava menettelyt ja toimet, joilla hallitaan turvallisesti ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin.

### Tarkoitus

Varmistetaan tuotantokäytössä olevien järjestelmien eheys ja estetään teknisten haavoittuvuuksien hyödyntäminen.

### Ohjeistus

Tuotantokäytössä olevissa järjestelmissä olevien ohjelmistojen muutosten ja asennusten turvallisessa hallinnassa olisi otettava huomioon seuraavat ohjeet:

- Vain koulutetut pääkäyttäjät päivittävät tuotantokäytössä olevat ohjelmistot saatuaan asianmukaisen valtuutuksen johdolta (ks. [kohta 8.5](#)).
- Varmistetaan, että tuotantokäytössä olevat järjestelmät sisältävät vain hyväksyttyä suorituskelvoista koodia, ei kehityskoodia tai käänräjäitä.
- Ohjelmistot ja päivitykset asennetaan vain laajan ja onnistuneen testauksen jälkeen (ks. [kohdat 8.29 ja 8.31](#)).
- Kaikki vastaavat ohjelmistojen lähdekirjastot päivitetään.
- Kaikkia tuotantokäytössä olevia ohjelmistoja samoin kuin järjestelmädokumentaatiota hallitaan konfiguraationhallintajärjestelmällä.
- Ennen muutosten toteuttamista määritellään palautusstrategia.
- Tuotantokäytössä olevien ohjelmistojen kaikista päivityksistä ylläpidetään tapahtumalokia.
- Ohjelmistojen vanhat versiot arkistoidaan varatoimenpiteenä yhdessä kaikkien vaadittujen tietojen ja parametriiden, menettelyjen, konfiguraation yksityiskohtien ja tukiohjelmistojen kanssa niin pitkäksi aikaa kuin ohjelmiston edellytetään pystyvän lukemaan tai käsittämään arkistoitua tietoa.

Kaikissa uuden version käyttöönnottoa koskevissa päätöksissä olisi otettava huomioon muutoksen liiketoiminnalliset vaatimukset ja version turvallisuus (esim. version sisältämät uudet tietoturvapiirteet tai sen sisältämien tietoturvahaavoittuvuuksien määrä ja vakavuus). Ohjelmistokorjaukset olisi otettava käyttöön, jos niillä voidaan poistaa tai vähentää tietoturvahaavoittuvuuksia (ks. [kohdat 8.8 ja 8.19](#)).

Tietokoneohjelmistot voivat luottaa ulkopuolisille ohjelmistoihin ja paketteihin (esim. ohjelmistot, jotka käyttävät ulkopuolisia moduuleita), joita olisi tarkkailtava ja hallittava, jotta voidaan estää luvattomat muutokset, koska ne voivat synnyttää tietoturvahaavoittuvuuksia.

Tuotantokäytössä olevien toimittajien toimittamien ohjelmistojen versioita olisi ylläpidettävä siten, että toimittajien tuki säilyy. Ajan myötä ohjelmistotoimittajat lakkavaat tukemasta ohjelmiston vanhoja versioita. Organisaation olisi otettava huomioon tukea vailla olevaan ohjelmistoon luottamisen riskit. Tuotantokäytössä olevissa järjestelmissä käytettäviä avoimen lähdekoodin ohjelmistoja olisi päivitetävä

ohjelmistojen viimeisimpään asianmukaiseen versioon. Ajan myötä avointa lähdekoodia ei enää vältämättä ylläpidetä, mutta se voi silti olla saatavilla avoimen lähdekoodin ohjelmistojen tietokannoissa. Organisaation olisi otettava huomioon myös tukea vailla olevan avoimen lähdekoodin ohjelmiston tuotantokäytössä olevissa järjestelmissä käyttöön liittyvät riskit.

Kun toimittajat asentavat tai päivittävät ohjelmistoja, fyysinen tai ohjelmallinen pääsy olisi annettava vain tarpeen mukaan ja vain tarvittavin valtuuksin. Toimittajan toimenpiteitä olisi valvottava (ks. [kohta 5.22](#)).

Organisaation olisi määriteltävä ja toteutettava tiukat säännöt siitä, minkä tyypisiä ohjelmistoja käyttäjät voivat asentaa.

Tuotantokäytössä oleviin järjestelmiin asennettavien ohjelmistojen kanssa olisi noudatettava vähimmän oikeuden periaatetta. Organisaation olisi yksilöitvä se, minkä tyypiset ohjelmistoasennukset ovat sallittuja (esim. olemassa olevien ohjelmistojen päivitykset ja tietoturvakorjaukset) ja minkä tyypiset asennukset on kielletty (esim. ohjelmisto, jota käytetään vain henkilökohtaiseen käyttöön, ja ohjelmisto, jonka haitallisuutta ei tiedetä tai jonka epäillään olevan haitallinen). Nämä oikeudet olisi myönnettävä kyseessä olevien käyttäjien roolien perusteella.

## Lisätiedot

Ei lisätietoja.

## 8.20 Verkkoturvallisuus ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Verkkoja ja verkossa olevia laitteita olisi suojahtava, hallittava ja valvottava, jotta voidaan suojaata järjestelmissä ja sovelluksissa olevaa tietoa.

### Tarkoitus

Suojataan verkossa olevia tietoja sekä niiden tukena toimivia tietojenkäsittelypalveluita vaarantumiselta verkon kautta.

### Ohjeistus

Olisi toteutettava hallintakeinot, joilla voidaan varmistaa, että verkoissa käsiteltävät tiedot ja niihin liittyvät palvelut on suojaattu luvattomalta pääsyltä. Erityisesti seuraaviin seikkoihin olisi kiinnitettävä huomiota:

- a) verkon tukeman tiedon tyyppi ja luokitustaso
- b) laaditaan verkkolaitteiden ja -välineiden hallinnan vastuut ja menettelyt
- c) ylläpidetään ajantasaista dokumentaatiota, mukaan lukien verkkokaavioita ja laitteiden (esim. reitittimien, kytkinten) konfiguraatiotiedostoja
- d) toimintavastuu verkoista erotetaan tarvittaessa tieto- ja viestintäteknisten järjestelmien hallinnasta (ks. [kohta 5.3](#))
- e) luodaan erityiset hallintakeinot julkisissa verkoissa, kolmannen osapuolen verkoissa tai langattomissa verkoissa kulkevan tiedon luottamuksellisuuden ja eheyden turvaamista sekä niihin liitettyjen järjestelmien ja sovellusten suojaamista varten (ks. [kohdat 5.22, 8.24, 5.14 ja 6.6](#)); myös verkkopalvelujen ja niihin liitettyjen tietokoneiden käytettävyyden ylläpitoon saatetaan tarvita erityisiä hallintakeinoja

- f) toteutetaan asianmukainen lokikirjaaminen ja seuranta, jotta mahdollistetaan tietoturvallisuuteen vaikuttavien, tai sen kannalta olennaisten toimenpiteiden, kirjaaminen ja havaitseminen (ks. [kohdat 8.16 ja 8.15](#))
- g) hallintatoimet koordinoidaan keskenään, jotta voidaan varmistaa sekä liiketoimintapalvelujen optimointi että turvatoimien soveltamisen yhdenmukaisuus kaikissa hankituissa tietojenkäsittelytäytyissä
- h) verkossa olevat järjestelmät todennetaan
- i) järjestelmien yhteyksiä verkkoon rajoitetaan ja suodatetaan (esim. palomuureilla)
- j) laitteiden ja välineiden yhdistäminen verkkoon olisi havaitaan, sitä rajoitetaan ja ne todennetaan
- k) verkkolaitteita kovennetaan
- l) verkon hallintakanavat erotetaan muuta verkkoliikenteestä
- m) kriittiset aliverkostot eristetään tilapäisesti (esim. "lasku/nostosillalla"), jos verkkoon on hyökkäyksen kohteena
- n) haavoittuvat verkkokäytänteet poistetaan käytöstä.

Organisaation olisi varmistettava, että asianmukaisia turvallisuuden hallintakeinoja sovelletaan virtuaaliverkkoihin. Virtuaaliverkot kattavat myös ohjelmistoverkot (SDN, SD-WAN). Virtuaaliverkot voivat olla turvallisuuden näkökulmasta hyviä ratkaisuja, sillä ne voivat mahdollistaa fyysisissä verkoissa tapahtuvan viestinnän loogisen erottamisen etenkin järjestelmissä ja sovelluksissa, jotka on toteutettu jaettua laskentaa käyttäen.

### Lisätiedot

Lisätietoja verkkoturvallisuudesta löytyy standardisarjasta ISO/IEC 27033.

Lisätietoja virtuaaliverkoista löytyy teknisestä spesifikaatiosta ISO/IEC TS 23167.

## 8.21 Verkkopalvelujen turvaaminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Kaikkien verkkopalvelujen turvamekanismit, palvelutasot ja palveluvaatimukset olisi yksilöitää ja toteutettava, ja niitä olisi seurattava.

### Tarkoitus

Varmistetaan verkkopalvelujen käytön turvallisuus.

### Ohjeistus

Tiettyjen palvelujen tarvitsemat turvallisuustoimet, kuten turvallisuusominaisuudet, palvelutasot ja palveluvaatimukset, olisi tunnistettava ja toteutettava (sisäisesti tai ulkoisen verkkopalvelujen tuottajan toimesta). Organisaation olisi varmistettava, että verkkopalvelujen tuottajat toteuttavat nämä toimet.

Verkkopalvelujen tuottajan kyky hallita sovittuja palveluja turvallisesti olisi määritettävä ja sitä olisi seurattava säännöllisesti. Auditointioikeudesta olisi sovittava organisaation ja palveluntuottajan välillä. Organisaation olisi harkittava toimittajan tarjoamia kolmannen osapuolen todennuksia, joilla osoitetaan, että toimittaja ylläpitää asianmukaisia turvallisuustoimia.

Verkkojen ja verkkolaitteiden käyttöä koskevat säännöt olisi laadittava ja toteutettava. Niiden olisi katettava

- a) ne verkot ja verkkopalvelut, joihin pääsy sallitaan
- b) eri verkkopalveluita koskevat todentamisvaatimukset
- c) oikeuksien myöntämismenettely, jolla määritetään, kenellä on pääsy mihinkin verkkoon ja verkkopalveluun
- d) verkkoja ja teknologiaa koskevat hallintakeinot ja -menettelyt, joilla suojataan pääsyä verkkoyhteyksiin ja verkkopalveluihin
- e) keinot, joilla verkkoihin ja verkkopalveluihin päästään (esim. VPN-yhteydellä tai langattomasti)
- f) ajankohta, sijainti ja muut attribuutit, jotka koskevat käyttäjän yhteyttä
- g) verkkopalveluiden käytön seuranta.

Seuraavia verkkopalvelujen turvallisuusomaisuuksia olisi harkittava:

- a) verkkopalvelun turvallisuuteen sovellettu teknologia, kuten todennus, salaustekniikka ja verkkoyhteyden hallintakeinot
- b) verkkopalvelujen suojetun yhteyden edellyttämät tekniset parametrit, jotka ovat turvallisuus- ja verkkoyhteyssääntöjen mukaisia
- c) välimuistin tallentaminen (esim. sisällön toimittamisen verkoissa) ja sen parametrit, jotka tarjoavat käyttäjälle mahdollisuuden valita välimuistin tallentamisen käytön suorituskykyä, saatavuutta ja luottamuksellisuutta koskevien vaatimusten mukaisesti
- d) verkkopalvelun käyttömenettelyt, jotka tarvittaessa rajoittavat pääsyä verkkopalveluihin tai sovelluksiin.

## Lisätiedot

Verkkopalvelut sisältävät liitännöiden tarjoamisen, yksityiset verkkopalvelut hallitut verkon turvallisuusratkaisut, kuten palomuurit ja tietomurtohäälyttimet. Näiden palveluiden kirjo ulottuu yksinkertaisesta hallinnoimattomasta kaistanlevydestä monitahoisiin kaupallisiin palveluihin.

Lisätietoja pääsynhallinnan puitteista löytyy standardista ISO/IEC 29146.

## 8.22 Verkkojen eriyttäminen (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät olisi eriyttää toisistaan organisaation verkoissa.

### Tarkoitus

Jaetaan verkko erillisiin turvallisuusalueisiin ja hallitaan niiden välistä liikennettä liiketoiminnallisten tarpeiden mukaisesti.

### Ohjeistus

Organisaation olisi harkittava suurten verkkojen turvallisuuden hallinnan toteuttamista jakamalla verkot erillisiin verkkoalueisiin ja erottamalla ne julkisesta verkosta (eli internetistä). Verkkoalueet

voidaan valita luottamus-, kriittisyys- ja arkaluonteisuustasojen (esim. julkinen verkkoalue, työasemien verkkoalue, palvelimen verkkoalue, alhaisen ja korkean riskin järjestelmät), organisaatioyksiköiden (esim. henkilöstöhallinto, taloushallinto, markkinointi) tai jonkin yhdistelmän (esim. palvelimen verkkoalue, joka on yhdistetty useisiin organisaatioyksiköihin) perusteella. Eriytäminen voidaan toteuttaa joko fyysisesti erillisillä verkoilla tai eri loogisilla verkoilla.

Kunkin verkkoalueen rajat olisi määriteltävä selkeästi. Jos pääsy verkkoalueiden välillä on sallittua, sitä olisi hallittava rajapinnalla yhdyskäytävän avulla (esim. palomuuri, suodattava reititin). Kriteerien, joilla verkot eriytetään eri verkkoalueisiin, sekä yhdyskäytävien kautta sallitun pääsyn olisi perustuttava kunkin verkkoalueen turvallisuusvaatimusten arviointiin. Arvioinnin olisi oltava pääsynhallinta koskevien kohdennettujen toimintaperiaatteiden (ks. [kohta 5.15](#)), pääsynvaatimusten, arvon ja käsiteltävän tiedon luokitusten mukaista, ja siinä olisi otettava huomioon soveltuwan yhdyskäytävateknologian toteuttamisen suhteelliset kustannukset ja vaikutukset suorituskykyyn.

Langattomat verkot vaativat erityishuomiota, koska niiden verkkorajoja on vaikea määritellä. Radiopeittoalueen säätämistä olisi harkittava langattomien verkkojen eriyttämisessä. Arkaluonteisissa ympäristöissä langattomia yhteyksiä olisi käsiteltävä ulkoisina yhteyksinä ja nämä yhteydet olisi eriyttävä sisäverkoista, kunnes yhteys on kulkenut yhdyskäytävän kautta verkon hallintakeinojen (ks. [kohta 8.20](#)) mukaisesti. Vasta tämän jälkeen myönnetään pääsy sisäisiin järjestelmiin. Vierailijoille tarkoitettu langaton verkko olisi eriyttävä henkilöstölle tarkoitetuista, jos henkilöstö käyttää vain valvottuja käyttäjiä päätelaitteita, jotka ovat organisaation kohdennettujen toimintaperiaatteiden mukaisia. Vierailijoille tarkoitettulla langattomalla verkolla olisi oltava vähintään vastaavat rajoitukset kuin henkilöstön langattomilla verkoilla, jotta henkilöstö ei käytä vierailijaverkkoa.

## Lisätiedot

Verkot ulottuvat usein organisaatorojen yli, koska yritysten välisessä yhteistyössä tarvitaan tietojenkäsittely- ja verkkopalvelujen yhteyksiä tai jakamista. Tällainen laajentuminen voi lisätä luvattoman pääsyn riskiä verkkoa käyttäviin organisaation tietokonejärjestelmiin. Jotkin näistä tarvitsevat suojausta verkon muita käyttäjiä vastaan arkaluonteisuutensa tai kriittisyytensä takia.

## 8.23 Verkkosuodatus (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Pääsyä ulkoisiin verkkosivustoihin olisi hallittava, jotta voidaan vähentää altistumista haitallisille sisällöille.

### Tarkoitus

Suojellaan järjestelmiä haittaohjelmilta ja estetään pääsy luvattomiin verkkoresursseihin.

### Ohjeistus

Organisaation olisi lievnettävä riskiä siitä, että sen henkilöstö käy verkkosivustoilla, jotka sisältävät laitonta tietoa tai joiden tiedetään sisältävän viruksia tai kalastelumateriaalia. Tämä voidaan ratkaista estämällä kyseessä olevien verkkosivustojen IP-osoitteet tai verkkoalueet. Jotkin selaimet ja haittaohjelmien torjuntaohjelmistot tekevät tämän automaattisesti, tai ne voidaan konfiguroida tekemään niin.

Organisaation olisi yksilöitää verkkosivustotyyppit, joihin henkilöstöllä olisi oltava pääsy tai joihin pääsyn olisi oltava estetty. Organisaation olisi harkittava pääsyn estämistä seuraavan tyyppeille verkkosivustoille:

- a) verkkosivustot, joihin voi ladata tietoja, ellei tästä ole erikseen sallittu liiketoiminnallisista syistä
- b) tiedetyt tai epäillyt haitalliset verkkosivustot (esim. ne, jotka levittävät haittaohjelmia tai kalastelumateriaalia)
- c) komentopalvelimet
- d) haitalliset verkkosivustot, jotka on havaittu uhkatiedon seurannassa (ks. [kohta 5.7](#))
- e) laitonta sisältöä jakavat verkkosivustot.

Ennen tämän hallintakeinon käyttöönotto organisaation olisi laadittava verkkoresurssien turvallista ja asianmukaista käytöä koskevat säädöt, mukaan lukien ei-haluttujen tai sopimattomien verkkosivustojen ja verkkopohjaisten sovellusten käytön rajoittaminen. Nämä säädöt olisi pidettävä ajantasaisina.

Henkilöstölle olisi tarjottava koulutusta verkkoresurssien turvallisesta ja asianmukaisesta käytöstä, myös verkkoon pääsystä. Koulutuksen olisi sisällettävä organisaation säädöt, yhteydenottopisteet turvallisuushuolien ilmoittamiseen ja poikkeusprosessi tilanteisiin, joissa rajoitettuihin verkkoresursseihin tarvitaan pääsy oikeista liiketoiminnallisista syistä. Henkilöstöä olisi koulutettava myös, jotta voidaan varmistaa, että henkilöstö ei jätä huomioimatta selainten ilmoituksia, jotka kertovat verkkosiviston olevan suojaamaton mutta antavat käyttäjän silti jatkaa sille.

## Lisätiedot

Verkkosuodatus voi sisältää erilaisia tekniikoita mukaan lukien allekirjoitukset, heuristiikat, hyväksyttävien verkkosivustojen tai verkkoalueiden luettelot, kiellettyjen verkkosivustojen tai verkkoalueiden luettelot sekä valmiit konfiguraatiot haittaohjelmien ja muiden organisaation verkkoa ja järjestelmiä uhkaavien haitallisten toimintojen estämiseksi.

## 8.24 Salauksen käyttö (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi	#Suojaaminen

### Hallintakeino

Säädöt salauksen vaikuttavaan käyttöön, sisältäen salausavainten hallinnan, olisi määriteltävä ja toteutettava.

### Tarkoitus

Varmistetaan salauksen asianmukainen ja vaikuttava käyttö, jotta tiedon luottamuksellisuutta, aitous ja eheyttä kyettää suojamaan liiketoiminnallisten vaatimusten ja tietoturvavaatimusten mukaisesti ottaen huomioon salaukseen liittyvät lakiens, asetuksen, viranomaismääräysten ja sopimusten vaatimukset.

## Ohjeistus

### Yleistä

Salausta käytettäessä olisi otettava seuraavat asiat huomioon:

- a) Organisaation laatimat salausta koskevat kohdennetut toimintaperiaatteet, mukaan lukien tietojen suojaamista koskevat yleiset periaatteet, otetaan huomioon. Salauksen käyttöä koskevien kohdennettujen toimintaperiaatteiden määrittely on tarpeen, jotta salaustekniikasta saadaan mahdollisimman suuri hyöty ja mahdollisimman vähäiset riskit ja jotta vältetään asiaton tai virheellinen käyttö.
- b) Tietojen vaatima suojaustaso ja luokitus tunnistetaan ja sen perusteella määritellään tarvittavien salausalgoritmien tyyppi, vahvuus ja laatu.
- c) Salauksen käyttö suojaamaan tietoja, joita säilytetään siirrettävillä käyttäjien päätelaitteilla tai tallennusvälineillä ja joita siirretään verkkojen kautta tällaisiin laitteisiin tai tallennusvälineisiin.
- d) Avaintenhallinnan menettelyt, sisältäen salausvainten luomisen ja suojausmenetelmät ja salatun tiedon palauttamisen, jos salausvaimet katoavat, vaarantuvat tai vaurioituvat.
- e) Roolit ja vastuut
  - 1) salauksen vaikuttavaa käyttöä koskevien sääntöjen toteuttamiseen
  - 2) avaintenhallintaan, mukaan lukien salausvainten luomiseen (ks. [kohta 8.24](#)).
- f) Määritellään käyttöönottavat standardit sekä salausalgoritmit, salakirjoitusmenetelmän vahvuus, salausratkaisut ja käyttöä koskevat käytännöt, jotka on hyväksytty käytettäviksi tai joiden käyttöä vaaditaan organisaatiossa.
- g) Tiedon salauksen vaikutus hallintakeinoihin, jotka edellyttävät sisällön tarkastusta (esim. haittaohjelmien havaitseminen tai sisällön suodatus).

Organisaation vaikuttavaa salaamista koskevien sääntöjen toteutuksessa olisi otettava huomioon säännökset ja kansalliset rajoitukset, jotka voivat kohdistua salaustekniikoihin eri puolilla maailmaa sekä salakirjoitetun tiedon kulkuun rajojen yli (ks. [kohta 5.31](#)).

Ulkopuolisten salauspalvelujen toimittajien (esim. varmentajien) kanssa tehtyjen palvelutasosopimusten olisi katettava vahinkovastuu, palvelun luotettavuutta ja palvelujen sopimusehtoihin liittyviä vasteaikoa koskevat kysymykset (ks. [kohta 5.22](#)).

### Avaintenhallinta

Asianmukainen avaintenhallinta vaatii turvallisia prosesseja, joilla salausvaimet luodaan, säilytetään, arkistoidaan, haetaan, jaetaan, poistetaan ja hävitetään.

Avaintenhallintajärjestelmän olisi perustuttava yhteisesti sovittuihin standardeihin, menettelyihin ja turvallisiin menetelmiin, jotka kattavat

- a) avainten luomisen eri salausjärjestelmien ja eri sovellusten käyttöön
- b) julkisen avaimen varmenteiden myöntämisen ja hankkimisen
- c) avainten jakamisen asiaankuuluville tahoille, sekä ohjeet siitä, miten avaimet otetaan käyttöön niiden vastaanottamisen jälkeen
- d) avainten säilyttämisen sisältäen sen, kuinka luvalliset käyttäjät voivat saada avaimet käyttöönsä
- e) avainten muuttamisen tai päivittämisen sekä säännöt sille, milloin ja miten avaimia olisi muutettava
- f) vaarantuneiden avainten käsitteleminen

- g) avainten sulkemisen sekä sen, kuinka avaimet poistetaan käytöstä tai tehdään toimimattomiksi (esim. kun avain on vaarantunut tai kun käyttäjä lähtee organisaatiosta, jolloin avaimet olisi myös arkistoitava)
- h) hävinneiden tai turmeltuneiden avainten palauttamisen
- i) avainten varmuuskopioinnin tai arkistoinnin
- j) avainten hävittämisen
- k) avaintenhallintaan liittyvien toimintojen kirjaamisen ja jäljittämisen
- l) avainten aktivoitumis- ja vanhentumispäivämäärien asettamisen, jotta avaimia voidaan käyttää ainoastaan organisaation avaintenhallintaa koskevissa säännöissä määritellyn aikaa
- m) salausavainten saamista koskevien juridisten pyyntöjen käsittelyn (esim. voi olla tarpeen purkaa salattu tieto, jotta sitä voidaan käyttää todisteena oikeustapauksissa).

Kaikki salausavaimet olisi suojahtava muuttamiselta ja katoamiselta. Lisäksi salaiset ja yksityiset salausavaimet täytyy suojaata luvatonta käyttöä ja paljastumista vastaan. Laitteet, joilla luodaan, säilytetään ja arkistoitaan salausavaimia, olisi suojahtava fyysisesti.

Eheyden lisäksi monissa käyttötapauksissa myös julkisten avainten aitous olisi otettava huomioon.

### Lisätiedot

Julkisten avainten aitous varmistetaan yleensä julkisten avaintenhallintaprosesseissa varmenneviranomaisten ja julkisen avaimen varmenteiden avulla, mutta on myös mahdollista varmistaa se muilla teknologioilla, kuten manuaalisten prosessien kohdentamisella pieneen määrään avaimia.

Salausella voidaan saavuttaa erilaisia tietoturvatavoitteita, esimerkiksi

- a) luottamuksellisuus: tiedon salaaminen suojaamaan arkaluonteista tai kriittistä tietoa joko säilytettäessä tai siirrettäessä
- b) eheys tai aitous: digitaalisten allekirjoitusten tai viestin todennuskoodien käyttö, jolla suojaataan tallennetun tai siirretyn arkaluonteisen tai kriittisen tiedon aitoutta ja eheyttä; tiedostojen eheys voidaan varmistaa algoritmeilla
- c) kiistämättömyys: salaustekniikan käyttö tuottamaan todisteita siitä, onko jokin tapahtuma tai toiminto esiintynyt vai ei
- d) todentaminen: salaustekniikan käyttö, kun todennetaan käyttäjiä ja muita järjestelmäpalveluita ja -komponentteja, jotka pyytävät järjestelmän muita käyttäjiä, kokonaisuksia tai resursseja koskevaa pääsy- tai käyttöoikeutta.

Lisätietoja avaintenhallinnasta löytyy standardisarjasta ISO/IEC 11770.

## 8.25 Turvallinen kehittämisen elinkaari ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Ohjelmistojen ja järjestelmien turvallista kehittämistä koskevat säännöt olisi laadittava, ja niitä olisi sovellettava.

## Tarkoitus

Varmistetaan, että tietoturvallisuus suunnitellaan ja toteutetaan osana ohjelmistojen ja järjestelmien turvallista kehittämisen elinkaarta.

## Ohjeistus

Turvallinen kehittäminen on vaatimus turvallisen palvelun, arkkitehtuurin, ohjelmiston ja järjestelmän rakentamiselle. Sen saavuttamisessa olisi otettava huomioon seuraavat asiat:

- a) kehitys-, testaus- ja tuotanto-ympäristöjen erottaminen (ks. [kohta 8.31](#))
- b) ohjelmisto-kehityksen elinkaaren turvallisuutta koskeva ohjeistus:
  - 1) ohjelmisto-kehitysmenetelyjen turvallisuus (ks. [kohdat 8.28 ja 8.27](#))
  - 2) kunkin käytetyn ohjelmostikielen turvallisen ohjelmoinnin ohjeet (ks. [kohta 8.28](#))
- c) turvallisuusvaatimukset määrittely- ja suunnitteluvaiheessa (ks. [kohta 5.8](#))
- d) turvallisuuden tarkistuspisteet projekteissa (ks. [kohta 5.8](#))
- e) järjestelmä- ja turvallisuustestaus, kuten regressiotestaus, koodiskannaus ja tunkeutumistestaus (ks. [kohta 8.29](#))
- f) turvalliset ohjelmistovarastot lähdekoodeille ja konfiguraatioille (ks. [kohdat 8.4 ja 8.9](#))
- g) versionhallinnan turvallisuus (ks. [kohta 8.32](#))
- h) vaadittava sovellusturvallisuuden osaaminen ja koulutus (ks. [kohta 8.28](#))
- i) kehittäjän kyky estää haavoittuvuuksien syntymisen, löytää niitä ja korjata ne (ks. [kohta 8.28](#))
- j) lisensointitarpeet ja -vaihtoehdot, jotta voidaan varmistaa ratkaisujen kustannustehokkuus ja välttää tulevat lisensointiongelmat (ks. [kohta 5.32](#)).

Jos kehitys on ulkoistettu, organisaation olisi varmistuttava siitä, että toimittaja noudattaa organisaation turvallisen kehittämisen sääntöjä (ks. [kohta 8.30](#)).

## Lisätiedot

Kehitys voi myös tapahtua sovellusten sisällä, kuten toimistosovelluksissa, skriptauksella, selaimissa ja tietokannoissa.

## 8.26 Sovelluksia koskevat turvallisuusvaatimukset ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen #Puolustus

## Hallintakeino

Tietoturvavaatimukset olisi tunnistettava, määriteltävä ja hyväksyttävä, kun suunnitellaan tai hankitaan sovelluksia.

## Tarkoitus

Varmistetaan, että kaikki tietoturvavaatimukset on tunnistettu ja otettu huomioon, kun kehitetään tai hankitaan sovelluksia.

## Ohjeistus

### Yleistä

Sovelluksia koskevat turvallisuusvaatimukset olisi tunnistettava ja määriteltävä. Yleensä nämä vaatimukset määritetään riskien arvioinnilla. Vaatimukset olisi laadittava tietoturvallisuuden asiantuntijoiden tukemana.

Sovelluksia koskevat turvallisuusvaatimukset voivat kattaa laajan joukon aiheita sovelluksen tarkoituksesta riippuen.

Sovelluksia koskevien turvallisuusvaatimusten olisi soveltuvin osin sisällettävä

- a) tahojen identiteettien luottamustason (esim. todentamisella, ks. [kohdat 5.17, 8.2 ja 8.5](#))
- b) sovelluksen käsittelemien tietojen tyyppien ja luokitustasojen tunnistamisen
- c) tarve eriyttää tietoihin ja toimintoihin pääsy ja pääsytaiso sovelluksessa
- d) haitallisten hyökkäysten ja tahattomien häiriöiden sietokyky (esim. suojaus puskurin ylivuotoja tai SQL-injektiota vastaan)
- e) lakien, asetusten ja viranomaisten vaatimukset lainsäädäntöalueella, josta transaktio on syntynyt, jossa sitä on käsitelty, jossa se on toteutettu tai jossa sitä säilytetään
- f) tarve kaikkiin osapuoliin liittyvään tietosuojaan
- g) mahdollisen luottamuksellisen tiedon suojausvaatimukset
- h) tietojen suojaaminen käsittelyn, siirron ja säilytyksen aikana
- i) tarve turvallisesti salata kaikkien osapuolten välinen viestintä
- j) syötteitä koskevat hallintakeinot, kuten eheyden tarkistus ja syötteiden oikeellisuustarkistus
- k) automatisoidut hallintakeinot (esim. hyväksyntärajat tai kaksoishyväksyntä)
- l) tulosteita koskevat hallintakeinot, joissa otetaan huomioon myös se, kenellä on pääsy tulosteisiin sekä pääsyn myöntäminen
- m) rajoitukset vapaiden tekstikenttien sisällölle, koska ne voivat johtaa luottamuksellisen tiedon (esim. henkilötietojen) hallinnoimattomaan säilyttämiseen
- n) liiketoimintaprosessista johdetut vaatimukset, kuten transaktiolokit ja valvonta, kiistämättömyysvaatimukset
- o) muiden turvallisuuden hallintakeinojen edellyttämät vaatimukset (esim. rajapinnat tapahtumalokia ja valvontaa tai tietovuotojen havaitsemisjärjestelmää varten)
- p) virheilmoitusten käsittely.

### Transaktiopalvelut

Näiden lisäksi organisaation ja yhteistyökumppanin välisiä transaktiopalveluja tarjoavien sovellusten tietoturvavaatimusten tunnistamisessa olisi otettava huomioon seuraavat asiat:

- a) kunkin osapuolen edellyttämä luottamustaso vastapuolen identiteettivätteisiin
- b) vaihdetun tai käsitellyn tiedon eheydeltä edellytetty luottamustaso sekä mekanismit eheyden menetyksen tunnistamiseen (esim. CRC-tarkistus, tiivistimet, digitaaliset allekirjoitukset)
- c) valtuutusprosessit, jotka määrittävät, kuka voi hyväksyä transaktioihin liittyvien avainasiakirjojen sisällön, jakaa tai allekirjoittaa ne

- d) avainasiakirjojen luottamuksellisuus ja eheys, lähetyksen ja vastaanoton todentaminen sekä kiistämättömyys (esim. tarjous- ja sopimusprosesseihin liittyvät sopimukset)
- e) kaikkien transaktioiden (esim. tilausten, toimitusositteiden ja vastaanoton vahvistuksen) luottamuksellisuus ja eheys
- f) vaatimukset siitä, kuinka kauan transaktioita pidetään luottamuksellisina
- g) vakuutukset ja muut sopimukselliset vaatimukset.

#### Sähköisen tilaamisen ja maksamisen sovellukset

Lisäksi sähköisen tilaamisen ja maksamisen sovelluksissa olisi otettava huomioon seuraavat asiat:

- a) tilaustietojen luottamuksellisuuden ja eheyden ylläpitämistä koskevat vaatimukset
- b) minkä tasoista todentamista asiakkaan esittämät maksutiedot tarvitsevat
- c) tapahtuman tietojen häviämisen tai kahdentumisen ehkäiseminen
- d) transaktioita koskevien tietojen säilyttäminen julkisesti saatavilla olevan ympäristön ulkopuolella (esim. käytäen organisaation sisäverkossa sijaitsevaa tallennusalustaa, eikä säilytetä tallennusvälineellä, johon on suora pääsy internetistä)
- e) kun käytetään luotettavaa tahoa (esim. digitaalisten allekirjoitusten tai varmenteiden myöntämiseen ja ylläpitoon) turvallisuudesta muodostetaan kokonaisuus, joka kattaa koko varmenteiden ja allekirjoitusten hallintaprosessin päästä pähän.

Monet edellä esitettyt näkökohdat voidaan ratkaista soveltamalla salausta (ks. [kohta 8.24](#)) ottaen samalla huomioon lakisääteiset vaatimukset (ks. [kohdat 5.31–5.36](#), etenkin salausta koskeva lainsääädäntöä käsittelevä [kohta 5.31](#)).

#### Lisätiedot

Julkisten verkkojen kautta saatavilla olevat sovellukset ovat alttiita erilaisille verkkopohjaisille uhkille, kuten petoksiin, sopimuksen vastaiselle toiminnalle tai tiedon julkiselle paljastumiselle, epätäydelliselle lähetykselle, väärään paikkaan ohjautumiselle, viestien luvattomalle muuttamiselle sekä viestin luvattomalle kopioinnille tai toistolle. Tästä syystä riskien arviointi ja hallintakeinojen tarkka määritäminen ovat korvaamattomia. Vaadittavat hallintakeinot sisältävät yleensä salausmenetelmien käytön todentamista ja turvallista tiedonsiirtoa varten.

Lisätietoja sovellusten suojaamisesta löytyy standardisarjasta ISO/IEC 27034.

## 8.27 Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsittimet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

#### Hallintakeino

Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet olisi laadittava ja dokumentoitava. Niitä olisi ylläpidettävä, ja niitä olisi sovellettava kaikkiin tietojärjestelmien kehitystoimiin.

#### Tarkoitus

Varmistetaan, että tietojärjestelmät on suunniteltu ja toteutettu ja että niitä käytetään turvallisesti kehittämisen koko elinkaaren ajan.

## Ohjeistus

Turvallisuuden suunnitteluperiaatteet olisi laadittava ja dokumentoitava, ja niitä olisi sovellettava tietojärjestelmien suunnittelutoimiin. Turvallisuus olisi suunniteltava siten, että se kattaa kaikki arkkitehtuurin kerrokset (liiketoiminta, tieto, sovellukset ja teknologia). Uusi teknologia olisi analysoitava turvallisuusriskien varalta, ja suunnitelma olisi katselmoitava tunnettujen hyökkäysmenettelyjen suhtein.

Turvalliset suunnitteluperiaatteet tuottavat ohjeita käyttäjien todentamistekniikoille, turvalliseen istunnonhallintaan ja tietojen oikeellisuuden tarkistamiseen ja hävittämiseen.

Turvallisen järjestelmäsuunnittelun periaatteiden olisi sisällettävä seuraavien asioiden analysointi:

- a) kaikki tietojen ja järjestelmien tunnistetuista uhkista suojaamiseen tarvittavat turvallisuuden hallintakeinot
- b) turvallisuuden hallintakeinojen kyvykkyydet estää, havaita ja reagoida turvallisuustapahtumiin
- c) kunkin liiketoimintaprosessin edellyttämät yksilöidyt turvallisuuden hallintakeinot (esim. arkaluonteisten tietojen salaus, eheyden varmistaminen ja tietojen sähköinen allekirjoittaminen)
- d) missä ja miten turvallisuuden hallintakeinoja sovelletaan (esim. integroimalla ne turvallisuusarkkitehtuurin ja tekniseen infrastruktuuriin)
- e) miten yksittäiset (manuaaliset ja automatisoidut) turvallisuuden hallintakeinot toimivat yhdessä tuottaen integroidun hallintakeinojen yhdistelmän.

Turvallisuuden suunnitteluperiaatteissa olisi otettava huomioon

- a) integraatiotarve turvallisuusarkkitehtuurin kanssa
- b) tekninen turvallisuusinfrastrukturi (esim. julkisen avaimen järjestelmä (PKI), identiteetti- ja käyttöövaltuushallinta (IAM), tietovuotojen estäminen ja dynaaminen pääsynhallinta)
- c) organisaation kyky kehittää ja tukea valittuja teknolojioita
- d) turvallisuusvaatimusten saavuttamisen kustannukset, aikataulut ja monimutkaisuus
- e) senhetkiset hyvät käytännöt.

Turvallisen järjestelmäsuunnittelun olisi sisällettävä

- a) turvallisuusarkkitehtuurin liittyvien periaatteiden käytön, kuten "sisäänrakennettu turvallisuus", "syvyyssuuntainen turvallisuus", "oletusarvoisen turvallisuus", "oletusarvoisen estäminen", "turvallinen vikaantuminen", "ulkoisten sovellusten syötteiden epäileminen", "käyttöönoton aikainen turvallisuus", "murron olettaminen", "vähin oikeus", "käytettävyys ja hallittavuus" ja "vähin toiminnallisuus"
- b) turvallisuuteen painottuva suunnittelun katselointi, jolla tunnistetaan tietoturvahaavoittuvuuksia ja varmistetaan, että turvallisuuden hallintakeinot on määritelty ja että ne täytyvät turvallisuusvaatimukset
- c) niiden turvallisuuden hallintakeinojen dokumentointi ja muodollinen hyväksyminen, jotka eivät täysin täytä vaatimuksia (esim. turvallisuusvaatimusten ohittamisen vuoksi)
- d) järjestelmien koventaminen.

Organisaation olisi harkittava "nollaluottamus (*zero trust*)" -periaatteita, kuten

- a) sen olettaminen, että organisaation tietojärjestelmät on jo murrettu, eikä luoteta pelkkään verkkoturvallisuuteen
- b) "älä koskaan luota, vaan todenna aina" -toimintamallin soveltamista tietojärjestelmiin pääsyn
- c) sen varmistaminen, että tietojärjestelmään tehtävät pyynnöt on salattu päästä pähän

- d) kaikkien tietojärjestelmää koskevien pyyntöjen todentaminen niin kuin pyyntö olisi peräisin avoimesta, ulkoisesta verkosta, vaikka pyyntö olisi peräisin organisaation sisältä (eli ei automaatisesti luoteta kaikkeen organisaation turva-alueen sisä- eikä ulkopuoliseen)
- e) "vähimmän oikeuden" ja dynaamisen pääsynhallinnan tekniikoiden käyttöä (ks. [kohdat 5.15, 5.18](#) ja [8.2](#)); tämä sisältää tietoja tai järjestelmiä koskevien pyyntöjen todentamisen ja valtuuttamisen perustuen asiayhteyspohjaiseen tietoon, kuten tunnistautumistietoihin (ks. [kohta 5.17](#)), käyttäjäidentiteeteihin (ks. [kohta 5.16](#)), käyttäjien päätelaitteita koskeviin tietoihin ja tietojen luokittelun (ks. [kohta 5.12](#))
- f) sen, että pyyntöjen esittäjät todennetaan ja tietojärjestelmiin pääsyn pyyntöjen oikeellisuus tarkistetaan aina perustuen tunnistautumistietoihin (ks. [kohta 5.17](#)), ja käyttäjäidentiteeteihin (ks. [kohta 5.16](#)), käyttäjien päätelaitteita koskeviin tietoihin ja tietojen luokittelun (ks. [kohta 5.12](#)), esimerkiksi vaatimalla vahvan todennuksen käyttöä (esim. monivaiheinen, ks. [kohta 8.5](#)).

Yleisiä turvallisuuden suunnitteluperiaatteita olisi sovellettava mahdollisuksien mukaan myös tietojärjestelmien ulkoistettuun kehittämiseen sopimusten ja muiden sitovien järjestelyjen kautta organisaation ja organisaation valitseman ulkoistusta hoitavan toimittajan välillä. Organisaation olisi varmistettava, että toimittajien turvallisuuden suunnittelukäytännöt ovat linjassa organisaation tarpeiden kanssa.

Nämä turvallisuuden suunnitteluperiaatteet ja yleiset suunnittelumenetelmät olisi katselmoitava säännöllisesti, jotta voidaan varmistaa, että ne edistävät tehokkaasti suunnitteluprosessin turvallisuustasoa. Ne olisi myös säännöllisesti katselmoitava, jotta voidaan varmistaa, että ne ovat ajantasaisia mahdollisten uusien uhkien torjunnassa ja niitä voidaan soveltaa teknologian kehittyessä ja kun uusia ratkaisuja otetaan käyttöön.

## Lisätiedot

Turvallisia suunnitteluperiaatteita voidaan soveltaa erilaisten tekniikoiden suunnittelun ja konfigurointiin. Tällaisia ovat esim.

- vikasietoisuus ja muut sietokykyä parantavat tekniikat
- eriyttäminen (esim. virtualisoinnilla tai osittamisella)
- luvattoman muuttamisen kestävyys.

Turvallisen virtualisoinnin tekniikoita voidaan käyttää estämään samassa fyysisessä laitteessa ajettavien sovellusten keskinäiset häiriöt. Jos hyökkääjä pääsee käsiksi sovelluksen virtuaalikopioon, vain kyseinen kopio altistuu vaikutuksille. Hyökkäyksellä ei ole vaikutusta muihin sovelluksiin tai tietoihin

Luvattomalta muuttamiselta suojaavia tekniikoita voidaan käyttää tietojen peukaloinnin havaitsemiseen, oli kyseessä sitten fyysinen (esim. murtohälytin) tai looginen (esim. tiedosto) tekniikka. Näille tekniikoille on ominaista, että luvattomasta muutosrytyksestä jää tallenne. Lisäksi hallintakeino voi estää tietojen onnistuneen kaappaamisen tuhoamalla tiedot (esim. laitteen muisti voidaan tyhjentää).

## 8.28 Turvallinen ohjelointi ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

## Hallintakeino

Ohjelmistokehityksessä olisi sovellettava turvallisen ohjelmoinnin periaatteita.

## Tarkoitus

Varmistetaan, että ohjelmisto on kirjoitettu turvallisesti ja näin on pienennetty ohjelmistossa olevien mahdollisten tietoturvaavaavottuvuuksien lukumäärää.

## Ohjeistus

### Yleistä

Organisaation olisi laadittava koko organisaation kattavat prosessit, joilla varmistetaan ohjelmointia koskeva hyvä hallintotapa. Olisi laadittava vähimmäisturvallisuuden vähimmäistaso, jota olisi sovellettava. Lisäksi tällaisia prosesseja ja hallintotapoja olisi laajennettava koskemaan kolmansilta osapuolilta olevat ohjelmistokomponentit sekä avoimen lähteenvohjelmistot.

Organisaation olisi seurattava todellisen maailman uhkia ja ajantasaisia ohjeita sekä ohjelmistojen haavoittuvuuksia koskevia tietoja, koska niistä on apua organisaation turvallisen ohjelmoinnin periaatteiden laativisessa jatkuvan parantamisen ja oppimisen kautta. Tästä voi olla apua sen varmistamisessa, että turvallisen ohjelmoinnin vaikuttavat käytännöt toteutetaan vasteena nopeasti muuttuvaan uhkaympäristöön.

### Suunnittelu ja toiminta ennen ohjelmoinnin aloittamista

Turvallisen ohjelmoinnin periaatteita olisi noudatettava sekä uusissa kehitysprojekteissa että uudelleenkäyttötilanteissa. Näitä periaatteita olisi sovellettava kehitystoimintoihin sekä organisaation sisällä että organisaation muille tahoille toimittamiin tuotteisiin ja palveluihin. Ohjelmosta edeltävän suunnittelun ja toiminnan olisi sisällettävä

- a) turvallista ohjelmosta koskevat organisaatiokohtaiset odotukset ja hyväksytyt periaatteet, joita sovelletaan sekä sisäiseen että ulkoiseen ohjelmostiin
- b) yleiset ja historialliset ohjelmostikäytännöt ja -virheet, jotka johtavat tietoturvaavaavottuvuuksien syntyn
- c) kehitystyökalujen, kuten integroitujen kehitysympäristöjen, konfigurointi turvallisen koodin luomiseen
- d) kehitystyökalujen ja suoritusympäristöjen toimittajien antamien ohjeiden noudattaminen tapauskohtaisesti
- e) päivitettyjen kehitystyökalujen (esim. käänäjien) ylläpito ja käyttö
- f) kehittäjien pätevyydet turvallisen koodin kirjoittamiseen
- g) turvallinen suunnittelu ja arkkitehtuuri, mukaan lukien uhkamallinnus
- h) turvalliset ohjelmostandardit ja velvoittaminen niiden käyttöön, missä se on olennaista
- i) hallittujen kehitysympäristöjen käyttö

### Ohjelmoinnin aikana

Ohjelmoinnin aikana tarkasteltavien näkökohtien olisi sisällettävä

- a) käytettäviä ohjelmostikieliä ja -tekniikoita koskevat turvallisen ohjelmoinnin periaatteet
- b) turvallisen ohjelmoinnin tekniikkoiden, kuten pariohjelmoinnin, refaktoriointin, vertaisarvioinnin, turvallisuusiterointien ja testipohjaisen kehittämisen, käyttö
- c) jäseneltyjen ohjelmostekniikkoiden käyttö

- d) koodin dokumentointi ja sellaisten ohjelmointivirheiden poisto, mitkä voisivat mahdollistaa tietoturvahaavoittuvuuksien hyödyntämisen
- e) turvattomien suunnitteluteknikkoiden käytön kieltäminen (esim. kovakoodattujen salasanojen käyttö, luvattomat koodinäytteet ja todentamattomat sovelluspalvelut).

Testausta olisi tehtävä kehittämisen aikana ja sen jälkeen (ks. [kohta 8.29](#)). Lähdekoodin analysoinnilla analyysityökaluilla voidaan tunnistaa ohjelmiston turvallisuushaavoittuvuuksia.

Ennen ohjelmiston tuotantoymääräistöön siirtämistä, olisi arvioitava

- a) hyökkäyspinta ja vähimmän oikeuden periaate
- b) yleisimpien ohjelmointivirheiden analysointi ja niiden lieventämistoimien dokumentointi.

#### Katselointi ja ylläpito

Kun koodi on siirretty tuotantoymääräistöön

- a) päivitykset olisi paketoitava ja otettava käyttöön turvallisesti
- b) raportoidut tietoturvahaavoittuvuudet olisi käsiteltävä (ks. [kohta 8.8](#))
- c) virheet ja epäillyt hyökkäykset olisi kirjattava ja lokeja katselmoitava säännöllisesti, jotta koodiin voidaan tehdä tarvittavia muutoksia
- d) lähdekoodia olisi suojeleva luvattomalta käytöltä ja muuttamiselta (esim. konfiguraationhallinnan työkalulla, joissa on usein hyödyllisiä toimintoja, kuten pääsynhallinta ja versionhallinta).

Jos käytetään ulkoisia työkaluja ja kirjastoja, organisaation olisi otettava huomioon seuraavat asiat:

- a) varmistetaan, että ulkoisia kirjastoja hallitaan (esim. ylläpitämällä luetteloita kirjastoista ja niiden versioista) ja päivitetään säännöllisesti julkaisujaksojen mukaisesti
- b) valitaan, hyväksytään ja uudelleen käytetään hyvin tarkistettuja komponentteja, erityisesti todentamisen ja salauksen komponentteja
- c) ulkoisten komponenttien lisenssit, turvallisuus ja käyttöhistoria
- d) varmistetaan, että ohjelmisto on ylläpidettävässä, seurattavissa ja että se on peräisin todennetusta ja hyvämaineisesta lähteestä
- e) että kehitysresurssit ja -tuotteet ovat riittävän pitkään saatavilla.

Mikäli ohjelmistopakettiin tarvitaan muutoksia, olisi seuraavat asiat otettava huomioon:

- a) sisäisten hallintakeinojen ja eheysmenetelmien vaarantumisen riski
- b) suostumuksen mahdollinen pyytäminen toimittajalta
- c) mahdollisuus saada tarvittavat muutokset myyjältä tavanomaisina ohjelmistopäivityksinä
- d) organisaation mahdollisuus joutua vastaamaan ohjelmiston ylläpidosta tulevaisuudessa muutosten seurauksena.
- e) Yhteensopivuus muiden käytössä olevien ohjelmistojen kanssa.

#### Lisätiedot

Ohjaavana periaatteena on sen varmistaminen, että turvallisuuden kannalta oleellista koodia kutsutaan tarvittaessa ja että se on luvattomalta muuttamiselta suojattua. Ohjelmilla, jotka on asennettu käännetystä binäärikoodista, on myös nämä ominaisuudet, mutta ne koskevat vain sovelluksessa säilyttäviä tietoja. Tulkituilla kielillä tämä konsepti toimii vain, kun koodi suoritetaan palvelimella, joka on muuten sitä käyttävien käyttäjien ja prosessien ulottumattomissa ja kun tietoja säilytetään vastaavasti suojatuissa tietokannassa. Esimerkiksi tulkittu koodi voidaan ajaa pilvipalvelusta, jossa pääsy itse koodiin vaatii

ylläpito-oikeudet. Tällaista ylläpito-oikeuksin pääsyä olisi suojattava turvallisuusmekanismeilla, kuten oikea-aikaisen hallinnan periaatteilla ja vahvalla todennuksella. Jos sovelluksen omistajalla on pääsy skripteihin suoralla etäyhteydellä palvelimeen, on periaatteessa pääsy myös hyökkääjällä. Näissä tapauksissa verkkopalvelimista olisi estettävä hakemistoselaus.

Sovelluksen koodi kannattaa suunnitella sillä oletuksella, että siihen kohdistuu aina hyökkäyksiä, joko virheistä tai haitallisista toimista johtuvia. Lisäksi kriittiset sovellukset voidaan suunnitella sisäisiä virheitä sietäviksi. Esimerkiksi monimutkaisen algoritmin tuotos voidaan tarkistaa, jotta voidaan varmistaa, että se on turvarajojen sisällä ennen kuin tietoja käytetään tietynlaisessa sovelluksessa, kuten turvallisuuteen tai talouteen liittyvässä kriittisessä sovelluksessa. Turvarajojen tarkistamisen suorittava koodi on yksinkertainen ja siksi sen virheettömyys on paljon helpompi osoittaa.

Jotkin verkkosovelluksen ovat alttiita erilaisille haavoittuvuuksille, kuten tietokantainjektioille ja selainskriptihyökkäyksille, jotka ovat seurausta huonosta suunnittelusta ja ohjelmoinnista. Näissä hyökkäyksissä pyyntöjä voidaan manipuloida siten, että verkkopalvelimen toimintoja kyetään väärinkäyttämään.

Lisätietoja tieto- ja viestintäteknisen turvallisuuden arvioinnista löytyy standardisarjasta ISO/IEC 15408.

## 8.29 Tietoturvatestaus kehitys- ja hyväksyntävaiheissa (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Sovelluksen_turvallisuus #Tietoturvallisuuden_varmentaminen #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Kehittämisen elinkaareen liittyvät turvallisuuden testiprosessit olisi määriteltävä ja toteutettava.

### Tarkoitus

Todennetaan, onko tietoturvavaatimukset toteutettu, kun sovelluksia tai koodia otetaan käyttöön tuotantoypäristössä.

### Ohjeistus

Uudet tietojärjestelmät, päivitykset ja uudet versiot olisi testattava ja varmennettava huolellisesti kehitysprosessin aikana. Turvallisuustestauksen olisi oltava kiinteä osa järjestelmien tai komponenttien testausta.

Turvallisuustestauksessa olisi käytettävä joukkoa vaatimuksia, jotka voidaan kuvata joko toiminnallisina tai ei-toiminnallisina vaatimuksina. Turvallisuustestauksen olisi sisällettävä seuraavien asioiden testaus:

- turvallisuustoiminnot (esim. käyttäjän todentaminen, ks. [kohta 8.5](#), pääsyrajoitukset, ks. [kohta 8.3](#), ja salauksen käyttö, ks. [kohta 8.24](#))
- turvallinen ohjelointi (ks. [kohta 8.28](#))
- turvalliset konfiguraatiot (ks. [kohdat 8.9, 8.20 ja 8.22](#)), sisältäen käyttöjärjestelmät, palomuurit ja muut turvallisuuskomponentit.

Testisuunnitelmien olisi perustuttava joukkoon kriteereitä. Testauksen laajuuden olisi oltava suhteessa järjestelmän tärkeyteen ja luonteeseen sekä toteutettavan muutoksen mahdolliseen vaikutukseen. Testisuunnitelman olisi sisällettävä

- a) toimintojen ja testien yksityiskohtainen aikataulu
- b) syötteet ja odotetut tuotokset erilaisissa olosuhteissa
- c) tulosten arviontikriteerit
- d) jatkotoimenpiteitä koskevat päätökset tarvittaessa.

Organisaatiot voivat hyödyntää automaattisia työkaluja, kuten koodin analysointityökaluja tai haavoittuvuusskannereita, ja organisaation olisi todennettava turvallisuuteen liittyvien puutteiden korjaaminen.

Organisaation sisäisessä kehityksessä kehitysryhmän olisi tehtävä tällaiset testit ensin. Tämän jälkeen olisi tehtävä riippumaton hyväksymistestaus, jotta voidaan varmistaa, että järjestelmä toimii odotetulla tavalla ja vain odotetulla tavalla (ks. [5.8](#)). Seuraavat seikat olisi otettava huomioon:

- a) Koodin katselointeja olennaisena osana testausta koodivirheiden, kuten odottamattomien syötteiden ja olosuhteiden, varalta.
- b) Haavoittuvuusskannauksia olisi tehtävä, jotta voidaan tunnistaa turvattomat konfiguraatiot ja järjestelmän haavoittuvuudet.
- c) Tunkeutumistestausta olisi tehtävä, jotta voidaan tunnistaa turvattomat koodit ja rakenteet.

Ulkoistetun kehityksen ja komponenttien ostamisen yhteydessä olisi noudatettava hankintaprosessia. Toimittajien kanssa tehtäviin sopimuksiin olisi liitetty tunnistetut turvallisuusvaatimukset (ks. [kohta 5.20](#)). Tuotteita ja palveluita olisi arvioitava näitä kriteereitä vasten ennen hankkimista.

Testaus olisi tehtävä tuotantoympäristöä mahdollisimman tarkasti vastaavassa testausympäristössä, jotta voidaan varmistaa, että järjestelmä ei tuo organisaation ympäristöön haavoittuvuuksia ja että testaus on luotettavaa (ks. [kohta 8.31](#)).

## Lisätiedot

Testiympäristöjä voidaan toteuttaa useampia, joita voidaan hyödyntää erilaisissa testauksissa (esim. toiminnallisessa ja suorituskyvyn testauksissa). Nämä eri ympäristöt voivat olla virtuaalisia ja niiden konfiguraatioilla voidaan mallintaa erilaisia tuotantoympäristöjä.

Testiympäristöjen, -työkalujen ja -teknologoiden testausta ja valvontaa on myös tarkasteltava, jotta voidaan varmistaa testauksen vaikuttavuus. Samat näkökohdat koskevat myös kehitys-, testaus- ja tuotantoympäristöissä käytettävien valvontajärjestelmien valvontaa. Järjestelmän ja tietojen arkuontereisuuteen perustuvaa harkintaan tarvitaan sen määrittämiseen, kuinka monta metatestauskerrosta on hyödyllistä.

## 8.30 Ulkoistettu kehittäminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvali-suuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus #Havainto	#Järjestelmän_ja_verkon_turvallisuus #Sovelluksen_turvallisuus #Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen

## Hallintakeino

Organisaation olisi ohjattava, valvottava ja katselmoitava toimintoja, jotka liittyvät ulkoistettuun järjestelmäkehitykseen.

## Tarkoitus

Varmistetaan, että organisaation vaatimusten mukaisia tietoturvatoimia noudatetaan ulkoistetussa järjestelmäkehityksessä.

## Ohjeistus

Kun järjestelmäkehitys on ulkoistettu, organisaation olisi viestittävä ja sovittava vaatimuksista ja odotuksista sekä jatkuvasti valvottava ja katselmoitava sitä, täytäänkö toimitettu ulkoistettu työ nämä odotukset. Seuraavat seikat olisi otettava huomioon organisaation koko ulkoisessa toimitusketjussa:

- a) ulkoistettuun sisältöön liittyvät lisenssisopimukset, koodin omistajuudet ja immateriaalioikeudet (ks. [kohta 5.32](#))
- b) turvallisia suunnittelu-, ohjelmointi- ja testauskäytäntöjä koskevat sopimukselliset vaatimukset (ks. [kohdat 8.25–8.29](#))
- c) uhkamallin toimittaminen ulkoisille kehittäjille
- d) tuotosten laadun ja oikeellisuuden hyväksymistestaus (ks. [kohta 8.29](#))
- e) todisteiden toimittaminen siitä, että turvallisuus- ja tietosuojakyvykkyyksien hyväksyttävät vähimmäistasot on toteutettu (esim. varmennusraportit)
- f) todistusaineisto siitä, että riittävällä testauksella on suojauduttu (sekä tahalliselta että tahattomalta) haitalliselta sisällöltä toimitushetkellä
- g) todistusaineisto siitä, että riittävällä testauksella on suojauduttu tunnetuilta haavoittuvuksilta
- h) turvatalletussopimukset ohjelmiston lähdekoodille (esim. jos toimittaja ajautuu konkurssiin)
- i) sopimukselliset oikeudet auditoida kehitysprosessia ja hallintakeinoja
- j) kehitysympäristön turvallisuusvaatimukset (ks. [kohta 8.31](#))
- k) soveltuvan lainsääädännön huomioon ottaminen (esim. henkilötietojen suojaus).

## Lisätiedot

Lisätietoja toimittajasuheteista löytyy standardisarjasta ISO/IEC 27036.

## 8.31 Kehitys-, testaus- ja tuotantoymäristöjen erotaminen ([EN](#))

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

## Hallintakeino

Kehitys-, testaus- ja tuotantoymäristöt olisi erotettava, ja niitä olisi suojattava.

## Tarkoitus

Suojataan tuotantoymäristöä ja tietoja kehittämisen ja testauksen aiheuttamalta vaarantumiselta.

## Ohjeistus

Tuotannossa ilmenevien ongelmien ehkäisemiseen tarvittava tuotanto-, testaus- ja kehitysympäristöjen erottamisen taso olisi yksilöitvä ja toteutettava.

Seuraavat seikat olisi otettava huomioon:

- a) Kehitys- ja tuotantojärjestelmät erotetaan riittäväällä tavalla ja niitä käytetään eri toimialueilla (esim. erillisillä virtuaalisissa tai fyysisissä ympäristöissä).
- b) Ohjelmiston siirtämistä kehitystilasta tuotantotilaan koskevat säännot ja valtuudet määritellään, dokumentoidaan ja toteutetaan.
- c) Muutoksia tuotantojärjestelmiin ja -sovelluksiin testataan testaus- tai koeypäristössä ennen tuotantojärjestelmiin siirtämistä (ks. [kohta 8.29](#)).
- d) Testausta ei tehdä tuotantoypäristössä muulloin kuin määritellyissä ja hyväksytyissä olosuhteissa.
- e) Kääntäjät, muokkausohjelmat ja muut kehitystyökalut tai apuohjelmat eivät ole käytettävissä tuotantojärjestelmissä, mikäli niitä ei tarvita.
- f) Valikoissa esitetään asianmukaiset ympäristön osoittavat merkinnät, jotta voidaan vähentää virheiden riskiä.
- g) Arkaluonteista tietoa ei kopioida kehitys- ja testausympäristöihin, ellei kehitys- ja testausympäristöjä hallita samatasoin hallintakeinoin.

Kaikissa tapauksissa kehitys- ja testausympäristöjen suojaamisen olisi sisällettävä seuraavat asiat:

- a) kaikkien kehitys-, integrointi- ja testaustyökalujen korjaaminen ja päivittäminen (mukaan lukien rakentajat, integroijat, kääntäjät, konfigurointijärjestelmät ja -kirjastot)
- b) järjestelmien ja ohjelmistojen turvallinen konfiguointi
- c) ympäristöjä koskeva pääsynhallinta
- d) ympäristön ja siihen varastoidun koodin muutosten seuranta
- e) ympäristöjen turvallinen seuranta
- f) ympäristöjen varmuuskopointi.

Yksittäisellä ihmisellä ei pitäisi olla mahdollisuutta tehdä muutoksia sekä kehittämiseen että tuotantoon ilman edeltävää katselmointia ja hyväksyttämistä. Tämä voidaan varmistaa esim. pääsyoikeuksien eriyttämällä tai säännöillä, jota valvotaan. Poikkeustilanteissa olisi toteutettava lisätoimintoja, kuten yksityiskohtainen lokikirjanpito ja reaalialainen valvonta, jotta luvattomat muutokset voidaan havaita ja käynnistää niitä koskevat toiminnot.

## Lisätiedot

Jos kehittäjillä ja testaajilla on pääsy tuotantoypäristöön eikä käytössä ole riittäviä turvallisuustoimia ja -menettelyjä, voi syntyä merkittäviä riskejä (esim. tiedostojen tai järjestelmäympäristöjen tahaton muokkautuminen, järjestelmän vikaantuminen, luvattomien ja testaamattonien koodien ajaminen tuotantojärjestelmissä, luottamuksellisen tiedon paljastuminen, tietojen eheyden vaarantuminen ja saatavuuteen liittyvät ongelmat). On tarpeen ylläpitää tunnettua ja vakaata ympäristöä tarkoitukseenmukaista testausta varten ja estää ohjelmiston kehittäjiltä turha pääsy tuotantoypäristöön.

Toimiin ja menettelyihin sisältyvä huolellisesti suunnitellut roolit yhdessä tehtäviä eriyttämistä koskevien vaatimusten toteuttamisen kanssa sekä riittävien valvontaprosessien toteuttaminen.

Kehitys- ja testaushenkilööön kuuluvat voivat myös vaarantaa tuotantotietojen luottamuksellisuuden. Kehitys- ja testaustoiminnot voivat aiheuttaa tahattomia muutoksia ohjelmiin ja tietoihin, jos niitä käytetään samassa tietokoneympäristössä. Kehitys-, testaus- ja tuotantoypäristöjen pitäminen erillään on tämän vuoksi suositeltavaa, jotta vähennettäisiin tuotannossa oleville ohjelmille ja liiketoiminnan

tiedoille vahingossa tapahtuvien muutosten ja luvattoman käytön riskiä (ks. [kohta 8.33](#), testitietojen suojaaminen).

Joissain tapauksissa kehitys-, testaus- ja tuotantoymäristöjen eroa voidaan tarkoituksellisesti hämärryttää ja testausta voidaan tehdä tuotantoymäristössä tai hallituilla asteittaisilla käyttöönnotolla käyttäjille ja palvelimille (esim. pienelle joukolle pilottikäyttäjiä). Joissain tapauksissa tuotteen testaus voi tapahtua tuotteen organisaation sisäisen tuotantokäytön kautta. Lisäksi käyttöönnoton häiriöajan lyhentämiseksi voidaan tukea kahta identtistä tuotantoymäristöä, joista vain toinen on kullakin hetkellä käytössä.

Tuotantotietojen käytöä kehitys- ja testausympäristöissä tukevat prosessit ovat tarpeellisia (ks. [kohta 8.33](#)).

Organisaatiot voivat harkita tässä kohdassa esitettyjen ohjeiden soveltamista myös koulutusympäristöihin kouluttaessaan loppukäyttäjiä.

## 8.32 Muutoksenhallinta (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuden liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

### Hallintakeino

Tietojenkäsittelypalveluihin ja tietojärjestelmiin tehtäviä muutoksia olisi hallittava muutoksenhallintamenettelyillä.

### Tarkoitus

Ylläpidetään tietoturvallisuutta muutosten toteuttamisen aikana.

### Ohjeistus

Uusien järjestelmien ja suurien muutosten tekemisen olemassa oleviin järjestelmiin olisi noudatettava sovittuja säädöjä ja muodollista prosessia, johon kuuluu dokumentointi, määrittely, testaus, laadunvarmistus ja hallittu toteutus. Hallintavastuiden ja menettelyjen olisi oltava käytössä, jotta muutoksia voidaan hallita tyydyttävästi.

Muutoksenhallintamenettelyt olisi dokumentoitava ja pantava täytäntöön, jotta tietojenkäsittelypalveluissa ja tietojärjestelmissä olevien tietojen luottamuksellisuus, eheys ja saatavuus voidaan varmistaa järjestelmän koko kehityskaaren ajan aina varhaisesta suunnittelusta valmiin järjestelmän ylläpitotoimiin.

Tieto- ja viestintäteknisten infrastruktuurien ja ohjelmistojen muutostenhallintamenettelyt olisi integroitava mahdollisuuksien mukaan.

Muutostenhallintamenettelyjen olisi sisällettävä

- muutosten suunnittelu ja niiden mahdollisten vaikutusten arvointi suhteessa kaikkiin riippuvuuksiin
- muutosten valtuuttaminen
- muutoksia koskeva viestintä olennaisille sidosryhmille
- muutosten testaus ja testien hyväksyntä (ks. [kohta 8.29](#))
- muutosten toteuttaminen, mukaan lukien käyttöönottosuunnitelmat
- häät- ja poikkeustilanteita koskevat näkökohdat, mukaan lukien perääntymismenettelyt

- g) kaiken edellä esitetty tiedon sisältävien muutosta koskevien tallenteiden ylläpitäminen
- h) varmistetaan, että toimintaohjeita (ks. [kohta 5.37](#)) ja käyttäjän menettelyohjeita muutetaan tarvittaessa, jotta ne säilyvät asianmukaisina
- i) varmistetaan, että tieto- ja viestintätekniikkaa koskevia jatkuvuussuunnitelmia sekä vaste- ja toipumismenettelyjä (ks. [kohta 5.30](#)) muutetaan tarvittaessa, jotta ne säilyvät asianmukaisina.

### Lisätiedot

Riittämätön muutostenhallinta on tietojenkäsittelypalvelujen ja tietojärjestelmien toiminta- ja turvallisuushäiriöiden yleinen syy. Tuotantoypäristön muutokset, erityisesti siirrettäessä ohjelmisto kehitysympäristöstä käyttöympäristöön, voivat vaikuttaa sovellusten eheyteen ja saatavuuteen.

Ohjelmistojen muutokset voivat vaikuttaa tuotantoypäristön toimintaan ja päinvastoin.

Hyvään käytäntöön kuuluu uusien tieto- ja viestintäteknisten komponenttien testaus ympäristössä, joka on erotettu sekä tuotanto- että kehitysympäristöstä (ks. [kohta 8.31](#)). Tällä tavoin uusia ohjelmia voidaan valvoa ja testitarkoituksiin käytettävälle tuotantotiedolle saadaan järjestettyä lisäsuojaus. Tämän käytännön olisi koskettava korjaustiedostoja, huoltopaketteja ja muita päivityksiä.

Tuotantoypäristöjä ovat mm. käyttöjärjestelmät, tietokannat ja välioijelmistoalustat. Tätä hallintakeinoa olisi sovellettava myös sovelluksiin ja infrastruktuureihin tehtäviin muutoksiin.

### 8.33 Testauksessa käytettävät tiedot (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuteen liittyvät käsitteet	Toiminnalliset kyvykkydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys	#Suojaus	#Tietojen_suojaaminen	#Suojaaminen

#### Hallintakeino

Testauksessa käytettävät tiedot olisi valittava, suojattava ja hallittava asianmukaisesti.

#### Tarkoitus

Varmistetaan testauksen riittävyys sekä testaukseen käytettävien tuotantotietojen suojaus.

#### Ohjeistus

Testauksessa käytettävät tiedot olisi valittava siten, että voidaan varmistaa testitulojen luotettavuus sekä käytettävien tuotantotietojen luottamuksellisuus. Arkaluonteista tietoa (esim. henkilötietoja) ei saisi kopioida kehitys- ja testausympäristöön (ks. [kohta 8.31](#)).

Seuraavia hallintakeinoja olisi sovellettava testaustarkoituksiin käytettävien tuotantotietojen kopioiden suojaamiseen riippumatta siitä, onko testausympäristö rakennettu organisaation sisälle vai sijaitseeko se pilvipalvelussa:

- a) Samojen pääsynhallinnan menettelyjen soveltaminen testausympäristöön kuin tuotantoypäristöönkin.
- b) Erillisen valtuutuksen edellyttäminen joka kerta, kun tuotantotietoja kopioidaan testausympäristöön.
- c) Tuotantotietojen kopioinnin ja käytön kirjaaminen, jotta kyötään luomaan kirjausketju.
- d) Arkaluonteisten tietojen suojaaminen poistamalla tai peittämällä (ks. [kohta 8.11](#)), jos niitä käytetään.
- e) Tuotantotietojen tunnollinen poistaminen (ks. [kohta 8.10](#)) testausympäristöstä välittömästi testauksen päätyttyä, jotta estetään testauksessa käytettävien tietojen luvaton käyttö.

Testauksessa käytettävät tiedot olisi säilytettävä turvallisesti (jotta estetään luvaton muuttaminen, joka voi johtaa epäpäteviin tuloksiin) ja niitää saisi käyttää vain testaustarkoituksiin.

## Lisätiedot

Järjestelmä- ja hyväksymistestaus voivat edellyttää merkittävää määrää testitietoa, joka on mahdollisimman lähellä tuotantotietoja.

### 8.34 Tietojärjestelmien suojaus auditointitestauksen aikana (EN)

Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ja_verkon_turvallisuus #Tietojen_suojaaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen

#### Hallintakeino

Testaajan ja asiaankuuluvan johdon olisi suunniteltava ja sovittava auditointitestauksista ja muista käytössä olevien järjestelmien arvioinnin sisältävistä varmennustoiminoista.

#### Tarkoitus

Varmistetaan, että auditointi ja muut varmennustoiminnot vaikuttavat käytössä oleviin järjestelmiin ja liiketoimintaprosesseihin mahdollisimman vähän.

#### Ohjeistus

Seuraavia ohjeita olisi noudatettava:

- Järjestelmään ja tietoihin pääsyä koskevista auditointipyynnöistä sovitaan asianmukaisen johdon kanssa.
- Teknisen auditointitestauksen laajuudesta sovitaan ja sitä hallitaan.
- Auditointitestaukset rajoitetaan pelkästään ohjelmistojen ja tietojen lukuoikeuteen. Jos ei voida myöntää vain lukuoikeutta tarvittavien tietojen hankkimiseen, testin voi tehdä auditoijan puolesta kokenut pääkäyttäjä, jolla on tarvittavat pääsyoikeudet.
- Jos pääsy myönnetään, laaditaan ja todennetaan järjestelmän käyttöön käytettyjä laitteita (esim. kannettavat tietokoneet tai tablet-tietokoneen) koskevat turvallisuusvaatimukset (esim. viruksentorjunta ja päivitykset) ennen pääsyn myötämistä.
- Muunlainen pääsyoikeus kuin lukuoikeus sallitaan vain erillisin järjestelmätiedostokopioihin, jotka poistetaan auditoinnin jälkeen tai suojataan asianmukaisesti, jos tällaisten tiedostojen säilyttämistä edellytetään auditoinnin dokumentointivaatimuksissa.
- Erityistä ja lisäkäsittelyä koskevat pyynnöt, kuten auditointityökalujen käyttö, tunnistetaan ja niistä sovitaan.
- Järjestelmän käytettävyyteen mahdollisesti vaikuttavat auditointitestaukset tehdään työajan ulkopuolella.
- Kaikkia auditointi- ja testaustarkoitoksissa annettuja pääsyoikeuksien valvotaan ja niiden toimet kirjataan.

#### Lisätiedot

Auditointitestaus ja muut varmennustoiminnot voidaan tehdä kehitys- ja testausjärjestelmissä, jolloin testaus voi vaikuttaa koodin eheyteen tai johtaa tällaisissa ympäristöissä olevien arkaluonteisten tietojen paljastumiseen.

## Liite A (opastava) **Attribuuttien käyttö (EN)**

### A.1 Yleistä (EN)

Tässä liitteessä on taulukko, jossa esitellään attribuuttien käytöä keinona luoda erilaisia hallintakeinojen näkymiä. Viisi attribuuttiesimerkkiä ovat (ks. [kohta 4.2](#))

- Hallintakeinojen tyypit (#Ehkäisevä, #Havaitseva, #Korjaava)
- Tietoturvaominaisuudet (#Luottamuksellisuus #Eheys #Saatavuus)
- Kyberturvallisuuteen liittyvät käsitteet (#Tunnistus #Suojaus #Vaste #Palautus)
- Toiminnalliset kyvykkyydet (#Hallintotapa, #Omaisuudenhallinta, #Tietojen\_suojaaminen, #Henkilöstöturvallisuus, #Fyysinen\_turvallisuus, #Järjestelmän\_ja\_verkon\_turvallisuus, #Sovelluksen\_turvallisuus, #Turvallinen\_konfigurointi, #Identiteetti\_-ja\_käyttövaltuushallinta, #Uhkien\_ja\_haavoittuvuuksien\_hallinta, #Toimittajasuheteiden\_hallinta, #Lait\_ja\_vaatimustenmukaisuus, #Tietoturvatapahtumien\_hallinta ja #Tietoturvallisuuden\_varmentaminen)
- Tietoturvan osa-alueet (#Hallintotapa\_ja\_ekosysteemi, #Suojaaminen, #Puolustus ja #Kriisinkestävyys).

[Taulukossa A.1](#) on kaikkien tässä asiakirjassa esitettyjen hallintakeinojen ja niille annettujen attribuuttien arvojen matriisi.

Tätä matriisia voidaan suodattaa tai järjestellä tietynlaisella työkalulla, kuten yksinkertaisella laskutaulukolla tai tietokannalla, joka voi sisältää enemmänkin tietoja, kuten hallintakeinon selitteet, sitä koskevan ohjeistuksen, organisaatiokohtaisen ohjeistuksen tai attribuutit (ks. [kohta A.2](#)).

**Taulukko A.1 Hallintakeinojen ja niiden attribuuttien arvojen matriisi**

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">5.1</a>	Tietoturvallisuutta koskevat toimintaperiaatteet	#Ehkäisevä	#Luotta-muksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Kriisinkestävyys
<a href="#">5.2</a>	Tietoturvaroolit ja -vastuu	#Ehkäisevä	#Luotta-muksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Kriisinkestävyys
<a href="#">5.3</a>	Tehtävien eriyttäminen	#Ehkäisevä	#Luotta-muksellisuus #Eheys #Saatavuus	#Suojaus	#Hallintotapa #Identiteetti_-ja_käyttö-valtuushallinta	#Hallintotapa_ja_ekosysteemi
<a href="#">5.4</a>	Johdon vastuu	#Ehkäisevä	#Luotta-muksellisuus #Eheys #Saatavuus	#Tunnistus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi
<a href="#">5.5</a>	Yhteydet viranomaisiin	#Ehkäisevä #Korjaava	#Luotta-muksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus #Kriisinkestävyys

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
<a href="#">5.6</a>	Yhteydet osaan-misyhteisiin	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus
<a href="#">5.7</a>	Uhkatieloston seuranta	#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Havainto #Vaste	#Uhkien_ja_haavoittuvuusk-sien_hallinta	#Puolustus #Kriisinkestäävyyt
<a href="#">5.8</a>	Tietoturvallisuus projektinhallinnassa	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Hallintotapa	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.9</a>	Tietojen ja niihin liittyvien omaisuuserien luettelo	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Omaisuuden-hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.10</a>	Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käytö	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuuden-hallinta #Tietojen_suojaaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.11</a>	Suojattavan omaisuuden palauttaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuuden-hallinta	#Suojaaminen
<a href="#">5.12</a>	Tiedon luokittelut	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Tietojen_suojaaminen	#Suojaaminen #Puolustus
<a href="#">5.13</a>	Tiedon merkintä	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Tietojen_suojaaminen	#Puolustus #Suojaaminen
<a href="#">5.14</a>	Tietojen siirtäminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuuden-hallinta #Tietojen_suojaaminen	#Suojaaminen
<a href="#">5.15</a>	Pääsy- ja käyttö-oikeuksien valvonta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">5.16</a>	Identiteetin hallinta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">5.17</a>	Tunnistautumis-tiedot	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">5.18</a>	Pääsyoikeudet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">5.19</a>	Tietoturvallisuus toimittajasuheteissa	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.20</a>	Toimittajasopimusten tietoturvallisuus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.21</a>	Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.22</a>	Toimittajien palvelujen seuranta, katselointi ja muutoksenhallinta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Toimittajasuheteiden_hallinta #Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus
<a href="#">5.23</a>	Pilvipalvelujen tietoturvallisuus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Toimittajasuheteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.24</a>	Tietoturva-häiriöiden hallinnan suunnittelu ja valmistelu	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Hallintotapa_ja_tietoturvataaptumien_hallinta	#Puolustus
<a href="#">5.25</a>	Tietoturva-tapahtumien arviointi ja niitä koskevien päätösten tekeminen	#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturva-tapahtumien_hallinta	#Puolustus
<a href="#">5.26</a>	Tietoturva-häiriöihin vastaaminen	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Tietoturva-tapahtumien_hallinta	#Puolustus
<a href="#">5.27</a>	Tietoturva-häiriöstä oppiminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietoturva-tapahtumien_hallinta	#Puolustus
<a href="#">5.28</a>	Todisteiden kerääminen	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturva-tapahtumien_hallinta	#Puolustus
<a href="#">5.29</a>	Tietoturvallisuus häiriötilanteessa	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste	#Jatkuvuus	#Suojaaminen #Kriisinkestävyys

Taulukko A.1 (*Jatkuu*)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
<a href="#">5.30</a>	Tieto- ja viestintäteknikan valmius liiketoiminnan jatkuvuussuunnitelussa	#Korjaava	#Saatavuus	#Vaste	#Jatkuuus	#Kriisinkestävyys
<a href="#">5.31</a>	Lainsääädäntöön, asetuksiin, viranomaismäääräyksiin ja sopimuksiin sisältyväät vaatimukset	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Lait_ja_vaatinmustenmukaisuus	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">5.32</a>	Immateriaalioikeudet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Lait_ja_vaatinmustenmukaisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">5.33</a>	Tallenteiden suojaaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Lait_ja_vaatinmustenmukaisuus #Omaisuudenhallinta #Tietojen_suojaaminen	#Puolustus
<a href="#">5.34</a>	Tietosuoja ja henkilötietojen suojaaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietojen_suojaaminen #Lait_ja_vaatinmustenmukaisuus	#Suojaaminen
<a href="#">5.35</a>	Tietoturvallisuuden riippumaton katselointi	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ekosysteemi
<a href="#">5.36</a>	Tietoturvallisuutta koskevien toimintaperiaatteiden, säädöjen ja standardien noudattaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Lait_ja_vaatimustenmukaisuus #Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ekosysteemi

Taulukko A.1 (jatkuu)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">5.37</a>	Dokumentoidut toimintaohjeet	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Palautus	#Omaisuudenhallinta #Fyysinen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus #Sovelluksen_turvallisuus #Turvallinen_konfigurointi #Identiteetti_ ja_käyttövaltuushallinta #Uhkien_ja_haavoittuvuuksien_hallinta #Jatkuvuus #Tietoturvatahtumien_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus
<a href="#">6.1</a>	Taustatarkistus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">6.2</a>	Työsuhteen ehdot	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">6.3</a>	Tietoturvatietoisuus, -opastus ja -koulutus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">6.4</a>	Kurinpitoprosessi	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">6.5</a>	Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Henkilöstöturvallisuus #Omaisuudenhallinta	#Hallintotapa_ja_ekosysteemi
<a href="#">6.6</a>	Salassapito- ja vaitiolasitoumukset	#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Henkilöstöturvallisuus #Tietojen_suojaaminen #Toimittajasuheteiden_hallinta <sup>1)</sup>	#Hallintotapa_ja_ekosysteemi
<a href="#">6.7</a>	Etätyöskentely	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen #Fyysinen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen

<sup>1)</sup> Kansallinen huomautus: Englannin kielisessä tekstissä lukee virheellisesti #Supplier\_relationships, kun kohdassa tulisi lukea #Supplier\_relationships\_security

Taulukko A.1 (*jatkuu*)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
<a href="#">6.8</a>	Tietoturvata-pahtumista raportointi	#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto	#Tietoturva-tapahtumien_hallinta	#Puolustus
<a href="#">7.1</a>	Fyysiset turvaluheet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus	#Suojaaminen
<a href="#">7.2</a>	Kulunvalvonta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus #Identiteetti_ ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">7.3</a>	Toimistojen, tilojen ja laitteistojen suojaus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus #Omaisuuden-hallinta	#Suojaaminen
<a href="#">7.4</a>	Fyysisen turvalisuuden valvonta	#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Fyysinen_turvalisuus	#Suojaaminen #Puolustus
<a href="#">7.5</a>	Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus	#Suojaaminen
<a href="#">7.6</a>	Turva-alueilla työskentely	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus	#Suojaaminen
<a href="#">7.7</a>	Puhdas pöytä ja puhdas näyttö	#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Fyysinen_turvalisuus	#Suojaaminen
<a href="#">7.8</a>	Laitteiden sijoitus ja suojaus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus #Omaisuuden-hallinta	#Suojaaminen
<a href="#">7.9</a>	Toimitilojen ulkopuolelle viedyn omaisuuden turvalisuus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus #Omaisuuden-hallinta	#Suojaaminen
<a href="#">7.10</a>	Tallennus-välineet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysinen_turvalisuus #Omaisuuden-hallinta	#Suojaaminen
<a href="#">7.11</a>	Tukipalvelut	#Ehkäisevä #Havaitseva	#Eheys #Saatavuus	#Suojaus #Havainto	#Fyysinen_turvalisuus	#Suojaaminen
<a href="#">7.12</a>	Kaapeloinnin turvalisuus	#Ehkäisevä	#Luottamuksellisuus #Saatavuus	#Suojaus	#Fyysinen_turvalisuus	#Suojaaminen

Taulukko A.1 (jatkuu)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">7.13</a>	Laitteiden huolto	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Fyysisen_turvallisuus #Omaisuudenhallinta	#Suojaaminen #Kriisinkestävyys
<a href="#">7.14</a>	Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen	#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Fyysisen_turvallisuus #Omaisuudenhallinta	#Suojaaminen
<a href="#">8.1</a>	Käyttäjien päätelaitteet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Omaisuudenhallinta #Tietojen_suojaaminen	#Suojaaminen
<a href="#">8.2</a>	Ylläpito-oikeudet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">8.3</a>	Tietoihin pääsyn rajoittaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">8.4</a>	Pääsy lähdekoodiin	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta #Sovelluksen_turvallisuus #Turvallinen_konfigurointi	#Suojaaminen
<a href="#">8.5</a>	Turvallinen todentaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Identiteetti_ja_käyttövaltuushallinta	#Suojaaminen
<a href="#">8.6</a>	Kapasiteetin-hallinta	#Ehkäisevä #Havaitseva	#Eheys #Saatavuus	#Tunnistus #Suojaus #Havainto	#Jatkuvuus	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">8.7</a>	Haittaohjelmilta suojautuminen	#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Järjestelmä_ja_verkon_turvallisuus #Tietojen_suojaaminen	#Suojaaminen #Puolustus
<a href="#">8.8</a>	Teknisten haavoittuvuuksien hallinta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Uhkien_ja_haavoittuvuuksien_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus
<a href="#">8.9</a>	Konfiguraationhallinta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi	#Suojaaminen
<a href="#">8.10</a>	Tietojen poistaminen	#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Tietojen_suojaaminen #Lait_ja_vaatimustenmukaisuus	#Suojaaminen

Taulukko A.1 (jatkuu)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyyydet	Tietoturvan osa-alueet
<a href="#">8.11</a>	Tietojen peittäminen	#Ehkäisevä	#Luottamuksellisuus	#Suojaus	#Tietojen_suojaaminen	#Suojaaminen
<a href="#">8.12</a>	Tietovuotojen estäminen	#Ehkäisevä #Havaitseva	#Luottamuksellisuus	#Suojaus #Havainto	#Tietojen_suojaaminen #Puolustus	#Suojaaminen
<a href="#">8.13</a>	Tietojen varmuuskopiointi	#Korjaava	#Eheys #Saatavuus	#Palautus	#Jatkuvuus	#Suojaaminen
<a href="#">8.14</a>	Tietojenkäsittelypalvelujen vikasietoisuus	#Ehkäisevä	#Saatavuus	#Suojaus	#Jatkuvuus #Omaisuuden-hallinta	#Suojaaminen #Kriisinkestävyys
<a href="#">8.15</a>	Lokikirjaukset	#Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto	#Tietoturvatapahtumien_hallinta	#Suojaaminen #Puolustus
<a href="#">8.16</a>	Valvontatoiminnot	#Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturvatapahtumien_hallinta	#Puolustus
<a href="#">8.17</a>	Kellojen synkronointi	#Havaitseva	#Eheys	#Suojaus #Havainto	#Tietoturvatapahtumien_hallinta	#Suojaaminen #Puolustus
<a href="#">8.18</a>	Ylläpito- ja hallintasovel-lukset	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmä_ja_verkon_turvallisuus #Turvallinen_konfigurointi #Sovelluksen_turvallisuus	#Suojaaminen
<a href="#">8.19</a>	Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi #Sovelluksen_turvallisuus	#Suojaaminen
<a href="#">8.20</a>	Verkkoturvallisus	#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Järjestelmä_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.21</a>	Verkkopalvelujen turvaami-nen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmä_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.22</a>	Verkkojen eriyttäminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmä_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.23</a>	Verkkosuodatus	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmä_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.24</a>	Salausken käyttö	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Turvallinen_konfigurointi	#Suojaaminen

Taulukko A.1 (jatkuu)

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">8.25</a>	Turvallinen kehittämisen elinkaari	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.26</a>	Sovelluksia koskevat turvallisuusvaatimukset	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen #Puolustus
<a href="#">8.27</a>	Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.28</a>	Turvallinen ohjelointi	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.29</a>	Tietoturvates-taus kehitys- ja hyväksyntä-vaiheissa	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus	#Sovelluksen_turvallisuus #Tietoturvallisuuden_varmentaminen #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.30</a>	Ulkoistettu kehittäminen	#Ehkäisevä #Havaitseva	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus #Havainto	#Järjestelmän_ja_verkon_turvallisuus #Sovelluksen_turvallisuus #Toimittaja-suhteiden_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen
<a href="#">8.31</a>	Kehitys-, testaus- ja tuotanto-ympäristöjen erottaminen	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.32</a>	Muutoksen-hallinta	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Sovelluksen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus	#Suojaaminen
<a href="#">8.33</a>	Testauksessa käytettävät tiedot	#Ehkäisevä	#Luottamuksellisuus #Eheys	#Suojaus	#Tietojen_suojaaminen	#Suojaaminen
<a href="#">8.34</a>	Tietojärjestelmien suojaus auditointites-tauksen aikana	#Ehkäisevä	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus	#Järjestelmän_ja_verkon_turvallisuus #Tietojen_suojaaminen	#Hallintotapa_ja_ekosysteemi #Suojaaminen

[Taulukossa A.2](#) on esimerkki siitä, miten voidaan luoda haluttu näkymä suodattamalla tiettyjä attribuuttien arvoja, tässä tapauksessa arvoa #Korjaava.

### Taulukko A.2 #Korjaavien hallintakeinojen näkymä

Standardin ISO/IEC 27002 hallintakeinon tunniste	Hallintakeinon nimi	Hallintakeinon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">5.5</a>	Yhteydet viranomaisiin	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus #Kriisinkestävyys
<a href="#">5.6</a>	Yhteydet osaamisyhteisöihin	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste #Palautus	#Hallintotapa	#Puolustus
<a href="#">5.7</a>	Uhkatiledon seuranta	#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Havainto #Vaste	#Uhkien_ja_haavoittuvuuskien_hallinta	#Puolustus #Kriisinkestävyys
<a href="#">5.24</a>	Tietoturva-häiriöiden hallinnan suunnittelu ja valmistelu	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Hallintotapa #Tietoturvatapahtumien_hallinta	#Puolustus
<a href="#">5.26</a>	Tietoturvahäiriöihin vastaaminen	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Vaste #Palautus	#Tietoturvatapahtumien_hallinta	#Puolustus
<a href="#">5.28</a>	Todisteiden kerääminen	#Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturvatapahtumien_hallinta	#Puolustus
<a href="#">5.29</a>	Tietoturvallisuus häiriötilanteessa	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste	#Jatkuvuus	#Suojaaminen #Kriisinkestävyys
<a href="#">5.30</a>	Tieto- ja viestintäteknikan valmius liiketoiminnan jatkuvuussuunnitelussa	#Korjaava	#Saatavuus	#Vaste	#Jatkuvuus	#Kriisinkestävyys
<a href="#">5.35</a>	Tietoturvallisuuden riippumaton katselointi	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Tunnistus #Suojaus	#Tietoturvallisuuden_varmentaminen	#Hallintotapa_ja_ekosysteemi

Taulukko A.2 (jatkuu)

Standardin ISO/IEC 27002 hallintakeidon tunniste	Hallintakeidon nimi	Hallintakeidon tyyppi	Tietoturva-ominaisuudet	Kyberturvallisuuteen liittyvät käsitteet	Toiminnalliset kyvykkyydet	Tietoturvan osa-alueet
<a href="#">5.37</a>	Dokumentoidut toimintaohjeet	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Palautus	#Omaisuudenhallinta #Fyysisen_turvallisuus #Järjestelmän_ja_verkon_turvallisuus #Soveluksen_turvallisuus #Turvallinen_konfigurointi #Identiteetti ja käyttövaltuushallinta #Uhkien_ja_haavoittuvuuskien_hallinta #Jatkuvuus #Tietoturvatapahtumien_hallinta	#Hallintotapa_ja_ekosysteemi #Suojaaminen #Puolustus
<a href="#">6.4</a>	Kurinpito-prosessi	#Ehkäisevä #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Vaste	#Henkilöstöturvallisuus	#Hallintotapa_ja_ekosysteemi
<a href="#">8.7</a>	Haittaohjelmilta suojautuminen	#Ehkäisevä #Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Suojaus #Havainto	#Järjestelmän_ja_verkon_turvallisuus #Tietojen_suojaaminen	#Suojaaminen #Puolustus
<a href="#">8.13</a>	Tietojen varmuuskopiointi	#Korjaava	#Eheys #Saatavuus	#Palautus	#Jatkuvuus	#Suojaaminen
<a href="#">8.16</a>	Valvontatoiminnot	#Havaitseva #Korjaava	#Luottamuksellisuus #Eheys #Saatavuus	#Havainto #Vaste	#Tietoturvatapahtumien_hallinta	#Puolustus

## A.2 Organisaation näkymät (EN)

Koska attribuuteilla voidaan luoda erilaisia hallintakeinoja koskevia näkymiä, organisaatiot voivat hylätä tässä asiakirjassa ehdotetut attribuutit ja luoda omat attribuuttinsa, joilla on organisaation tarpeisiin pohjautuvat erilaiset arvot. Lisäksi kullekin attribuutille annetut arvot voivat vaihdella organisaatioittain, koska organisaatioilla voi olla erilaiset näkemykset hallintakeinot käytöstä tai sovellettavuudesta tai attribuuttiin liittyvistä arvoista (kun arvot koskevat nimenomaista organisaation toimintaympäristöä). Ensimmäinen vaihe on perustella, miksi tarvitaan organisaatiokohtaisia attribuutteja. Jos organisaatio on esimerkiksi perustanut riskinkäsittelysuunnitelmansa (ks. standardin ISO/IEC 27001:2013 kohta 6.1.3 e) tapahtumiin, voi se haluta yhdistää riskiskenaarioiden attribuutit kuhunkin tämän asiakirjan hallintakeinoon.

Tällaisten attribuuttien etuna on standardissa ISO/IEC 27001 esitettyjen riskien käsittelyyn liittyvien vaatimusten nopeampi täyttäminen, kun riskien käsittelyprosessissa määriteltyjä hallintakeinoja (joihin viitataan "tarvittavina" hallintakeinoina) verrataan standardin ISO/IEC 27001:2013 [liitteen A](#) hallintakeinoihin (jotka ovat peräisin tästä asiakirjasta), jotta voidaan varmistaa, että yhtäkään tarvittavaa hallintakeinoa ei ole ohitettu.

Kun tarkoitus ja hyödyt ovat selvillä, seuraava vaihe on määrittää attribuuttien arvot. Organisaatio voi tunnistaa esimerkiksi 9 tapahtumaa:

- 1) mobiililaitteiden häviäminen tai varkaus
- 2) organisaation tiloissa tapahtuva tavaroiden häviäminen tai varkaus
- 3) force majeure -kriisit, vandalismi ja terrorismi
- 4) ohjelmistojen, laitteistojen, virransaannin, internetyhteyden ja viestintäyhteyksien vikaantuminen
- 5) petos
- 6) hakkerointi
- 7) tietojen paljastaminen
- 8) rikokset
- 9) sosiaalinen tiedustelu.

Toinen vaihe voidaan siis toteuttaa osoittamalla tunnisteet kullekin tapahtumalle (esim. E1, E2, ..., E9).

Kolmannessa vaiheessa kopioidaan hallintakeinojen tunnisteet ja nimet tästä asiakirjasta laskutaulukkoon tai tietokantaan ja määritellään attribuuttien arvot kullekin hallintakeinolle. On muistettava, että kullakin hallintakeinolla voi olla useampi attribuutin arvo.

Viimeisessä vaiheessa järjestetään laskutaulukko tai tehdään tietokantakysely, jotta voidaan saada tarvittava tieto.

Muita esimerkkejä organisaatiokohtaisista attribuuteista (ja mahdollisista arvoista) ovat esim.

- a) kypsyys (arvot standardisarjasta ISO/IEC 33000 tai muista kypyysmallista)
- b) toteuttamisen aste (tehtävä, toteutuksessa, osittain toteutettu, täysin toteutettu)
- c) prioriteetti (1, 2, 3 jne.)
- d) organisaation asiaan liittyvät alueet (turvallisuus, tieto- ja viestintätekniikka, henkilöresurssit, ylin johto jne.)
- e) tapahtumat
- f) niihin liittyvä omaisuus
- e) koostaminen ja käyttö (*build and run*), jolla erotetaan palvelun elinkaaren eri vaiheissa käytettävät hallintakeinot
- g) muut puitteet, joita organisaatio käyttää tai joista se on ehkä siirtymässä.

**Liite B**  
**(opastava)**  
**Standardin ISO/IEC 27002:2022 (tämä asiakirja)**  
**vastaavuus standardiin ISO/IEC 27002:2013 (EN)**

Tämän liitteen tarkoitus on mahdollistaa yhteensopivuus standardin ISO/IEC 27002:2012 kanssa organisaatioille, jotka käyttävät kyseistä standardia mutta haluavat siirtyä tähän uuteen versioon.

[Taulukossa B.1](#) luetellaan tämän asiakirjan [kohdissa 5–8](#) määriteltyjen hallintakeinojen vastaavuus standardissa ISO/IEC 27002:2013 määriteltyjen hallintakeinojen kanssa.

**Taulukko B.1 Tässä asiakirjassa olevien hallintakeinojen vastaavuus standardissa ISO/IEC 27002:2013 oleviin hallintakeinoihin**

Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Hallintakeinon nimi
<a href="#">5.1</a>	05.1.1, 05.1.2	Tietoturvallisuutta koskevat toimintaperiaatteet
<a href="#">5.2</a>	06.1.1	Tietoturvaroolit ja -vastuut
<a href="#">5.3</a>	06.1.2	Tehtävien eriyttäminen
<a href="#">5.4</a>	07.2.1	Johdon vastuut
<a href="#">5.5</a>	06.1.3	Yhteydet viranomaisiin
<a href="#">5.6</a>	06.1.4	Yhteydet osaamisyhteisöihin
<a href="#">5.7</a>	New	Ulkotiedon seuranta
<a href="#">5.8</a>	06.1.5, 14.1.1	Tietoturvallisuus projektinhallinnassa
<a href="#">5.9</a>	08.1.1, 08.1.2	Tietojen ja niihin liittyvien omaisuuserien luettelo
<a href="#">5.10</a>	08.1.3, 08.2.3	Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö
<a href="#">5.11</a>	08.1.4	Omaisuuden palauttaminen
<a href="#">5.12</a>	08.2.1	Tiedon luokittelu
<a href="#">5.13</a>	08.2.2	Tiedon merkintä
<a href="#">5.14</a>	13.2.1, 13.2.2, 13.2.3	Tietojen siirtäminen
<a href="#">5.15</a>	09.1.1, 09.1.2	Pääsynhallinta
<a href="#">5.16</a>	09.2.1	Identiteetin hallinta
<a href="#">5.17</a>	09.2.4, 09.3.1, 09.4.3	Tunnistautumistiedot
<a href="#">5.18</a>	09.2.2, 09.2.5, 09.2.6	Pääsyoikeudet
<a href="#">5.19</a>	15.1.1	Tietoturvallisuus toimittajasuheteissa
<a href="#">5.20</a>	15.1.2	Toimittajasopimusten tietoturvallisuus
<a href="#">5.21</a>	15.1.3	Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa
<a href="#">5.22</a>	15.2.1, 15.2.2	Toimittajien palvelujen seuranta, katselointi ja muutoksenhallinta
<a href="#">5.23</a>	Uusi	Pilvipalvelujen tietoturvallisuus
<a href="#">5.24</a>	16.1.1	Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu
<a href="#">5.25</a>	16.1.4	Tietoturvatapahtumien arvointi ja niitä koskevien päätösten tekeminen
<a href="#">5.26</a>	16.1.5	Tietoturvahäiriöihin reagointi
<a href="#">5.27</a>	16.1.6	Tietoturvahäiriöistä oppiminen
<a href="#">5.28</a>	16.1.7	Todisteiden kerääminen
<a href="#">5.29</a>	17.1.1, 17.1.2, 17.1.3	Tietoturvallisuus häiriötilanteessa
<a href="#">5.30</a>	Uusi	Tieto- ja viestintätekniikan valmias liiketoiminnan jatkuvuussuunnitte-lussa

**Taulukko B.1 (jatkuu)**

Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Hallintakeinon nimi
<a href="#">5.31</a>	18.1.1, 18.1.5	Lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset
<a href="#">5.32</a>	18.1.2	Immateriaalioikeudet
<a href="#">5.33</a>	18.1.3	Tallenteiden suojaaminen
<a href="#">5.34</a>	18.1.4	Tietosuoja ja henkilötietojen suojaaminen
<a href="#">5.35</a>	18.2.1	Tietoturvallisuuden riippumaton katselointi
<a href="#">5.36</a>	18.2.2, 18.2.3	Tietoturvallisuutta koskevien toimintaperiaatteiden, sääntöjen ja standarien noudattaminen
<a href="#">5.37</a>	12.1.1	Dokumentoidut toimintaohjeet
<a href="#">6.1</a>	07.1.1	Taustatarkistus
<a href="#">6.2</a>	07.1.2	Työsuhteen ehdot
<a href="#">6.3</a>	07.2.2	Tietoturvatisuojaus, -opastus ja -koulutus
<a href="#">6.4</a>	07.2.3	Kurinpitoprosessi
<a href="#">6.5</a>	07.3.1	Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut
<a href="#">6.6</a>	13.2.4	Salassapito- ja vaitiilositoumukset
<a href="#">6.7</a>	06.2.2	Etätyöskentely
<a href="#">6.8</a>	16.1.2, 16.1.3	Tietoturvatapahtumista raportointi
<a href="#">7.1</a>	11.1.1	Fyysiset turva-alueet
<a href="#">7.2</a>	11.1.2, 11.1.6	Kulunvalvonta
<a href="#">7.3</a>	11.1.3	Toimistojen, tilojen ja laitteistojen suojaus
<a href="#">7.4</a>	Uusi	Fyysisen turvallisuuden valvonta
<a href="#">7.5</a>	11.1.4	Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan
<a href="#">7.6</a>	11.1.5	Turva-alueilla työskentely
<a href="#">7.7</a>	11.2.9	Puhdas pöytä ja puhdas näyttö
<a href="#">7.8</a>	11.2.1	Laitteiden sijoitus ja suojaus
<a href="#">7.9</a>	11.2.6	Toimitilojen ulkopuolelle viedyn omaisuuden turvallisuus
<a href="#">7.10</a>	08.3.1, 08.3.2, 08.3.3, 11.2.5	Tallennusvälineet
<a href="#">7.11</a>	11.2.2	Tukipalvelut
<a href="#">7.12</a>	11.2.3	Kaapeloinnin turvallisuus
<a href="#">7.13</a>	11.2.4	Laitteiden huolto
<a href="#">7.14</a>	11.2.7	Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen
<a href="#">8.1</a>	06.2.1, 11.2.8	Käyttäjien päätelaitteet
<a href="#">8.2</a>	09.2.3	Ylläpito-oikeudet
<a href="#">8.3</a>	09.4.1	Tietoihin pääsyn rajoittaminen
<a href="#">8.4</a>	09.4.5	Pääsy lähdekoodiin
<a href="#">8.5</a>	09.4.2	Turvallinen todentaminen
<a href="#">8.6</a>	12.1.3	Kapasiteetinhallinta
<a href="#">8.7</a>	12.2.1	Haittaohjelmilta suojautuminen
<a href="#">8.8</a>	12.6.1, 18.2.3	Teknisten haavoittuvuuksien hallinta
<a href="#">8.9</a>	Uusi	Konfiguraationhallinta
<a href="#">8.10</a>	Uusi	Tietojen poistaminen
<a href="#">8.11</a>	Uusi	Tietojen peittäminen

**Taulukko B.1 (jatkuu)**

Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Hallintakeinon nimi
<a href="#">8.12</a>	Uusi	Tietovuotojen estäminen
<a href="#">8.13</a>	12.3.1	Tietojen varmuuskopiointi
<a href="#">8.14</a>	17.2.1	Tietojenkäsittelypalvelujen vikasietoisuus
<a href="#">8.15</a>	12.4.1, 12.4.2, 12.4.3	Lokkirajaukset
<a href="#">8.16</a>	Uusi	Valvontatoiminnot
<a href="#">8.17</a>	12.4.4	Kellojen synkronointi
<a href="#">8.18</a>	09.4.4	Ylläpito- ja hallintasovellukset
<a href="#">8.19</a>	12.5.1, 12.6.2	Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin
<a href="#">8.20</a>	13.1.1	Verkkoturvallisuus
<a href="#">8.21</a>	13.1.2	Verkkopalvelujen turvaaminen
<a href="#">8.22</a>	13.1.3	Verkkojen eriyttäminen
<a href="#">8.23</a>	Uusi	Verkkosuodatus
<a href="#">8.24</a>	10.1.1, 10.1.2	Salaksen käyttö
<a href="#">8.25</a>	14.2.1	Turvallinen kehittämisen elinkaari
<a href="#">8.26</a>	14.1.2, 14.1.3	Sovelluksia koskevat turvallisuusvaatimukset
<a href="#">8.27</a>	14.2.5	Turvallisen järjestelmäärrikkitehtuurin ja -suunnittelun periaatteet
<a href="#">8.28</a>	Uusi	Turvallinen ohjelmointi
<a href="#">8.29</a>	14.2.8, 14.2.9	Tietoturvatestaus kehitys- ja hyväksyntävaiheissa
<a href="#">8.30</a>	14.2.7	Ulkoistettu kehittäminen
<a href="#">8.31</a>	12.1.4, 14.2.6	Kehitys-, testaus- ja tuotantoypäristöjen erottaminen
<a href="#">8.32</a>	12.1.2, 14.2.2, 14.2.3, 14.2.4	Muutoksenhallinta
<a href="#">8.33</a>	14.3.1	Testauksessa käytettävät tiedot
<a href="#">8.34</a>	12.7.1	Tietojärjestelmien suojaus auditointitestauksen aikana

[Taulukossa B.2](#) esitetään standardissa ISO/IEC 27002:2013 olevien hallintakeinojen vastaavuus tässä asiakirjassa oleviin hallintakeinoihin

**Taulukko B.2 Standardissa ISO/IEC 27002:2013 olevien hallintakeinojen vastaavuus tässä asiakirjassa oleviin hallintakeinoihin**

Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Hallintakeinon nimi standardissa EN ISO/IEC 27002:2013.
5		Tietoturvalaitteet
5.1		Johdon ohjaus tietoturvallisuutta koskevissa asioissa
5.1.1	<a href="#">5.1</a>	Tietoturvalaitteet
5.1.2	<a href="#">5.1</a>	Tietoturvalaitteiden katselointi
6		Tietoturvallisuuden organisointi
6.1		Sisäinen organisaatio
6.1.1	<a href="#">5.2</a>	Tietoturvaroolit ja -vastuu
6.1.2	<a href="#">5.3</a>	Tehtävien eriyttäminen
6.1.3	<a href="#">5.5</a>	Yhteydet viranomaisiin
6.1.4	<a href="#">5.6</a>	Yhteydet osaamisyhteisöihin

**Taulukko B.2 (jatkuu)**

Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Hallintakeinon nimi standardissa EN ISO/IEC 27002:2013.
6.1.5	<a href="#">5.8</a>	Tietoturvallisuus projektinhallinnassa
6.2		Mobiililaitteet ja etätyö
6.2.1	<a href="#">8.1</a>	Mobiililaitteita koskeva poliittikka
6.2.2	<a href="#">6.7</a>	Etätyö
7		Henkilöstöturvallisuus
7.1		Ennen työsuhteen alkua
7.1.1	<a href="#">6.1</a>	Taustatarkistus
7.1.2	<a href="#">6.2</a>	Työsopimuksen ehdot
7.2		Työsuhteen aikana
7.2.1	<a href="#">5.4</a>	Johdon vastuut
7.2.2	<a href="#">6.3</a>	Tietoturvatietoisuus, -opastus ja -koulutus
7.2.3	<a href="#">6.4</a>	Kurinpitoprosessi
7.3		Työsuhteen päättyminen tai muuttuminen
7.3.1	<a href="#">6.5</a>	Työsuhteen päättyminen tai vastuiden muuttuminen
8		Suojattavan omaisuuden hallinta
8.1		Vastuu suojattavasta omaisuudesta
8.1.1	<a href="#">5.9</a>	Suojattavan omaisuuden luetteloiminen
8.1.2	<a href="#">5.9</a>	Suojattavan omaisuuden omistajuus
8.1.3	<a href="#">5.10</a>	Suojattavan omaisuuden hyväksyttävä käyttö
8.1.4	<a href="#">5.11</a>	Suojattavan omaisuuden palauttaminen
8.2		Tietojen luokittelut
8.2.1	<a href="#">5.12</a>	Tiedon luokittelut
8.2.2	<a href="#">5.13</a>	Tiedon merkintä
8.2.3	<a href="#">5.10</a>	Suojattavan omaisuuden käsitteily
8.3		Tietovälineiden käsitteily
8.3.1	<a href="#">7.10</a>	Siirrettävien tietovälineiden hallinta
8.3.2	<a href="#">7.10</a>	Tietovälineiden hävittäminen
8.3.3	<a href="#">7.10</a>	Fyysisien tietovälineiden siirtäminen
9		Pääsynhallinta
9.1		Pääsynhallinnan liiketoiminnalliset vaatimukset
9.1.1	<a href="#">5.15</a>	Pääsynhallintapolitiikka
9.1.2	<a href="#">5.15</a>	Pääsy verkkoihin ja verkkopalveluihin
9.2		Pääsyoikeuksien hallinta
9.2.1	<a href="#">5.16</a>	Käyttäjien rekisteröinti ja poistaminen
9.2.2	<a href="#">5.18</a>	Pääsyoikeuksien jakaminen
9.2.3	<a href="#">8.2</a>	Ylläpito-oikeuksien hallinta
9.2.4	<a href="#">5.17</a>	Käyttäjien tunnistautumistietojen hallinta
9.2.5	<a href="#">5.18</a>	Pääsyoikeuksien uudelleenarvointi
9.2.6	<a href="#">5.18</a>	Pääsyoikeuksien poistaminen tai muuttaminen
9.3		Käyttäjän vastuut
9.3.1	<a href="#">5.17</a>	Tunnistautumistietojen käyttö
9.4		Järjestelmien ja sovellusten pääsynhallinta

**Taulukko B.2 (jatkuu)**

Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Hallintakeinon nimi standardissa EN ISO/IEC 27002:2013.
9.4.1	<a href="#">8.3</a>	Tietoihin pääsyn rajoittaminen
9.4.2	<a href="#">8.5</a>	Turvallinen kirjautuminen
9.4.3	<a href="#">5.17</a>	Salasanojen hallintajärjestelmä
9.4.4	<a href="#">8.18</a>	Ylläpito- ja hallintasovellukset
9.4.5	<a href="#">8.4</a>	Lähdekoodin suojaaminen pääsynhallinnalla
10		Salaus
10.1		Salausen hallinta
10.1.1	<a href="#">8.24</a>	Salausen käytön periaatteet
10.1.2	<a href="#">8.24</a>	Salausavainten hallinta
11		Fyysinen turvallisuus ja ympäristön turvallisuus
11.1		Turva-alueet
11.1.1	<a href="#">7.1</a>	Fyysinen turva-alue
11.1.2	<a href="#">7.2</a>	Kulunvalvonta
11.1.3	<a href="#">7.3</a>	Toimistojen, tilojen ja laitteistojen suojaus
11.1.4	<a href="#">7.5</a>	Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan
11.1.5	<a href="#">7.6</a>	Turva-alueilla työskentely
11.1.6	<a href="#">7.2</a>	Toimitus- ja kuormausalueet
11.2		Laitteet
11.2.1	<a href="#">7.8</a>	Laitteiden sijoitus ja suojaus
11.2.2	<a href="#">7.11</a>	Peruspalvelut
11.2.3	<a href="#">7.12</a>	Kaapeloinnin turvallisuus
11.2.4	<a href="#">7.13</a>	Laitteiden huolto
11.2.5	<a href="#">7.10</a>	Suojattavan omaisuuden poistaminen
11.2.6	<a href="#">7.9</a>	Toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus
11.2.7	<a href="#">7.14</a>	Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen
11.2.8	<a href="#">8.1</a>	Ilman valvontaa jäävät laitteet
11.2.9	<a href="#">7.7</a>	Puhtaan pöydän ja puhtaan näytön periaate
12		Käyttöturvallisuus
12.1		Toimintaohjeet ja velvollisuudet
12.1.1	<a href="#">5.37</a>	Dokumentoidut toimintaohjeet
12.1.2	<a href="#">8.32</a>	Muutoksenhallinta
12.1.3	<a href="#">8.6</a>	Kapasiteetinhallinta
12.1.4	<a href="#">8.31</a>	Kehitys-, testaus- ja tuotantoympäristöjen erottaminen
12.2		Haittaohjelmilta suojaaminen
12.2.1	<a href="#">8.7</a>	Haittaohjelmilta suojaaminen
12.3		Varmuuskopiointi
12.3.1	<a href="#">8.13</a>	Tietojen varmuuskopiointi
12.4		Kirjaaminen ja seuranta
12.4.1	<a href="#">8.15</a>	Tapahtumien kirjaaminen
12.4.2	<a href="#">8.15</a>	Lokitietojen suojaaminen
12.4.3	<a href="#">8.15</a>	Pääkäyttäjä- ja operaattorilokit

**Taulukko B.2 (jatkuu)**

Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Hallintakeinon nimi standardissa EN ISO/IEC 27002:2013.
12.4.4	<a href="#">8.17</a>	Kellojen synkronointi
12.5		Tuotantokäytössä olevien ohjelmistojen hallinta
12.5.1	<a href="#">8.19</a>	Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin
12.6		Teknisten haavoittuvuuksien hallinta
12.6.1	<a href="#">8.8</a>	Teknisten haavoittuvuuksien hallinta
12.6.2	<a href="#">8.19</a>	Ohjelmien asentamisen rajoittaminen
12.7		Tietojärjestelmien auditointinäkökohtia
12.7.1	<a href="#">8.34</a>	Tietojärjestelmien auditointimekanismit
13		Viestintäturvallisuus
13.1		Verkon turvallisuuden hallinta
13.1.1	<a href="#">8.20</a>	Verkon hallinta
13.1.2	<a href="#">8.21</a>	Verkkopalvelujen turvaaminen
13.1.3	<a href="#">8.22</a>	Ryhmiä eriyttäminen verkossa
13.2		Tietojen siirtäminen
13.2.1	<a href="#">5.14</a>	Tiedonsiirtopoliikit ja -menettelyt
13.2.2	<a href="#">5.14</a>	Tiedonsiirtoa koskevat sopimukset
13.2.3	<a href="#">5.14</a>	Sähköinen viestintä
13.2.4	<a href="#">6.6</a>	Salassapito- ja vaitioloitoumukset
14		Järjestelmien hankkiminen, kehittäminen ja ylläpito
14.1		Tietojärjestelmiä koskevat turvallisuusvaatimukset
14.1.1	<a href="#">5.8</a>	Tietoturvavaatimusten analysointi ja määrittely
14.1.2	<a href="#">8.26</a>	Sovelluspalveluiden suojaaminen julkisissa verkoissa
14.1.3	<a href="#">8.26</a>	Sovelluspalvelutapahtumien suojaaminen
14.2		Kehitys- ja tukiprosessien turvallisuus
14.2.1	<a href="#">8.25</a>	Turvallisen kehittämisen poliittika
14.2.2	<a href="#">8.32</a>	Järjestelmään tehtävien muutosten hallintamenettelyt
14.2.3	<a href="#">8.32</a>	Sovellusten tekninen katselointi käyttöalustan muutosten jälkeen
14.2.4	<a href="#">8.32</a>	Ohjelmistopakettien muutoksia koskevat rajoitukset
14.2.5	<a href="#">8.27</a>	Turvallisen järjestelmäsuunnittelun periaatteet
14.2.6	<a href="#">8.31</a>	Turvallinen kehitysympäristö
14.2.7	<a href="#">8.30</a>	Ulkoistettu kehittäminen
14.2.8	<a href="#">8.29</a>	Järjestelmän turvallisuustestaus
14.2.9	<a href="#">8.29</a>	Järjestelmän hyväksymistestaus
14.3		Testiaineisto
14.3.1	<a href="#">8.33</a>	Testiaineiston suojaaminen
15		Suhteet toimittajiin
15.1		Tietoturvallisuus toimittajasuhdeissa
15.1.1	<a href="#">5.19</a>	Toimittajasuhdeiden tietoturvapolitiikka
15.1.2	<a href="#">5.20</a>	Toimittajasopimusten turvallisuus
15.1.3	<a href="#">5.21</a>	Tieto- ja viestintätekniikan toimitusketju
15.2		Toimittajien palveluiden hallinta
15.2.1	<a href="#">5.22</a>	Toimittajien palvelujen seuranta ja katselointi

**Taulukko B.2 (jatkuu)**

Standardin ISO/ IEC 27002:2013 hallintakeinon tunniste	Standardin ISO/ IEC 27002:2022 hallintakeinon tunniste	Hallintakeinon nimi standardissa EN ISO/IEC 27002:2013.
15.2.2	<a href="#">5.22</a>	Toimittajan palveluihin tulevien muutosten hallinta
16		Tietoturvahäiriöiden hallinta
16.1		Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta
16.1.1	<a href="#">5.24</a>	Vastuu ja menettelyt
16.1.2	<a href="#">6.8</a>	Tietoturvatahtumien raportointi
16.1.3	<a href="#">6.8</a>	Tietoturvaheikkouksien raportointi
16.1.4	<a href="#">5.25</a>	Tietoturvatahtumien arvointi ja niitä koskevien päätösten tekeminen
16.1.5	<a href="#">5.26</a>	Tietoturvahäiriöihin vastaaminen
16.1.6	<a href="#">5.27</a>	Tietoturvahäiriöistä oppiminen
16.1.7	<a href="#">5.28</a>	Todisteiden kokoaminen
17		Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
17.1		Tietoturvallisuuden jatkuvuus
17.1.1	<a href="#">5.29</a>	Tietoturvallisuuden jatkuvuuden suunnittelu
17.1.2	<a href="#">5.29</a>	Tietoturvallisuuden jatkuvuuden toteuttaminen
17.1.3	<a href="#">5.29</a>	Tietoturvallisuuden jatkuvuuden todentaminen, katselointi ja arvointi
17.2		Vikasietoisuus
17.2.1	<a href="#">8.14</a>	Tietojenkäsittelypalvelujen saatavuus
18		Vaatimustenmukaisuus
18.1		Lainsääädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen
18.1.1	<a href="#">5.31</a>	Sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen
18.1.2	<a href="#">5.32</a>	Immateriaalioikeudet
18.1.3	<a href="#">5.33</a>	Tallenteiden suojaaminen
18.1.4	<a href="#">5.34</a>	Tietosuoja ja henkilötietojen suojaaminen
18.1.5	<a href="#">5.31</a>	Salaustekniikan hallintaa koskevat säädökset
18.2		Tietoturvallisuuden katselmoinnit
18.2.1	<a href="#">5.35</a>	Tietoturvallisuuden riippumaton katselointi
18.2.2	<a href="#">5.36</a>	Turvallisuuuspolitiikkojen ja -standardien noudattaminen
18.2.3	<a href="#">5.36, 8.8</a>	Teknisen vaatimustenmukaisuuden katselointi

## Kirjallisuus [\(EN\)](#)

- [1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO 55001, *Asset management — Management systems — Requirements*
- [3] ISO/IEC 11770 (kaikki osat), *Information security — Key management*
- [4] ISO/IEC 15408 (kaikki osat), *Information technology — Security techniques — Evaluation criteria for IT security*
- [5] ISO 15489 (kaikki osat), *Information and documentation — Records management*
- [6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
- [7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
- [8] ISO/IEC 19086 (kaikki osat), *Cloud computing — Service level agreement (SLA) framework*
- [9] ISO/IEC 19770 (kaikki osat), *Information technology — IT asset management*
- [10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- [11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
- [12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
- [13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
- [14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
- [15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
- [16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
- [17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
- [18] ISO/IEC/TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
- [19] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
- [20] ISO/IEC 24760 (kaikki osat), *IT Security and Privacy — A framework for identity management*
- [21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
- [22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
- [23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
- [24] ISO/IEC/TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*
- [25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*

- [26] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
- [27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
- [30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [31] ISO/IEC 27033 (kaikki osat), *Information technology — Security techniques — Network security*
- [32] ISO/IEC 27034 (kaikki osat), *Information technology — Application security*
- [33] ISO/IEC 27035 (kaikki osat), *Information technology — Security techniques — Information security incident management*
- [34] ISO/IEC 27036 (kaikki osat), *Information technology — Security techniques — Information security for supplier relationships*
- [35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [37] ISO/IEC 27050 (kaikki osat), *Information technology — Electronic discovery*
- [38] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
- [39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
- [40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
- [41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
- [42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
- [43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*
- [44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
- [45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
- [46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
- [47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
- [48] ISO 31000:2018, *Risk management — Guidelines*
- [49] IEC 31010, *Risk management — Risk assessment techniques*
- [50] ISO/IEC 22123 (kaikki osat), *Information technology — Cloud computing*
- [51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

- [52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at <https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/>
- [53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076
- [54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-37r2>
- [55] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at [https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/)
- [56] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at <https://github.com/OWASP/DevGuide>
- [57] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-63b>
- [58] OASIS. Structured Threat Information Expression. Available at <https://www.oasis-open.org/standards#stix2.0>
- [59] OASIS. Trusted Automated Exchange of Indicator Information. Available at <https://www.oasis-open.org/standards#taxii2.0>

## **SFS-EN ISO/IEC 27002:2022**

*Information security, cybersecurity and privacy protection.  
Information security controls (ISO/IEC 27002:2022)*

### **Contents**

	Page
<b>European foreword (CEN) .....</b>	<b>167</b>
<b>Foreword (ISO).....</b>	<b>168</b>
<b>Introduction.....</b>	<b>169</b>
<b>1 Scope .....</b>	<b>172</b>
<b>2 Normative references .....</b>	<b>172</b>
<b>3 Terms, definitions and abbreviated terms .....</b>	<b>172</b>
3.1 Terms and definitions .....	172
3.2 Abbreviated terms.....	177
<b>4 Structure of this document.....</b>	<b>178</b>
4.1 Clauses.....	178
4.2 Themes and attributes .....	178
4.3 Control layout.....	180

<b>5</b>	<b>Organizational controls.....</b>	<b>180</b>
5.1	Policies for information security.....	180
5.2	Information security roles and responsibilities.....	182
5.3	Segregation of duties.....	183
5.4	Management responsibilities.....	184
5.5	Contact with authorities.....	185
5.6	Contact with special interest groups.....	185
5.7	Threat intelligence.....	186
5.8	Information security in project management.....	187
5.9	Inventory of information and other associated assets.....	189
5.10	Acceptable use of information and other associated assets.....	190
5.11	Return of assets.....	191
5.12	Classification of information.....	192
5.13	Labelling of information.....	194
5.14	Information transfer.....	195
5.15	Access control.....	197
5.16	Identity management.....	199
5.17	Authentication information.....	200
5.18	Access rights.....	202
5.19	Information security in supplier relationships.....	203
5.20	Addressing information security within supplier agreements.....	205
5.21	Managing information security in the ICT supply chain.....	207
5.22	Monitoring, review and change management of supplier services.....	209
5.23	Information security for use of cloud services.....	211
5.24	Information security incident management planning and preparation.....	213
5.25	Assessment and decision on information security events.....	214
5.26	Response to information security incidents.....	215
5.27	Learning from information security incidents.....	216
5.28	Collection of evidence.....	217
5.29	Information security during disruption.....	218
5.30	ICT readiness for business continuity.....	218
5.31	Legal, statutory, regulatory and contractual requirements.....	220
5.32	Intellectual property rights.....	221
5.33	Protection of records.....	222
5.34	Privacy and protection of PII.....	223
5.35	Independent review of information security.....	224
5.36	Compliance with policies, rules and standards for information security.....	225
5.37	Documented operating procedures.....	226
<b>6</b>	<b>People controls.....</b>	<b>227</b>
6.1	Screening.....	227
6.2	Terms and conditions of employment.....	229
6.3	Information security awareness, education and training.....	230
6.4	Disciplinary process.....	231
6.5	Responsibilities after termination or change of employment.....	232
6.6	Confidentiality or non-disclosure agreements.....	233
6.7	Remote working.....	234
6.8	Information security event reporting.....	236

<b>7</b>	<b>Physical controls</b>	<b>237</b>
7.1	Physical security perimeters	237
7.2	Physical entry	237
7.3	Securing offices, rooms and facilities	239
7.4	Physical security monitoring	240
7.5	Protecting against physical and environmental threats	241
7.6	Working in secure areas	242
7.7	Clear desk and clear screen	242
7.8	Equipment siting and protection	243
7.9	Security of assets off-premises	244
7.10	Storage media	245
7.11	Supporting utilities	246
7.12	Cabling security	247
7.13	Equipment maintenance	248
7.14	Secure disposal or re-use of equipment	249
<b>8</b>	<b>Technological controls</b>	<b>250</b>
8.1	User endpoint devices	250
8.2	Privileged access rights	252
8.3	Information access restriction	253
8.4	Access to source code	255
8.5	Secure authentication	256
8.6	Capacity management	258
8.7	Protection against malware	259
8.8	Management of technical vulnerabilities	260
8.9	Configuration management	263
8.10	Information deletion	265
8.11	Data masking	267
8.12	Data leakage prevention	268
8.13	Information backup	270
8.14	Redundancy of information processing facilities	271
8.15	Logging	272
8.16	Monitoring activities	275
8.17	Clock synchronization	276
8.18	Use of privileged utility programs	277
8.19	Installation of software on operational systems	278
8.20	Networks security	279
8.21	Security of network services	280
8.22	Segregation of networks	281
8.23	Web filtering	282
8.24	Use of cryptography	283
8.25	Secure development life cycle	285
8.26	Application security requirements	286
8.27	Secure system architecture and engineering principles	288
8.28	Secure coding	290
8.29	Security testing in development and acceptance	293
8.30	Outsourced development	294
8.31	Separation of development, test and production environments	295
8.32	Change management	296
8.33	Test information	297
8.34	Protection of information systems during audit testing	298
	<b>Annex A (informative) Using attributes</b>	<b>300</b>
	<b>Annex B (informative) Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013</b>	<b>311</b>
	<b>Bibliography</b>	<b>318</b>

## European foreword (CEN) [\(FI\)](#)

The text of ISO/IEC 27002:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27002:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2023, and conflicting national standards shall be withdrawn at the latest by May 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27002:2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

### Endorsement notice

The text of ISO/IEC 27002:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27002:2022 without any modification.

## Foreword (ISO) [\(FI\)](#)

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)) or the IEC list of patent declarations received (see [patents.iec.ch](http://patents.iec.ch)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

'This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27002:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27002:2013/Cor. 1:2014 and ISO/IEC 27002:2013/Cor. 2:2015.

The main changes are as follows:

- the title has been modified;
- the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;
- some controls have been merged, some deleted and several new controls have been introduced. The complete correspondence can be found in [Annex B](#).

This corrected version of ISO/IEC 27002:2022 incorporates the following corrections:

- non-functioning hyperlinks throughout the document have been restored;
- in the introductory table in [subclause 5.22](#) and in [Table A.1](#) (row 5.22), "#information\_security\_assurance" has been moved from the column headed "Security domains" to the column headed "Operational capabilities".

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction (FI)

### 0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

### 0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

- a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;
- b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;
- c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

### 0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

### 0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

### 0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

### 0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

## 0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in [Clauses 5-8](#).

## 1 Scope [\(FI\)](#)

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;
- b) for implementing information security controls based on internationally recognized best practices;
- c) for developing organization-specific information security management guidelines.

## 2 Normative references [\(FI\)](#)

There are no normative references in this document.

## 3 Terms, definitions and abbreviated terms [\(FI\)](#)

### 3.1 Terms and definitions [\(FI\)](#)

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

#### 3.1.1

##### access control

means to ensure that physical and logical access to *assets* [\(3.1.2\)](#) is authorized and restricted based on business and information security requirements

#### 3.1.2

##### asset

anything that has value to the organization

Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:

- the primary assets:
  - information;
  - business *processes* [\(3.1.27\)](#) and activities;
- the supporting assets (on which the primary assets rely) of all types, for example:
  - hardware;
  - software;
  - network;
  - *personnel* [\(3.1.20\)](#);
  - site;
  - organization's structure.

#### 3.1.3

##### attack

successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an *asset* [\(3.1.2\)](#) or any attempt to expose, steal, or make unauthorized use of an *asset* [\(3.1.2\)](#)

### 3.1.4

#### **authentication**

provision of assurance that a claimed characteristic of an *entity* (3.1.11) is correct

### 3.1.5

#### **authenticity**

property that an *entity* (3.1.11) is what it claims to be

### 3.1.6

#### **chain of custody**

demonstrable possession, movement, handling and location of material from one point in time until another

Note 1 to entry: Material includes information and other associated *assets* (3.1.2) in the context of ISO/IEC 27002.

[SOURCE: ISO/IEC 27050-1:2019, 3.1, modified — “Note 1 to entry” added]

### 3.1.7

#### **confidential information**

information that is not intended to be made available or disclosed to unauthorized individuals, *entities* (3.1.11) or *processes* (3.1.27)

### 3.1.8

#### **control**

measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any *process* (3.1.27), *policy* (3.1.24), device, practice or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

### 3.1.9

#### **disruption**

incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization’s objectives

[SOURCE: ISO 22301:2019, 3.10]

### 3.1.10

#### **endpoint device**

network connected information and communication technology (ICT) hardware device

Note 1 to entry: Endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and Internet of things (IoT) devices.

### 3.1.11

#### **entity**

item relevant for the purpose of operation of a domain that has recognizably distinct existence

Note 1 to entry: An entity can have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

### 3.1.12

#### **information processing facility**

any information processing system, service or infrastructure, or the physical location housing it

[SOURCE: ISO/IEC 27000:2018, 3.27, modified — “facilities” has been replaced with facility.]

### 3.1.13

#### **information security breach**

compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

### 3.1.14

#### **information security event**

occurrence indicating a possible *information security breach* (3.1.13) or failure of *controls* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — “breach of information security” has been replaced with “information security breach”]

### 3.1.15

#### **information security incident**

one or multiple related and identified *information security events* (3.1.14) that can harm an organization’s *assets* (3.1.2) or compromise its operations

[SOURCE: ISO/IEC 27035-1:2016, 3.4]

### 3.1.16

#### **information security incident management**

exercise of a consistent and effective approach to the handling of *information security incidents* (3.1.15)

[SOURCE: ISO/IEC 27035-1:2016, 3.5]

### 3.1.17

#### **information system**

set of applications, services, information technology *assets* (3.1.2), or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

### 3.1.18

#### **interested party**

stakeholder

person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 27000:2018, 3.37]

### 3.1.19

#### **non-repudiation**

ability to prove the occurrence of a claimed event or action and its originating *entities* (3.1.11)

### 3.1.20

#### **personnel**

persons doing work under the organization’s direction

Note 1 to entry: The concept of personnel includes the organization’s members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.

### 3.1.21

#### **personally identifiable information**

##### **PII**

any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The “natural person” in the definition is the *PII principal* (3.1.22). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

### 3.1.22

#### **PII principal**

natural person to whom the *personally identifiable information (PII)* ([3.1.21](#)) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011, 2.11]

### 3.1.23

#### **PII processor**

privacy stakeholder that processes *personally identifiable information (PII)* ([3.1.21](#)) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

### 3.1.24

#### **policy**

intentions and direction of an organization, as formally expressed by its top management

[SOURCE: ISO/IEC 27000:2018, 3.53]

### 3.1.25

#### **privacy impact assessment**

##### **PIA**

overall *process* ([3.1.27](#)) of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information (PII)* ([3.1.21](#)), framed within an organization’s broader risk management framework

[SOURCE: ISO/IEC 29134:2017, 3.7, modified — Note 1 to entry removed.]

### 3.1.26

#### **procedure**

specified way to carry out an activity or a *process* ([3.1.27](#))

[SOURCE: ISO 30000:2009, 3.12]

### 3.1.27

#### **process**

set of interrelated or interacting activities that uses or transforms inputs to deliver a result

[SOURCE: ISO 9000:2015, 3.4.1, modified— Notes to entry removed.]

### 3.1.28

#### **record**

information created, received and maintained as evidence and as an *asset* ([3.1.2](#)) by an organization or person, in pursuit of legal obligations or in the transaction of business

Note 1 to entry: Legal obligations in this context include all legal, statutory, regulatory and contractual requirements.

[SOURCE: ISO 15489-1:2016, 3.14, modified— “Note 1 to entry” added.]

### 3.1.29

#### **recovery point objective**

##### **RPO**

point in time to which data are to be recovered after a *disruption* ([3.1.9](#)) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.12, modified — “must” replaced by “are to be”.]

### **3.1.30 recovery time objective**

**RTO**  
period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions are to be recovered after a *disruption* ([3.1.9](#)) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.13, modified — "must" replaced by "are to be".]

### **3.1.31 reliability**

property of consistent intended behaviour and results

### **3.1.32 rule**

accepted principle or instruction that states the organization's expectations on what is required to be done, what is allowed or not allowed

Note 1 to entry: Rules can be formally expressed in *topic-specific policies* ([3.1.35](#)) and in other types of documents.

### **3.1.33**

#### **sensitive information**

information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety

### **3.1.34 threat**

potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

### **3.1.35**

#### **topic-specific policy**

intentions and direction on a specific subject or topic, as formally expressed by the appropriate level of management

Note 1 to entry: Topic-specific policies can formally express *rules* ([3.1.32](#)) or organization standards.

Note 2 to entry: Some organizations use other terms for these topic-specific policies.

Note 3 to entry: The topic-specific policies referred to in this document are related to information security.

EXAMPLE Topic-specific policy on *access control* ([3.1.1](#)), topic-specific policy on clear desk and clear screen.

### **3.1.36 user**

*interested party* ([3.1.18](#)) with access to the organization's *information systems* ([3.1.17](#))

EXAMPLE *Personnel* ([3.1.20](#)), customers, suppliers.

### **3.1.37**

#### **user endpoint device**

*endpoint device* ([3.1.10](#)) used by users to access information processing services

Note 1 to entry: User endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, etc.

### **3.1.38**

#### **vulnerability**

weakness of an *asset* ([3.1.2](#)) or *control* ([3.1.8](#)) that can be exploited by one or more *threats* ([3.1.34](#))

[SOURCE: ISO/IEC 27000:2018, 3.77]

### 3.2 Abbreviated terms [\(FI\)](#)

ABAC	attribute-based access control
ACL	access control list
BIA	business impact analysis
BYOD	bring your own device
CAPTCHA	completely automated public Turing test to tell computers and humans apart
CPU	central processing unit
DAC	discretionary access control
DNS	domain name system
GPS	global positioning system
IAM	identity and access management
ICT	information and communication technology
ID	identifier
IDE	integrated development environment
IDS	intrusion detection system
IoT	internet of things
IP	internet protocol
IPS	intrusion prevention system
IT	information technology
ISMS	information security management system
MAC	mandatory access control
NTP	network time protocol
PIA	privacy impact assessment
PII	personally identifiable information
PIN	personal identification number
PKI	public key infrastructure
PTP	precision time protocol
RBAC	role-based access control
RPO	recovery point objective
RTO	recovery time objective
SAST	static application security testing

SD	secure digital
SDN	software-defined networking
SD-WAN	software-defined wide area networking
SIEM	security information and event management
SMS	short message service
SQL	structured query language
SSO	single sign on
SWID	software identification
UEBA	user and entity behaviour analytics
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
VM	virtual machine
VPN	virtual private network
WiFi	wireless fidelity

## 4 Structure of this document [\(FI\)](#)

### 4.1 Clauses [\(FI\)](#)

This document is structured as follows:

- a) Organizational controls ([Clause 5](#))
- b) People controls ([Clause 6](#))
- c) Physical controls ([Clause 7](#))
- d) Technological controls ([Clause 8](#))

There are 2 informative annexes:

- [Annex A](#) — Using attributes
- [Annex B](#) — Correspondence with ISO/IEC 27002:2013

[Annex A](#) explains how an organization can use attributes (see [4.2](#)) to create its own views based on the control attributes defined in this document or of its own creation.

[Annex B](#) shows the correspondence between the controls in this edition of ISO/IEC 27002 and the previous 2013 edition.

### 4.2 Themes and attributes [\(FI\)](#)

The categorization of controls given in [Clauses 5](#) to [8](#) are referred to as themes.

Controls are categorized as:

- a) people, if they concern individual people;
- b) physical, if they concern physical objects;
- c) technological, if they concern technology;
- d) otherwise they are categorized as organizational.

The organization can use attributes to create different views which are different categorizations of controls as seen from a different perspective to the themes. Attributes can be used to filter, sort or present controls in different views for different audiences. [Annex A](#) explains how this can be achieved and provides an example of a view.

By way of example, each control in this document has been associated with five attributes with corresponding attribute values (preceded by "#" to make them searchable), as follows:

a) Control type

Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident. Attribute values consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

b) Information security properties

Information security properties is an attribute to view controls from the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of Confidentiality, Integrity and Availability.

c) Cybersecurity concepts

Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of Identify, Protect, Detect, Respond and Recover.

d) Operational capabilities

Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of Governance, Asset\_management, Information\_protection, Human\_resource\_security, Physical\_security, System\_and\_network\_security, Application\_security, Secure\_configuration, Identity\_and\_access\_management, Threat\_and\_vulnerability\_management, Continuity, Supplier\_relationships\_security, Legal\_and\_compliance, Information\_security\_event\_management and Information\_security\_assurance.

e) Security domains

Security domains is an attribute to view controls from the perspective of four information security domains: "Governance and Ecosystem" includes "Information System Security Governance & Risk Management" and "Ecosystem cybersecurity management" (including internal and external stakeholders); "Protection" includes "IT Security Architecture", "IT Security Administration", "Identity and access management", "IT Security Maintenance" and "Physical and environmental security"; "Defence" includes "Detection" and "Computer Security Incident Management"; "Resilience" includes "Continuity of operations" and "Crisis management". Attribute values consist of Governance\_and\_Ecosystem, Protection, Defence and Resilience.

The attributes given in this document are selected because they are considered generic enough to be used by different types of organizations. Organizations can choose to disregard one or more of the attributes given in this document. They can also create attributes of their own (with the corresponding attribute values) to create their own organizational views. [Clause A.2](#) includes examples of such attributes.

#### 4.3 Control layout (FI)

The layout for each control contains the following:

- **Control title:** Short name of the control;
- **Attribute table:** A table shows the value(s) of each attribute for the given control;
- **Control:** What the control is;
- **Purpose:** Why the control should be implemented;
- **Guidance:** How the control should be implemented;
- **Other information:** Explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text. Subheadings are underlined.

### 5 Organizational controls (FI)

#### 5.1 Policies for information security (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

##### Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

##### Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

##### Guidance

At the highest level, the organization should define an “information security policy” which is approved by top management and which sets out the organization’s approach to managing its information security.

The information security policy should take into consideration requirements derived from:

- a) business strategy and requirements;
- b) regulations, legislation and contracts;
- c) the current and projected information security risks and threats.

The information security policy should contain statements concerning:

- a) definition of information security;
- b) information security objectives or the framework for setting information security objectives;
- c) principles to guide all activities relating to information security;

- d) commitment to satisfy applicable requirements related to information security;
- e) commitment to continual improvement of the information security management system;
- f) assignment of responsibilities for information security management to defined roles;
- g) procedures for handling exemptions and exceptions.

Top management should approve any changes to the information security policy.

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.

Examples of such topics include:

- a) access control;
- b) physical and environmental security;
- c) asset management;
- d) information transfer;
- e) secure configuration and handling of user endpoint devices;
- f) networking security;
- g) information security incident management;
- h) backup;
- i) cryptography and key management;
- j) information classification and handling;
- k) management of technical vulnerabilities;
- l) secure development.

The responsibility for the development, review and approval of the topic-specific policies should be allocated to relevant personnel based on their appropriate level of authority and technical competency. The review should include assessing opportunities for improvement of the organization's information security policy and topic-specific policies and managing information security in response to changes to:

- a) the organization's business strategy;
- b) the organization's technical environment;
- c) regulations, statutes, legislation and contracts;
- d) information security risks;
- e) the current and projected information security threat environment;
- f) lessons learned from information security events and incidents.

The review of information security policy and topic-specific policies should take the results of management reviews and audits into account. Review and update of other related policies should be considered when one policy is changed to maintain consistency.

The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible and understandable to the intended reader.

Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable. The organization can determine the formats and names of these policy documents that meet the organization's needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.

If the information security policy or any topic-specific policy is distributed outside the organization, care should be taken not to improperly disclose confidential information.

[Table 1](#) illustrates the differences between information security policy and topic-specific policy.

**Table 1 Differences between information security policy and topic-specific policy**

	Information security policy	Topic-specific policy
<b>Level of detail</b>	General or high-level	Specific and detailed
<b>Documented and formally approved by</b>	Top management	Appropriate level of management

#### Other information

Topic-specific policies can vary across organizations.

## 5.2 Information security roles and responsibilities [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience

#### Control

Information security roles and responsibilities should be defined and allocated according to the organization needs.

#### Purpose

To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

#### Guidance

Allocation of information security roles and responsibilities should be done in accordance with the information security policy and topic-specific policies (see [5.1](#)). The organization should define and manage responsibilities for:

- a) protection of information and other associated assets;
- b) carrying out specific information security processes;
- c) information security risk management activities and in particular acceptance of residual risks (e.g. to risk owners);
- d) all personnel using an organization's information and other associated assets.

These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Individuals with allocated information security responsibilities can assign security tasks to others. However, they remain accountable and should determine that any delegated tasks have been correctly performed.

Each security area for which individuals are responsible should be defined, documented and communicated. Authorization levels should be defined and documented. Individuals who take on a specific

information security role should be competent in the knowledge and skills required by the role and should be supported to keep up to date with developments related to the role and required in order to fulfil the responsibilities of the role.

### Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of risks and mitigating controls.

However, responsibility for resourcing and implementing the controls often remains with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

Depending on the size and resourcing of an organization, information security can be covered by dedicated roles or duties carried out in addition to existing roles.

## 5.3 Segregation of duties (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem

### Control

Conflicting duties and conflicting areas of responsibility should be segregated.

### Purpose

To reduce the risk of fraud, error and bypassing of information security controls.

### Guidance

Segregation of duties and areas of responsibility aims to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own.

The organization should determine which duties and areas of responsibility need to be segregated. The following are examples of activities that can require segregation:

- a) initiating, approving and executing a change;
- b) requesting, approving and implementing access rights;
- c) designing, implementing and reviewing code;
- d) developing software and administering production systems;
- e) using and administering applications;
- f) using applications and administering databases;
- g) designing, auditing and assuring information security controls.

The possibility of collusion should be considered in designing the segregation controls. Small organizations can find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls should be considered, such as monitoring of activities, audit trails and management supervision.

Care should be taken when using role-based access control systems to ensure that persons are not granted conflicting roles. When there is a large number of roles, the organization should consider using automated

tools to identify conflicts and facilitate their removal. Roles should be carefully defined and provisioned to minimize access problems if a role is removed or reassigned.

## Other information

No other information.

### 5.4 Management responsibilities (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

#### Control

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

#### Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

#### Guidance

Management should demonstrate support of the information security policy, topic-specific policies, procedures and information security controls.

Management responsibilities should include ensuring that personnel:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets;
- b) are provided with guidelines which state the information security expectations of their role within the organization;
- c) are mandated to fulfil the information security policy and topic-specific policies of the organization;
- d) achieve a level of awareness of information security relevant to their roles and responsibilities within the organization (see [6.3](#));
- e) compliance with the terms and conditions of employment, contract or agreement, including the organization's information security policy and appropriate methods of working;
- f) continue to have the appropriate information security skills and qualifications through ongoing professional education;
- g) where practicable, are provided with a confidential channel for reporting violations of information security policy, topic-specific policies or procedures for information security ("whistleblowing"). This can allow for anonymous reporting, or have provisions to ensure that knowledge of the identity of the reporter is known only to those who need to deal with such reports;
- h) are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.

#### Other information

No other information.

## 5.5 Contact with authorities (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Identify #Protect	#Governance	#Defence
#Corrective	#Integrity #Availability	#Respond #Recover		#Resilience

### Control

The organization should establish and maintain contact with relevant authorities.

### Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

### Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

### Other information

Organizations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be a requirement to support information security incident management (see [5.24](#) to [5.28](#)) or the contingency planning and business continuity processes (see [5.29](#) and [5.30](#)). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment)].

## 5.6 Contact with special interest groups (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect #Respond	#Governance	#Defence
#Corrective	#Integrity #Availability	#Recover		

### Control

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

### Purpose

To ensure appropriate flow of information takes place with respect to information security.

### Guidance

Membership of special interest groups or forums should be considered as a means to:

- a) improve knowledge about best practices and stay up to date with relevant security information;
- b) ensure the understanding of the information security environment is current;

- c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
- d) gain access to specialist information security advice;
- e) share and exchange information about new technologies, products, services, threats or vulnerabilities;
- f) provide suitable liaison points when dealing with information security incidents (see [5.24](#) to [5.28](#)).

## Other information

No other information.

## 5.7 Threat intelligence (EI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Identify	#Threat_and_vulnerability_management	#Defence
#Detective	#Integrity	#Detect		#Resilience
#Corrective	#Availability	#Respond		

### Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

### Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

### Guidance

Information about existing or emerging threats is collected and analysed in order to:

- a) facilitate informed actions to prevent the threats from causing harm to the organization;
- b) reduce the impact of such threats.

Threat intelligence can be divided into three layers, which should all be considered:

- a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks);
- b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved;
- c) operational threat intelligence: details about specific attacks, including technical indicators.

Threat intelligence should be:

- a) relevant (i.e. related to the protection of the organization);
- b) insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);
- c) contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);
- d) actionable (i.e. the organization can act on information quickly and effectively).

Threat intelligence activities should include:

- a) establishing objectives for threat intelligence production;
- b) identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence;
- c) collecting information from selected sources, which can be internal and external;
- d) processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information);
- e) analysing information to understand how it relates and is meaningful to the organization;
- f) communicating and sharing it to relevant individuals in a format that can be understood.

Threat intelligence should be analysed and later used:

- a) by implementing processes to include information gathered from threat intelligence sources into the organization's information security risk management processes;
- b) as additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions;
- c) as input to the information security test processes and techniques.

The organization should share threat intelligence with other organizations on a mutual basis in order to improve overall threat intelligence.

## Other information

Organizations can use threat intelligence to prevent, detect, or respond to threats. Organizations can produce threat intelligence, but more typically receive and make use of threat intelligence produced by other sources.

Threat intelligence is often provided by independent providers or advisors, government agencies or collaborative threat intelligence groups.

The effectiveness of controls such as [5.25](#), [8.7](#), [8.16](#) or [8.23](#), depends on the quality of available threat intelligence.

## 5.8 Information security in project management (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection

### Control

Information security should be integrated into project management.

### Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.

### Guidance

Information security should be integrated into project management to ensure information security risks are addressed as part of the project management. This can be applied to any type of project regardless of

its complexity, size, duration, discipline or application area (e.g. a project for a core business process, ICT, facility management or other supporting processes).

The project management in use should require that:

- a) information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle;
- b) information security requirements [e.g. application security requirements ([8.26](#)), requirements for complying with intellectual property rights ([5.32](#)), etc.] are addressed in the early stages of projects;
- c) information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle;
- d) progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested.

The appropriateness of the information security considerations and activities should be followed up at predefined stages by suitable persons or governance bodies, such as the project steering committee.

Responsibilities and authorities for information security relevant to the project should be defined and allocated to specified roles.

Information security requirements for products or services to be delivered by the project should be determined using various methods, including deriving compliance requirements from information security policy, topic-specific policies and regulations. Further information security requirements can be derived from activities such as threat modelling, incident reviews, use of vulnerability thresholds or contingency planning, thus ensuring that the architecture and design of information systems are protected against known threats based on the operational environment.

Information security requirements should be determined for all types of projects, not only ICT development projects. The following should also be considered when determining these requirements:

- a) what information is involved (information determination), what are the corresponding information security needs (classification; see [5.12](#)) and the potential negative business impact which can result from lack of adequate security;
- b) the required protection needs of information and other associated assets involved, particularly in terms of confidentiality, integrity and availability;
- c) the level of confidence or assurance required towards the claimed identity of entities in order to derive the authentication requirements;
- d) access provisioning and authorization processes, for customers and other potential business users as well as for privileged or technical users such as relevant project members, potential operation staff or external suppliers;
- e) informing users of their duties and responsibilities;
- f) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;
- g) requirements mandated by other information security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
- h) compliance with the legal, statutory, regulatory and contractual environment in which the organization operates;
- i) level of confidence or assurance required for third parties to meet the organization's information security policy and topic-specific policies including relevant security clauses in any agreements or contracts.

## Other information

The project development approach, such as waterfall life cycle or agile life cycle, should support information security in a structured way that can be adapted to suit the assessed severity of the information security risks, based on the character of the project. Early consideration of information security requirements for the product or service (e.g. at the planning and design stages), can lead to more effective and cost-efficient solutions for quality and information security. ISO 21500 and ISO 21502 provide guidance on concepts and processes of project management that are important for the performance of projects.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

## 5.9 Inventory of information and other associated assets [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

### Control

An inventory of information and other associated assets, including owners, should be developed and maintained.

### Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

### Guidance

#### Inventory

The organization should identify its information and other associated assets and determine their importance in terms of information security. Documentation should be maintained in dedicated or existing inventories as appropriate.

The inventory of information and other associated assets should be accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information and other associated assets include:

- a) conducting regular reviews of identified information and other associated assets against the asset inventory;
- b) automatically enforcing an inventory update in the process of installing, changing or removing an asset.

The location of an asset should be included in the inventory as appropriate.

The inventory does not need to be a single list of information and other associated assets. Considering that the inventory should be maintained by the relevant functions, it can be seen as a set of dynamic inventories, such as inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competence, capabilities and records.

Each asset should be classified in accordance with the classification of the information (see [5.12](#)) associated to that asset.

The granularity of the inventory of information and other associated assets should be at a level appropriate for the needs of the organization. Sometimes specific instances of assets in the information life cycle are not feasible to be documented due to the nature of the asset. An example of a short-lived asset is a VM instance whose life cycle can be of short duration.

## Ownership

For the identified information and other associated assets, ownership of the asset should be assigned to an individual or a group and the classification should be identified (see [5.12](#), [5.13](#)). A process to ensure timely assignment of asset ownership should be implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. Asset ownership should be reassigned as necessary when current asset owners leave or change job roles.

## Owner duties

The asset owner should be responsible for the proper management of an asset over the whole asset life cycle, ensuring that:

- a) information and other associated assets are inventoried;
- b) information and other associated assets are appropriately classified and protected;
- c) the classification is reviewed periodically;
- d) components supporting technology assets are listed and linked, such as database, storage, software components and sub-components;
- e) requirements for the acceptable use of information and other associated assets (see [5.10](#)) are established;
- f) access restrictions correspond with the classification and that they are effective and are reviewed periodically;
- g) information and other associated assets, when deleted or disposed, are handled in a secure manner and removed from the inventory;
- h) they are involved in the identification and management of risks associated with their asset(s);
- i) they support personnel who have the roles and responsibilities of managing their information.

## **Other information**

Inventories of information and other associated assets are often necessary to ensure the effective protection of information and can be required for other purposes, such as health and safety, insurance or financial reasons. Inventories of information and other associated assets also support risk management, audit activities, vulnerability management, incident response and recovery planning.

Tasks and responsibilities can be delegated (e.g. to a custodian looking after the assets on a daily basis), but the person or group who delegated them remains accountable.

It can be useful to designate groups of information and other associated assets which act together to provide a particular service. In this case, the owner of this service is accountable for the delivery of the service, including the operation of its assets.

See ISO/IEC 19770-1 for additional information on information technology (IT) asset management. See ISO 55001 for additional information on asset management.

## **5.10 Acceptable use of information and other associated assets ([FI](#))**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Eco-system #Protection

## Control

Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

## Purpose

To ensure information and other associated assets are appropriately protected, used and handled.

## Guidance

Personnel and external party users using or having access to the organization's information and other associated assets should be made aware of the information security requirements for protecting and handling the organization's information and other associated assets. They should be responsible for their use of any information processing facilities.

The organization should establish a topic-specific policy on the acceptable use of information and other associated assets and communicate it to anyone who uses or handles information and other associated assets. The topic-specific policy on acceptable use should provide clear direction on how individuals are expected to use information and other associated assets. The topic-specific policy should state:

- a) expected and unacceptable behaviours of individuals from an information security perspective;
- b) permitted and prohibited use of information and other associated assets;
- c) monitoring activities being performed by the organization.

Acceptable use procedures should be drawn up for the full information life cycle in accordance with its classification (see [5.12](#)) and determined risks. The following items should be considered:

- a) access restrictions supporting the protection requirements for each level of classification;
- b) maintenance of a record of the authorized users of information and other associated assets;
- c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- d) storage of assets associated with information in accordance with manufacturers' specifications (see [7.8](#));
- e) clear marking of all copies of storage media (electronic or physical) for the attention of the authorized recipient (see [7.10](#));
- f) authorization of disposal of information and other associated assets and supported deletion method(s) (see [8.10](#)).

## Other information

It can be the case that the assets concerned do not directly belong to the organization, such as public cloud services. The use of such third-party assets and any assets of the organization associated with such external assets (e.g. information, software) should be identified as applicable and controlled, for example, through agreements with cloud service providers. Care should also be taken when a collaborative working environment is used.

## 5.11 Return of assets (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

## Control

Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

## Purpose

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

## Guidance

The change or termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where personnel and other interested parties purchase the organization's equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment (see [7.14](#)).

In cases where personnel and other interested parties have knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period and thereafter, the organization should prevent unauthorized copying of relevant information (e.g. intellectual property) by personnel under notice of termination.

The organization should clearly identify and document all information and other associated assets to be returned which can include:

- a) user endpoint devices;
- b) portable storage devices;
- c) specialist equipment;
- d) authentication hardware (e.g. mechanical keys, physical tokens and smartcards) for information systems, sites and physical archives;
- e) physical copies of information.

## Other information

It can be difficult to return information held on assets which are not owned by the organization. In such cases, it is necessary to restrict the use of information using other information security controls such as access rights management ([5.18](#)) or use of cryptography ([8.24](#)).

## 5.12 Classification of information [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

## Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

## Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

## Guidance

The organization should establish a topic-specific policy on information classification and communicate it to all relevant interested parties.

The organization should take into account requirements for confidentiality, integrity and availability in the classification scheme.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, for protecting integrity of information and for assuring availability, as well as legal requirements concerning the confidentiality, integrity or availability of the information. Assets other than information can also be classified in compliance with classification of information, which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. Results of classification should be updated in accordance with changes of the value, sensitivity and criticality of information through their life cycle.

The scheme should be aligned to the topic-specific policy on access control (see [5.1](#)) and should be able to address specific business needs of the organization.

The classification can be determined by the level of impact that the information's compromise would have for the organization. Each level defined in the scheme should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization and included in its procedures so that everyone classifies information and applicable other associated assets in the same way. In this manner, everyone has a common understanding of protection requirements and applies appropriate protection.

The classification scheme used within the organization can be different from the schemes used by other organizations, even if the names for levels are similar. In addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical. Therefore, agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification levels from other organizations. Correspondence between different schemes can be determined by looking for equivalence in the associated handling and protection methods.

## Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time. For example, when the information has been made public, it no longer has confidentiality requirements but can still require protection for its integrity and availability properties. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or, on the contrary, under-classification can lead to insufficient controls to protect the information from compromise.

As an example, an information confidentiality classification scheme can be based on four levels as follows:

- a) disclosure causes no harm;
- b) disclosure causes minor reputational damage or minor operational impact;
- c) disclosure has a significant short-term impact on operations or business objectives;
- d) disclosure has a serious impact on long term business objectives or puts the survival of the organization at risk.

## 5.13 Labelling of information (E1)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_protection	#Defence #Protection

### Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

### Purpose

To facilitate the communication of classification of information and support automation of information processing and management.

### Guidance

Procedures for information labelling should cover information and other associated assets in all formats. The labelling should reflect the classification scheme established in [5.12](#). The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of storage media. The procedures can define:

- a) cases where labelling is omitted (e.g. labelling of non-confidential information to reduce workloads);
- b) how to label information sent by or stored on electronic or physical means, or any other format;
- c) how to handle cases where labelling is not possible (e.g. due to technical restrictions).

Examples of labelling techniques include:

- a) physical labels;
- b) headers and footers;
- c) metadata;
- d) watermarking;
- e) rubber-stamps.

Digital information should utilize metadata in order to identify, manage and control information, especially with regard to confidentiality. Metadata should also enable efficient and correct searching for information. Metadata should facilitate systems to interact and make decisions based on the associated classification labels.

The procedures should describe how to attach metadata to information, what labels to use and how data should be handled, in line with the organization's information model and ICT architecture.

Relevant additional metadata should be added by systems when they process information depending on its information security properties.

Personnel and other interested parties should be made aware of labelling procedures. All personnel should be provided with the necessary training to ensure that information is correctly labelled and handled accordingly.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

## Other information

Labelling of classified information is a key requirement for information sharing.

Other useful metadata that can be attached to the information is which organizational process created the information and at what time.

Labelling of information and other associated assets can sometimes have negative effects. Classified assets can be easier to identify by malicious actors for potential misuse.

Some systems do not label individual files or database records with their classification but protect all information at the highest level of classification of any of the information that it contains or is permitted to contain. It is usual in such systems to determine and then label information when it is exported.

## 5.14 Information transfer (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

### Control

Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

### Purpose

To maintain the security of information transferred within an organization and with any external interested party.

### Guidance

#### General

The organization should establish and communicate a topic-specific policy on information transfer to all relevant interested parties. Rules, procedures and agreements to protect information in transit should reflect the classification of the information involved. Where information is transferred between the organization and third parties, transfer agreements (including recipient authentication) should be established and maintained to protect information in all forms in transit (see [5.10](#)).

Information transfer can happen through electronic transfer, physical storage media transfer and verbal transfer.

For all types of information transfer, rules, procedures and agreements should include:

- a) controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the classification of the information involved and any special controls that are required to protect sensitive information, such as use of cryptographic techniques (see [8.24](#));
- b) controls to ensure traceability and non-repudiation, including maintaining a chain of custody for information while in transit;
- c) identification of appropriate contacts related to the transfer including information owners, risk owners, security officers and information custodians, as applicable;
- d) responsibilities and liabilities in the event of information security incidents, such as loss of physical storage media or data;
- e) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see [5.13](#));

- f) reliability and availability of the transfer service;
- g) the topic-specific policy or guidelines on acceptable use of information transfer facilities (see [5.10](#));
- h) retention and disposal guidelines for all business records, including messages;

NOTE Local legislation and regulations can exist regarding retention and disposal of business records.

- i) the consideration of any other relevant legal, statutory, regulatory and contractual requirements (see [5.31](#), [5.32](#), [5.33](#), [5.34](#)) related to transfer of information (e.g. requirements for electronic signatures).

### Electronic transfer

Rules, procedures and agreements should also consider the following items when using electronic communication facilities for information transfer:

- a) detection of and protection against malware that can be transmitted through the use of electronic communications (see [8.7](#));
- b) protection of communicated sensitive electronic information that is in the form of an attachment;
- c) prevention against sending documents and messages in communications to the wrong address or number;
- d) obtaining approval prior to using external public services such as instant messaging, social networking, file sharing or cloud storage;
- e) stronger levels of authentication when transferring information via publicly accessible networks;
- f) restrictions associated with electronic communication facilities (e.g. preventing automatic forwarding of electronic mail to external mail addresses);
- g) advising personnel and other interested parties not to send short message service (SMS) or instant messages with critical information since these can be read in public places (and therefore by unauthorized persons) or stored in devices not adequately protected;
- h) advising personnel and other interested parties about the problems of using fax machines or services, namely:
  - 1) unauthorized access to built-in message stores to retrieve messages;
  - 2) deliberate or accidental programming of machines to send messages to specific numbers.

### Physical storage media transfer

When transferring physical storage media (including paper), rules, procedures and agreements should also include:

- a) responsibilities for controlling and notifying transmission, dispatch and receipt;
- b) ensuring correct addressing and transportation of the message;
- c) packaging that protects the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that can reduce the effectiveness of restoring storage media such as exposure to heat, moisture or electromagnetic fields; using minimum technical standards for packaging and transmission (e.g. the use of opaque envelopes);
- d) a list of authorized reliable couriers agreed by management;
- e) courier identification standards;
- f) depending on the classification level of the information in the storage media to be transported, use tamper evident or tamper-resistant controls (e.g. bags, containers);

- g) procedures to verify the identification of couriers;
- h) approved list of third parties providing transportation or courier services depending on the classification of the information;
- i) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination.

#### Verbal transfer

To protect verbal transfer of information, personnel and other interested parties should be reminded that they should:

- a) not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorized persons;
- b) not leave messages containing confidential information on answering machines or voice messages since these can be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;
- c) be screened to the appropriate level to listen to the conversation;
- d) ensure that appropriate room controls are implemented (e.g. sound-proofing, closed door);
- e) begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.

#### **Other information**

No other information.

### **5.15 Access control (FI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

#### **Control**

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

#### **Purpose**

To ensure authorized access and to prevent unauthorized access to information and other associated assets.

#### **Guidance**

Owners of information and other associated assets should determine information security and business requirements related to access control. A topic-specific policy on access control should be defined which takes account of these requirements and should be communicated to all relevant interested parties.

These requirements and the topic-specific policy should consider the following:

- a) determining which entities require which type of access to the information and other associated assets;
- b) security of applications (see [8.26](#));
- c) physical access, which needs to be supported by appropriate physical entry controls (see [7.2](#), [7.3](#), [7.4](#));

- d) information dissemination and authorization (e.g. the need-to-know principle) and information security levels and classification of information (see [5.10](#), [5.12](#), [5.13](#));
- e) restrictions to privileged access (see [8.2](#));
- f) segregation of duties (see [5.3](#));
- g) relevant legislation, regulations and any contractual obligations regarding limitation of access to data or services (see [5.31](#), [5.32](#), [5.33](#), [5.34](#), [8.3](#));
- h) segregation of access control functions (e.g. access request, access authorization, access administration);
- i) formal authorization of access requests (see [5.16](#) and [5.18](#));
- j) the management of access rights (see [5.18](#));
- k) logging (see [8.15](#)).

Access control rules should be implemented by defining and mapping appropriate access rights and restrictions to the relevant entities (see [5.16](#)). An entity can represent a human user as well as a technical or logical item (e.g. a machine, device or a service). To simplify the access control management, specific roles can be assigned to entity groups.

The following should be taken into account when defining and implementing access control rules:

- a) consistency between the access rights and information classification;
- b) consistency between the access rights and the physical perimeter security needs and requirements;
- c) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use;
- d) considering how elements or factors relevant to dynamic access control can be reflected.

## Other information

There are often overarching principles used in the context of access control. Two of the most frequently used principles are:

- a) need-to-know: an entity is only granted access to the information which that entity requires in order to perform its tasks (different tasks or roles mean different need-to-know information and hence different access profiles);
- b) need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.

Care should be taken when specifying access control rules to consider:

- a) establishing rules based on the premise of least privilege, "Everything is generally forbidden unless expressly permitted", rather than the weaker rule, "Everything is generally permitted unless expressly forbidden";
- b) changes in information labels (see [5.13](#)) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
- c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
- d) when to define and regularly review the approval.

Access control rules should be supported by documented procedures (see [5.16](#), [5.17](#), [5.18](#), [8.2](#), [8.3](#), [8.4](#), [8.5](#), [8.18](#)) and defined responsibilities (see [5.2](#), [5.17](#)).

There are several ways to implement access control, such as MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control) and ABAC (attribute-based access control).

Access control rules can also contain dynamic elements (e.g. a function that evaluates past accesses or specific environment values). Access control rules can be implemented in different granularity, ranging from covering whole networks or systems to specific data fields and can also consider properties such as user location or the type of network connection that is used for access. These principles and how granular access control is defined can have a significant cost impact. Stronger rules and more granularity typically lead to higher cost. Business requirements and risk considerations should be used to define which access control rules are applied and which granularity is required.

## 5.16 Identity management (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

### Control

The full life cycle of identities should be managed.

### Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

### Guidance

The processes used in the context of identity management should ensure that:

- a) for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity;
- b) identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval and documentation;
- c) identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight;
- d) identities are disabled or removed in a timely fashion if they are no longer required (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the organization or changed the role);
- e) in a specific domain, a single identity is mapped to a single entity, [i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided];
- f) records of all significant events concerning the use and management of user identities and of authentication information are kept.

The organization should have a supporting process in place to handle changes to information related to user identities. These processes can include re-verification of trusted documents related to a person.

When using identities provided or issued by third parties (e.g. social media credentials), the organization should ensure the third-party identities provide the required trust level and any associated risks are known and sufficiently treated. This can include controls related to the third parties (see [5.19](#)) as well as controls related to associated authentication information (see [5.17](#)).

## Other information

Providing or revoking access to information and other associated assets is usually a multi-step procedure:

- a) confirming the business requirements for an identity to be established;
- b) verifying the identity of an entity before allocating them a logical identity;
- c) establishing an identity;
- d) configuring and activating the identity. This also includes configuration and initial setup of related authentication services;
- e) providing or revoking specific access rights to the identity, based on appropriate authorization or entitlement decisions (see [5.18](#)).

## 5.17 Authentication information ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

### Control

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

### Purpose

To ensure proper entity authentication and prevent failures of authentication processes.

### Guidance

#### Allocation of authentication information

The allocation and management process should ensure that:

- a) personal passwords or personal identification numbers (PINs) generated automatically during enrolment processes as temporary secret authentication information are non-guessable and unique for each person, and that users are required to change them after the first use;
- b) procedures are established to verify the identity of a user prior to providing new, replacement or temporary authentication information;
- c) authentication information, including temporary authentication information, is transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected (clear text) electronic mail messages for this purpose is avoided;
- d) users acknowledge receipt of authentication information;
- e) default authentication information as predefined or provided by vendors is changed immediately following installation of systems or software;
- f) records of significant events concerning allocation and management of authentication information are kept and their confidentiality is granted, and that the record-keeping method is approved (e.g. by using an approved password vault tool).

## User responsibilities

Any person having access to or using authentication information should be advised to ensure that:

- a) secret authentication information such as passwords are kept confidential. Personal secret authentication information is not to be shared with anyone. Secret authentication information used in the context of identities linked to multiple users or linked to non-personal entities are solely shared with authorized persons;
- b) affected or compromised authentication information is changed immediately upon notification of or any other indication of a compromise;
- c) when passwords are used as authentication information, strong passwords according to best practice recommendations are selected, for example:
  - 1) passwords are not based on anything somebody else can easily guess or obtain using person-related information (e.g. names, telephone numbers and dates of birth);
  - 2) passwords are not based on dictionary words or combinations thereof;
  - 3) use easy to remember passphrases and try to include alphanumerical and special characters;
  - 4) passwords have a minimum length;
- d) the same passwords are not used across distinct services and systems;
- e) the obligation to follow these rules is also included in terms and conditions of employment (see [6.2](#)).

## Password management system

When passwords are used as authentication information, the password management system should:

- a) allow users to select and change their own passwords and include a confirmation procedure to address input errors;
- b) enforce strong passwords according to good practice recommendations [see c) of "User responsibilities"];
- c) force users to change their passwords at first login;
- d) enforce password changes as necessary, for example after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);
- e) prevent re-use of previous passwords;
- f) prevent the use of commonly-used passwords and compromised usernames, password combinations from hacked systems;
- g) not display passwords on the screen when being entered;
- h) store and transmit passwords in protected form.

Password encryption and hashing should be performed according to approved cryptographic techniques for passwords (see [8.24](#)).

## **Other information**

Passwords or passphrases are a commonly used type of authentication information and are a common means of verifying a user's identity. Other types of authentication information are cryptographic keys, data stored on hardware tokens (e.g. smart cards) that produce authentication codes and biometric data such as iris scans or fingerprints. Additional information can be found in the ISO/IEC 24760 series.

Requiring frequent change of passwords can be problematic because users can get annoyed by the frequent changes, forget new passwords, note them down in unsafe places, or choose unsafe passwords. Provision of

single sign on (SSO) or other authentication management tools (e.g. password vaults) reduces the amount of authentication information that users are required to protect and can thereby increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of authentication information.

Some applications require user passwords to be assigned by an independent authority. In such cases, a), c) and d) of "Password management system" do not apply.

## 5.18 Access rights [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

### Control

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

### Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

### Guidance

#### Provision and revocation of access rights

The provisioning process for assigning or revoking physical and logical access rights granted to an entity's authenticated identity should include:

- a) obtaining authorization from the owner of the information and other associated assets for the use of the information and other associated assets (see [5.9](#)). Separate approval for access rights by management can also be appropriate;
- b) considering the business requirements and the organization's topic-specific policy and rules on access control;
- c) considering segregation of duties, including segregating the roles of approval and implementation of the access rights and separation of conflicting roles;
- d) ensuring access rights are removed when someone does not need to access the information and other associated assets, in particular ensuring access rights of users who have left the organization are removed in a timely fashion;
- e) considering giving temporary access rights for a limited time period and revoking them at the expiration date, in particular for temporary personnel or temporary access required by personnel;
- f) verifying that the level of access granted is in accordance with the topic-specific policies on access control (see [5.15](#)) and is consistent with other information security requirements such as segregation of duties (see [5.3](#));
- g) ensuring that access rights are activated (e.g. by service providers) only after authorization procedures are successfully completed;
- h) maintaining a central record of access rights granted to a user identifier (ID, logical or physical) to access information and other associated assets;
- i) modifying access rights of users who have changed roles or jobs;

- j) removing or adjusting physical and logical access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions;
- k) maintaining a record of changes to users' logical and physical access rights.

#### Review of access rights

Regular reviews of physical and logical access rights should consider the following:

- a) users' access rights after any change within the same organization (e.g. job change, promotion, demotion) or termination of employment (see [6.1](#) to [6.5](#));
- b) authorizations for privileged access rights.

#### Consideration before change or termination of employment

A user's access rights to information and other associated assets should be reviewed and adjusted or removed before any change or termination of employment based on the evaluation of risk factors such as:

- a) whether the termination or change is initiated by the user or by management and the reason for termination;
- b) the current responsibilities of the user;
- c) the value of the assets currently accessible.

#### **Other information**

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews of access rights are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel (see [5.20](#), [6.2](#), [6.4](#), [6.6](#)).

In cases of management-initiated termination, disgruntled personnel or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they can be tempted to collect information for future use.

Cloning is an efficient way for organizations to assign access to users. However, it should be done with care based on distinct roles identified by the organization rather than just cloning an identity with all associated access rights. Cloning has an inherent risk of resulting in excessive access rights to information and other associated assets.

### **5.19 Information security in supplier relationships (EI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

#### **Control**

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

#### **Purpose**

To maintain an agreed level of information security in supplier relationships.

## Guidance

The organization should establish and communicate a topic-specific policy on supplier relationships to all relevant interested parties.

The organization should identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers. This should also apply to the organization's use of resources of cloud service providers. These processes and procedures should include those to be implemented by the organization, as well as those the organization requires the supplier to implement for the commencement of use of a supplier's products or services or for the termination of use of a supplier's products and services, such as:

- a) identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;
- b) establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, on-site assessments, certifications);
- c) evaluating and selecting supplier's products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier's information and information processing and hence the organization's information security;
- d) defining the organization's information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;
- e) defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information;
- f) assessing and managing the information security risks associated with:
  - 1) the suppliers' use of the organization's information and other associated assets, including risks originating from potential malicious supplier personnel;
  - 2) malfunctioning or vulnerabilities of the products (including software components and sub-components used in these products) or services provided by the suppliers;
- g) monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;
- h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by other means;
- i) handling incidents and contingencies associated with supplier products and services including responsibilities of both the organization and suppliers;
- j) resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier's information and information processing and hence the availability of the organization's information;
- k) awareness and training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement, topic-specific policies, processes and procedures and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
- l) managing the necessary transfer of information, other associated assets and anything else that needs to be changed and ensuring that information security is maintained throughout the transfer period;

- m) requirements to ensure a secure termination of the supplier relationship, including:
- 1) de-provisioning of access rights;
  - 2) information handling;
  - 3) determining ownership of intellectual property developed during the engagement;
  - 4) information portability in case of change of supplier or insourcing;
  - 5) records management;
  - 6) return of assets;
  - 7) secure disposal of information and other associated assets;
  - 8) ongoing confidentiality requirements;
- n) level of personnel security and physical security expected from supplier's personnel and facilities.

The procedures for continuing information processing in the event that the supplier becomes unable to supply its products or services (e.g. because of an incident, because the supplier is no longer in business, or no longer provides some components due to technology advancements) should be considered to avoid any delay in arranging replacement products or services (e.g. identifying an alternative supplier in advance or always using alternative suppliers).

### Other information

In cases where it is not possible for an organization to place requirements on a supplier, the organization should:

- a) consider the guidance given in this control in making decisions about choosing a supplier and its product or service;
- b) implement compensating controls as necessary based on a risk assessment.

Information can be put at risk by suppliers with inadequate information security management. Controls should be determined and applied to manage the supplier's access to information and other associated assets. For example, if there is a special need for confidentiality of the information, non-disclosure agreements or cryptographic techniques can be used. Another example is personal data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

Risks can also be caused by inadequate controls of ICT infrastructure components or services provided by suppliers. Malfunctioning or vulnerable components or services can cause information security breaches in the organization or to another entity (e.g. they can cause malware infection, attacks or other harm on entities other than the organization).

See ISO/IEC 27036-2 for more detail.

## 5.20 Addressing information security within supplier agreements (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

### Control

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

## Purpose

To maintain an agreed level of information security in supplier relationships.

## Guidance

Supplier agreements should be established and documented to ensure that there is clear understanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms can be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

- a) description of the information to be provided or accessed and methods of providing or accessing the information;
- b) classification of information according to the organization's classification scheme (see [5.10](#), [5.12](#), [5.13](#));
- c) mapping between the organization's own classification scheme and the classification scheme of the supplier;
- d) legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;
- e) obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting and auditing, and the supplier's obligations to comply with the organization's information security requirements;
- f) rules of acceptable use of information and other associated assets, including unacceptable use if necessary;
- g) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel (e.g. through an explicit list of supplier personnel authorized to use the organization's information and other associated assets);
- h) information security requirements regarding the supplier's ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and risk criteria;
- i) indemnities and remediation for failure of contractor to meet requirements;
- j) incident management requirements and procedures (especially notification and collaboration during incident remediation);
- k) training and awareness requirements for specific procedures and information security requirements (e.g. for incident response, authorization procedures);
- l) relevant provisions for sub-contracting, including the controls that need to be implemented, such as agreement on the use of sub-suppliers (e.g. requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change);
- m) relevant contacts, including a contact person for information security issues;
- n) any screening requirements, where legally permissible, for the supplier's personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;
- o) the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls;
- p) right to audit the supplier processes and controls related to the agreement;

- q) supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
- r) defect resolution and conflict resolution processes;
- s) providing backup aligned with the organization's needs (in terms of frequency and type and storage location);
- t) ensuring the availability of an alternate facility (i.e. disaster recovery site) not subject to the same threats as the primary facility and considerations for fall back controls (alternate controls) in the event primary controls fail;
- u) having a change management process that ensures advance notification to the organization and the possibility for the organization of not accepting changes;
- v) physical security controls commensurate with the information classification;
- w) information transfer controls to protect the information during physical transfer or logical transmission;
- x) termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;
- y) provision of a method of securely destroying the organization's information stored by the supplier as soon as it is no longer required;
- z) ensuring, at the end of the contract, handover support to another supplier or to the organization itself.

The organization should establish and maintain a register of agreements with external parties (e.g. contracts, memorandum of understanding, information-sharing agreements) to keep track of where their information is going. The organization should also regularly review, validate and update their agreements with external parties to ensure they are still required and fit for purpose with relevant information security clauses.

### Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant requirements for addressing information security risks.

For details on supplier agreements, see ISO/IEC 27036 series. For cloud service agreements, see ISO/IEC 19086 series.

## 5.21 Managing information security in the ICT supply chain [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

### Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

### Purpose

To maintain an agreed level of information security in supplier relationships.

## Guidance

The following topics should be considered to address information security within ICT supply chain security in addition to the general information security requirements for supplier relationships:

- a) defining information security requirements to apply to ICT product or service acquisition;
- b) requiring that ICT services suppliers propagate the organization's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the organization;
- c) requiring that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities (e.g. sub-contracted software developers and hardware component providers);
- d) requesting that ICT products suppliers provide information describing the software components used in products;
- e) requesting that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation;
- f) implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements. Examples of such supplier review methods can include penetration testing and proof or validation of third-party attestations for the supplier's information security operations;
- g) implementing a process for identifying and documenting product or service components that are critical for maintaining functionality and therefore require increased attention, scrutiny and further follow up required when built outside of the organization especially if the supplier outsources aspects of product or service components to other suppliers;
- h) obtaining assurance that critical components and their origin can be traced throughout the supply chain;
- i) obtaining assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features;
- j) implementing processes to ensure that components from suppliers are genuine and unaltered from their specification. Example measures include anti-tamper labels, cryptographic hash verifications or digital signatures. Monitoring for out of specification performance can be an indicator of tampering or counterfeits. Prevention and detection of tampering should be implemented during multiple stages in the system development life cycle, including design, development, integration, operations and maintenance;
- k) obtaining assurance that ICT products achieve required security levels, for example, through formal certification or an evaluation scheme such as the Common Criteria Recognition Arrangement;
- l) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;
- m) implementing specific processes for managing ICT component life cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements. Identification of an alternative supplier and the process to transfer software and competence to the alternative supplier should be considered.

## Other information

The specific ICT supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the ICT supply chain and any matters that have an important effect on the products and services being provided. The organization can influence ICT

supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the ICT supply chain.

ICT should be acquired from reputable sources. The reliability of software and hardware is a matter of quality control. While it is generally not possible for an organization to inspect the quality control systems of its vendors, it can make reliable judgments based on the reputation of the vendor.

ICT supply chain as addressed here includes cloud services.

Examples of ICT supply chains are:

- a) cloud services provisioning, where the cloud service provider relies on the software developers, telecommunication service providers, hardware providers;
- b) IoT, where the service involves the device manufacturers, the cloud service providers (e.g. the IoT platform operators), the developers for mobile and web applications, the vendor of software libraries;
- c) hosting services, where the provider relies on external service desks including first, second and third support levels.

See ISO/IEC 27036-3 for more details including risk assessment guidance.

Software identification (SWID) tags can also help to achieve better information security in the supply chain, by providing information about software provenance. See ISO/IEC 19770-2 for more details.

## 5.22 Monitoring, review and change management of supplier services [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence

### Control

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

### Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements.

### Guidance

Monitoring, review and change management of supplier services should ensure the information security terms and conditions of the agreements are complied with, information security incidents and problems are managed properly and changes in supplier services or business status do not affect service delivery.

This should involve a process to manage the relationship between the organization and the supplier to:

- a) monitor service performance levels to verify compliance with the agreements;
- b) monitor changes made by suppliers including:
  - 1) enhancements to the current services offered;
  - 2) development of any new applications and systems;

- 3) modifications or updates of the supplier's policies and procedures;
- 4) new or changed controls to resolve information security incidents and to improve information security;
- c) monitor changes in supplier services including:
  - 1) changes and enhancement to networks;
  - 2) use of new technologies;
  - 3) adoption of new products or newer versions or releases;
  - 4) new development tools and environments;
  - 5) changes to physical location of service facilities;
  - 6) change of sub-suppliers;
  - 7) sub-contracting to another supplier;
- d) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
- e) conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;
- f) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;
- g) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
- h) respond to and manage any identified information security events or incidents;
- i) identify information security vulnerabilities and manage them;
- j) review information security aspects of the supplier's relationships with its own suppliers;
- k) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see [5.29](#), [5.30](#), [5.35](#), [5.36](#), [8.14](#));
- l) ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements;
- m) evaluate regularly that the suppliers maintain adequate information security levels.

The responsibility for managing supplier relationships should be assigned to a designated individual or team. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate actions should be taken when deficiencies in the service delivery are observed.

## Other information

See ISO/IEC 27036-3 for more detail.

## 5.23 Information security for use of cloud services (EI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

### Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

### Purpose

To specify and manage information security for the use of cloud services.

### Guidance

The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties.

The organization should define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how an organization manages services provided by external parties (see [5.21](#) and [5.22](#)).

The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and the organization acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.

The organization should define:

- a) all relevant information security requirements associated with the use of the cloud services;
- b) cloud service selection criteria and scope of cloud service usage;
- c) roles and responsibilities related to the use and management of cloud services;
- d) which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer;
- e) how to obtain and utilize information security capabilities provided by the cloud service provider;
- f) how to obtain assurance on information security controls implemented by cloud service providers;
- g) how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers;
- h) procedures for handling information security incidents that occur in relation to the use of cloud services;
- i) its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;
- j) how to change or stop the use of cloud services including exit strategies for cloud services.

Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, the organization should review cloud service agreements with the cloud service provider(s). A cloud service agreement should address the confidentiality, integrity, availability and information handling requirements of the organization, with appropriate cloud service level objectives and cloud service qualitative objectives. The organization should also undertake relevant risk assessments to identify the risks associated with

using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the appropriate management of the organization.

An agreement between the cloud service provider and the organization, acting as the cloud service customer, should include the following provisions for the protection of the organization's data and availability of services:

- a) providing solutions based on industry accepted standards for architecture and infrastructure;
- b) managing access controls of the cloud service to meet the requirements of the organization;
- c) implementing malware monitoring and protection solutions;
- d) processing and storing the organization's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction;
- e) providing dedicated support in the event of an information security incident in the cloud service environment;
- f) ensuring that the organization's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted);
- g) supporting the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;
- h) providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service;
- i) providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the organization, acting as the cloud service customer;
- j) providing and returning information such as configuration files, source code and data that are owned by the organization, acting as the cloud service customer, when requested during the service provision or at termination of service.

The organization, acting as the cloud service customer, should consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to the organization, including:

- a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering;
- b) processing or storing information in a new geographical or legal jurisdiction;
- c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

The organization using cloud services should maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and the organization, acting as the cloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

## Other information

This control considers cloud security from the perspective of the cloud service customer.

Additional information relating to cloud services can be found in ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 22123-1. Specifics related to cloud portability in support of exit strategies can be found in ISO/IEC 19941. Specifics related to information security and public cloud services are described in ISO/IEC 27017. Specifics related to PII protection in public clouds acting as PII processor are described in

ISO/IEC 27018. Supplier relationships for cloud services are covered by ISO/IEC 27036-4 and cloud service agreements and their contents are dealt with in the ISO/IEC 19086 series, with security and privacy specifically covered by ISO/IEC 19086-4.

## 5.24 Information security incident management planning and preparation (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

### Control

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

### Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.

### Guidance

#### Roles and responsibilities

The organization should establish appropriate information security incident management processes. Roles and responsibilities to carry out the incident management procedures should be determined and effectively communicated to the relevant internal and external interested parties.

The following should be considered:

- a) establishing a common method for reporting information security events including point of contact (see [6.8](#));
- b) establishing an incident management process to provide the organization with capability for managing information security incidents including administration, documentation, detection, triage, prioritization, analysis, communication and coordinating interested parties;
- c) establishing an incident response process to provide the organization with capability for assessing, responding to and learning from information security incidents;
- d) only allowing competent personnel to handle the issues related to information security incidents within the organization. Such personnel should be provided with procedure documentation and periodic training;
- e) establishing a process to identify required training, certification and ongoing professional development for incident response personnel.

#### Incident management procedures

The objectives for information security incident management should be agreed with management and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents including resolution time frame based on potential consequences and severity. Incident management procedures should be implemented to meet these objectives and priorities.

Management should ensure that an information security incident management plan is created considering different scenarios and procedures are developed and implemented for the following activities:

- a) evaluation of information security events according to criteria for what constitutes an information security incident;
- b) monitoring (see [8.15](#) and [8.16](#)), detecting (see [8.16](#)), classifying (see [5.25](#)), analysing and reporting (see [6.8](#)) of information security events and incidents (by human or automatic means);
- c) managing information security incidents to conclusion, including response and escalation (see [5.26](#)), according to the type and the category of the incident, possible activation of crisis management and activation of continuity plans, controlled recovery from an incident and communication to internal and external interested parties;
- d) coordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers and clients (see [5.5](#) and [5.6](#));
- e) logging incident management activities;
- f) handling of evidence (see [5.28](#));
- g) root cause analysis or post-mortem procedures;
- h) identification of lessons learned and any improvements to the incident management procedures or information security controls in general that are required.

### Reporting procedures

Reporting procedures should include:

- a) actions to be taken in case of an information security event (e.g. noting all pertinent details immediately such as malfunction occurring and messages on screen, immediately reporting to the point of contact and only taking coordinated actions);
- b) use of incident forms to support personnel to perform all necessary actions when reporting information security incidents;
- c) suitable feedback processes to ensure that those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed;
- d) creation of incident reports.

Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. breach notification requirements to regulators) should be considered when implementing incident management procedures.

### **Other information**

Information security incidents can transcend organizational and national boundaries. To respond to such incidents, it is beneficial to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in the ISO/IEC 27035 series.

## **5.25 Assessment and decision on information security events ([FI](#))**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

## Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

## Purpose

To ensure effective categorization and prioritization of information security events.

## Guidance

A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each information security event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

## Other information

The ISO/IEC 27035 series provides further guidance on incident management.

## 5.26 Response to information security incidents [\(E1\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

## Control

Information security incidents should be responded to in accordance with the documented procedures.

## Purpose

To ensure efficient and effective response to information security incidents.

## Guidance

The organization should establish and communicate procedures on information security incident response to all relevant interested parties.

Information security incidents should be responded to by a designated team with the required competency (see [5.24](#)).

The response should include the following:

- a) containing, if the consequences of the incident can spread, the systems affected by the incident;
- b) collecting evidence (see [5.28](#)) as soon as possible after the occurrence;
- c) escalation, as required including crisis management activities and possibly invoking business continuity plans (see [5.29](#) and [5.30](#));
- d) ensuring that all involved response activities are properly logged for later analysis;
- e) communicating the existence of the information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle;

- f) coordinating with internal and external parties such as authorities, external interest groups and forums, suppliers and clients to improve response effectiveness and help to minimize consequences for other organizations;
- g) once the incident has been successfully addressed, formally closing and recording it;
- h) conducting information security forensic analysis, as required (see [5.28](#));
- i) performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (see [5.27](#));
- j) identifying and managing information security vulnerabilities and weaknesses including those related to controls which have caused, contributed to or failed to prevent the incident.

## Other information

The ISO/IEC 27035 series provides further guidance on incident management.

## 5.27 Learning from information security incidents ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence

### Control

Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

### Purpose

To reduce the likelihood or consequences of future incidents.

### Guidance

The organization should establish procedures to quantify and monitor the types, volumes and costs of information security incidents.

The information gained from the evaluation of information security incidents should be used to:

- a) enhance the incident management plan including incident scenarios and procedures (see [5.24](#));
- b) identify recurring or serious incidents and their causes to update the organization's information security risk assessment and determine and implement necessary additional controls to reduce the likelihood or consequences of future similar incidents. Mechanisms to enable that include collecting, quantifying and monitoring information about incident types, volumes and costs;
- c) enhance user awareness and training (see [6.3](#)) by providing examples of what can happen, how to respond to such incidents and how to avoid them in the future.

## Other information

The ISO/IEC 27035 series provides further guidance.

## 5.28 Collection of evidence (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

### Control

The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

### Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.

### Guidance

Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of admission across the relevant jurisdictions.

In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off). Evidence typically needs to be collected in a manner that is admissible in the appropriate national courts of law or another disciplinary forum. It should be possible to show that:

- a) records are complete and have not been tampered with in any way;
- b) copies of electronic evidence are probably identical to the originals;
- c) any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Digital evidence can transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence.

### Other information

When an information security event is first detected, it is not always obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve legal advice or law enforcement early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037 provides definitions and guidelines for identification, collection, acquisition and preservation of digital evidence.

The ISO/IEC 27050 series deals with electronic discovery, which involves the processing of electronically stored information as evidence.

## 5.29 Information security during disruption (EI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Respond	#Continuity
#Corrective	#Integrity #Availability			#Protection #Resilience

### Control

The organization should plan how to maintain information security at an appropriate level during disruption.

### Purpose

To protect information and other associated assets during disruption.

### Guidance

The organization should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity management processes.

Plans should be developed, implemented, tested, reviewed and evaluated to maintain or restore the security of information of critical business processes following interruption or failure. Security of information should be restored at the required level and in the required time frames.

The organization should implement and maintain:

- a) information security controls, supporting systems and tools within business continuity and ICT continuity plans;
- b) processes to maintain existing information security controls during disruption;
- c) compensating controls for information security controls that cannot be maintained during disruption.

### Other information

In the context of business continuity and ICT continuity planning, it can be necessary to adapt the information security requirements depending on the type of disruption, compared to normal operational conditions. As part of the business impact analysis and risk assessment performed within business continuity management, the consequences of loss of confidentiality and integrity of information should be considered and prioritized in addition to the need for maintaining availability.

Information on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on business impact analysis (BIA) can be found in ISO/TS 22317.

## 5.30 ICT readiness for business continuity (EI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Continuity	#Resilience

### Control

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

### Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

## Guidance

ICT readiness for business continuity is an important component in business continuity management and information security management to ensure that the organization's objectives can continue to be met during disruption.

The ICT continuity requirements are the outcome of the business impact analysis (BIA). The BIA process should use impact types and criteria to assess the impacts over time resulting from the disruption of business activities that deliver products and services. The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). The BIA should then determine which resources are needed to support prioritized activities. An RTO should also be specified for these resources. A subset of these resources should include ICT services.

The BIA involving ICT services can be expanded to define performance and capacity requirements of ICT systems and recovery point objectives (RPO) of information required to support activities during disruption.

Based on the outputs from the BIA and risk assessment involving ICT services, the organization should identify and select ICT continuity strategies that consider options for before, during and after disruption. The business continuity strategies can comprise one or more solutions. Based on the strategies, plans should be developed, implemented and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

The organization should ensure that:

- a) an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence;
- b) ICT continuity plans, including response and recovery procedures detailing how the organization is planning to manage an ICT service disruption, are:
  - 1) regularly evaluated through exercises and tests;
  - 2) approved by management;
- c) ICT continuity plans include the following ICT continuity information:
  - 1) performance and capacity specifications to meet the business continuity requirements and objectives as specified in the BIA;
  - 2) RTO of each prioritized ICT service and the procedures for restoring those components;
  - 3) RPO of the prioritized ICT resources defined as information and the procedures for restoring the information.

## Other information

Managing ICT continuity forms a key part of business continuity requirements concerning availability to be able to:

- a) respond and recover from disruption to ICT services regardless of the cause;
- b) ensure continuity of prioritized activities are supported by the required ICT services;
- c) respond before a disruption to ICT services occurs, and upon detection of at least one incident that can result in a disruption to ICT services.

Further guidance on ICT readiness for business continuity can be found in ISO/IEC 27031.

Further guidance on business continuity management systems can be found in ISO 22301 and ISO 22313.

Further guidance on BIA can be found in ISO/TS 22317.

### 5.31 Legal, statutory, regulatory and contractual requirements (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection

#### Control

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.

#### Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

#### Guidance

##### General

External requirements including legal, statutory, regulatory or contractual requirements should be taken into consideration when:

- a) developing information security policies and procedures;
- b) designing, implementing or changing information security controls;
- c) classifying information and other associated assets as part of the process for setting information security requirements for internal needs or for supplier agreements;
- d) performing information security risk assessments and determining information security risk treatment activities;
- e) determining processes along with related roles and responsibilities relating to information security;
- f) determining suppliers' contractual requirements relevant to the organization and the scope of supply of products and services.

##### Legislation and regulations

The organization should:

- a) identify all legislation and regulations relevant to the organization's information security in order to be aware of the requirements for their type of business;
- b) take into consideration compliance in all relevant countries, if the organization:
  - conducts business in other countries;
  - uses products and services from other countries where laws and regulations can affect the organization;
  - transfers information across jurisdictional borders where laws and regulations can affect the organization;
- c) review the identified legislation and regulation regularly in order to keep up to date with the changes and identify new legislation;
- d) define and document the specific processes and individual responsibilities to meet these requirements.

## Cryptography

Cryptography is an area that often has specific legal requirements. Compliance with the relevant agreements, laws and regulations relating to the following items should be taken into consideration:

- a) restrictions on import or export of computer hardware and software for performing cryptographic functions;
- b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;
- c) restrictions on the usage of cryptography;
- d) mandatory or discretionary methods of access by the countries' authorities to encrypted information;
- e) validity of digital signatures, seals and certificates.

It is recommended to seek legal advice when ensuring compliance with relevant legislation and regulations, especially when encrypted information or cryptography tools are moved across jurisdictional borders.

## Contracts

Contractual requirements related to information security should include those stated in:

- a) contracts with clients;
- b) contracts with suppliers (see [5.20](#));
- c) insurance contracts.

## **Other information**

No other information.

### **5.32 Intellectual property rights ([FI](#))**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem

## **Control**

The organization should implement appropriate procedures to protect intellectual property rights.

## **Purpose**

To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

## **Guidance**

The following guidelines should be considered to protect any material that can be considered intellectual property:

- a) defining and communicating a topic-specific policy on protection of intellectual property rights;
- b) publishing procedures for intellectual property rights compliance that define compliant use of software and information products;
- c) acquiring software only through known and reputable sources, to ensure that copyright is not infringed upon;

- d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;
- e) maintaining proof and evidence of ownership of licences, manuals, etc.;
- f) ensuring that any maximum number of users or resources [e.g. central processing units (CPUs)] permitted within the licence is not exceeded;
- g) carrying out reviews to ensure that only authorized software and licensed products are installed;
- h) providing procedures for maintaining appropriate licence conditions;
- i) providing procedures for disposing of or transferring software to others;
- j) complying with terms and conditions for software and information obtained from public networks and outside sources;
- k) not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law or the applicable licences;
- l) not copying, in full or in part, standards (e.g. ISO/IEC International Standards), books, articles, reports or other documents, other than permitted by copyright law or the applicable licences.

## Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. See the ISO/IEC 19770 series for details about IT asset management.

Data can be acquired from outside sources. It is generally the case that such data is obtained under the terms of a data sharing agreement or similar legal instrument. Such data sharing agreements should make it clear what processing is permitted for the acquired data. It is also advisable that the provenance of the data is clearly stated. See ISO/IEC 23751 for details about data sharing agreements.

Legal, statutory, regulatory and contractual requirements can place restrictions on the copying of proprietary material. In particular, they can require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which can involve fines and criminal proceedings.

Aside from the organization needing to comply with its obligations towards third party intellectual property rights, the risks of personnel and third parties failing to uphold the organization's own intellectual property rights should also be managed.

### 5.33 Protection of records (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence

#### Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

#### Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

## Guidance

The organization should take the following steps to protect the authenticity, reliability, integrity and usability of records, as their business context and requirements for their management change over time:

- a) issue guidelines on the storage, handling chain of custody and disposal of records, which includes prevention of manipulation of records. These guidelines should be aligned with the organization's topic-specific policy on records management and other records requirements;
- b) draw up a retention schedule defining records and the period of time for which they should be retained.

The system of storage and handling should ensure identification of records and of their retention period taking into consideration national or regional legislation or regulations, as well as community or societal expectations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

When deciding on protection of specific organizational records, their corresponding information security classification, based on the organization's classification scheme, should be considered. Records should be categorized into record types (e.g. accounting records, business transaction records, personnel records, legal records), each with details of retention periods and type of allowable storage media which can be physical or electronic.

Data storage systems should be chosen such that required records can be retrieved in an acceptable time frame and format, depending on the requirements to be fulfilled.

Where electronic storage media are chosen, procedures to ensure the ability to access records (both storage media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be retained to enable decryption of the records for the length of time the records are retained (see [8.24](#)).

Storage and handling procedures should be implemented in accordance with recommendations provided by manufacturers of storage media. Consideration should be given to the possibility of deterioration of media used for storage of records.

## Other information

Records document individual events or transactions or can form aggregations that have been designed to document work processes, activities or functions. They are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business.

In the management of records, metadata is data describing the context, content and structure of records, as well as their management over time. Metadata is an essential component of any record.

It can be necessary to retain some records securely to meet legal, statutory, regulatory or contractual requirements, as well as to support essential business activities. National law or regulation can set the time period and data content for information retention. Further information about records management can be found in ISO 15489.

### 5.34 Privacy and protection of PII ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection

## Control

The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

## Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

## Guidance

The organization should establish and communicate a topic-specific policy on privacy and protection of PII to all relevant interested parties.

The organization should develop and implement procedures for the preservation of privacy and protection of PII. These procedures should be communicated to all relevant interested parties involved in the processing of personally identifiable information.

Compliance with these procedures and all relevant legislation and regulations concerning the preservation of privacy and protection of PII requires appropriate roles, responsibilities and controls. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to personnel, service providers and other interested parties on their individual responsibilities and the specific procedures that should be followed.

Responsibility for handling PII should be dealt with taking into consideration relevant legislation and regulations.

Appropriate technical and organizational measures to protect PII should be implemented.

## Other information

A number of countries have introduced legislation placing controls on the collection, processing, transmission and deletion of PII. Depending on the respective national legislation, such controls can impose duties on those collecting, processing and disseminating PII and can also restrict the authority to transfer PII to other countries.

ISO/IEC 29100 provides a high-level framework for the protection of PII within ICT systems. Further information on privacy information management systems can be found in ISO/IEC 27701. Specific information regarding privacy information management for public clouds acting as PII processors can be found in ISO/IEC 27018.

ISO/IEC 29134 provides guidelines for privacy impact assessment (PIA) and gives an example of the structure and content of a PIA report. Compared with ISO/IEC 27005, this is focused on PII processing and relevant to those organizations that process PII. This can help identify privacy risks and possible mitigations to reduce these risks to acceptable levels.

## 5.35 Independent review of information security [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
#Corrective	#Integrity #Availability			

## Control

The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

## Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.

## Guidance

The organization should have processes to conduct independent reviews.

Management should plan and initiate periodic independent reviews. The reviews should include assessing opportunities for improvement and the need for changes to the approach to information security, including the information security policy, topic-specific policies and other controls.

Such reviews should be carried out by individuals independent of the area under review (e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews). Individuals carrying out these reviews should have the appropriate competence. The person conducting the reviews should not be in the line of authority to ensure they have the independence to make an assessment.

The results of the independent reviews should be reported to the management who initiated the reviews and, if appropriate, to top management. These records should be maintained.

If the independent reviews identify that the organization's approach and implementation to managing information security is inadequate [e.g. documented objectives and requirements are not met or are not compliant with the direction for information security stated in the information security policy and topic-specific policies (see [5.1](#))], management should initiate corrective actions.

In addition to the periodic independent reviews, the organization should consider conducting independent reviews when:

- a) laws and regulations which affect the organization change;
- b) significant incidents occur;
- c) the organization starts a new business or changes a current business;
- d) the organization starts to use a new product or service, or changes the use of a current product or service;
- e) the organization changes the information security controls and procedures significantly.

## Other information

ISO/IEC 27007 and ISO/IEC TS 27008 provide guidance for carrying out independent reviews.

### 5.36 Compliance with policies, rules and standards for information security ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem

## Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

## Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

## Guidance

Managers, service, product or information owners should identify how to review that information security requirements defined in the information security policy, topic-specific policies, rules, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

- a) identify the causes of the non-compliance;
- b) evaluate the need for corrective actions to achieve compliance;
- c) implement appropriate corrective actions;
- d) review corrective actions taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers, service, product or information owners should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see [5.35](#)) when an independent review takes place in the area of their responsibility.

Corrective actions should be completed in a timely manner as appropriate to the risk. If not completed by the next scheduled review, progress should at least be addressed at that review.

## Other information

Operational monitoring of system use is covered in [8.15](#), [8.16](#), [8.17](#).

### 5.37 Documented operating procedures (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Asset_management	#Governance_and_Ecosystem
#Corrective	#Integrity #Availability	#Recover	#Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Protection #Defence

## Control

Operating procedures for information processing facilities should be documented and made available to personnel who need them.

## Purpose

To ensure the correct and secure operation of information processing facilities.

## Guidance

Documented procedures should be prepared for the organization's operational activities associated with information security, for example:

- a) when the activity needs to be performed in the same way by many people;
- b) when the activity is performed rarely and when next performed the procedure is likely to have been forgotten;
- c) when the activity is new and presents a risk if not performed correctly;
- d) prior to handing over the activity to new personnel.

The operating procedures should specify:

- a) the responsible individuals;
- b) the secure installation and configuration of systems;
- c) processing and handling of information, both automated and manual;
- d) backup (see [8.13](#)) and resilience;
- e) scheduling requirements, including interdependencies with other systems;
- f) instructions for handling errors or other exceptional conditions [e.g. restrictions on the use of utility programs (see [8.18](#))], which can arise during job execution;
- g) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
- h) storage media handling instructions (see [7.10](#) and [7.14](#));
- i) system restart and recovery procedures for use in the event of system failure;
- j) the management of audit trail and system log information (see [8.15](#) and [8.17](#)) and video monitoring systems (see [7.4](#));
- k) monitoring procedures such as capacity, performance and security (see [8.6](#) and [8.16](#));
- l) maintenance instructions.

Documented operating procedures should be reviewed and updated when needed. Changes to documented operating procedures should be authorized. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

## Other information

No other information.

## 6 People controls [\(FI\)](#)

### 6.1 Screening [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

## Control

Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

## Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

## Guidance

A screening process should be performed for all personnel including full-time, part-time and temporary staff. Where these individuals are contracted through suppliers of services, screening requirements should be included in the contractual agreements between the organization and the suppliers.

Information on all candidates being considered for positions within the organization should be collected and handled taking into consideration any appropriate legislation existing in the relevant jurisdiction. In some jurisdictions, the organization can be legally required to inform the candidates beforehand about the screening activities.

Verification should take into consideration all relevant privacy, PII protection and employment-based legislation and should, where permitted, include the following:

- a) availability of satisfactory references (e.g. business and personal references);
- b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity verification (e.g. passport or other acceptable document issued by appropriate authorities);
- e) more detailed verification, such as credit review or review of criminal records if the candidate takes on a critical role.

When an individual is hired for a specific information security role, the organization should make sure the candidate:

- a) has the necessary competence to perform the security role;
- b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities and, in particular, if these involve handling confidential information (e.g. financial information, personal information or health care information) the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews (e.g. who is eligible to screen people and how, when and why verification reviews are carried out).

In situations where verification cannot be completed in a timely manner, mitigating controls should be implemented until the review has been finished, for example:

- a) delayed onboarding;
- b) delayed deployment of corporate assets;
- c) onboarding with reduced access;
- d) termination of employment.

Verification checks should be repeated periodically to confirm ongoing suitability of personnel, depending on the criticality of a person's role.

### Other information

No other information.

## 6.2 Terms and conditions of employment (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

### Control

The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.

### Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered.

### Guidance

The contractual obligations for personnel should take into consideration the organization's information security policy and relevant topic-specific policies. In addition, the following points can be clarified and stated:

- a) confidentiality or non-disclosure agreements that personnel who are given access to confidential information should sign prior to being given access to information and other associated assets (see [6.6](#));
- b) legal responsibilities and rights [e.g. regarding copyright laws or data protection legislation (see [5.32](#) and [5.34](#))];
- c) responsibilities for the classification of information and management of the organization's information and other associated assets, information processing facilities and information services handled by the personnel (see [5.9](#) to [5.13](#));
- d) responsibilities for the handling of information received from interested parties;
- e) actions to be taken if personnel disregard the organization's security requirements (see [6.4](#)).

Information security roles and responsibilities should be communicated to candidates during the pre-employment process.

The organization should ensure that personnel agree to terms and conditions concerning information security. These terms and conditions should be appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The terms and conditions concerning information security should be reviewed when laws, regulations, the information security policy or topic-specific policies change.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see [6.5](#)).

### Other information

A code of conduct can be used to state personnel's information security responsibilities regarding confidentiality, PII protection, ethics, appropriate use of the organization's information and other associated assets, as well as reputable practices expected by the organization.

An external party, with which supplier personnel are associated, can be required to enter into contractual agreements on behalf of the contracted individual.

If the organization is not a legal entity and does not have employees, the equivalent of contractual agreement and terms and conditions can be considered in line with the guidance of this control.

## 6.3 Information security awareness, education and training (E1)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

### Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

### Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

### Guidance

#### General

An information security awareness, education and training programme should be established in line with the organization's information security policy, topic-specific policies and relevant procedures on information security, taking into consideration the organization's information to be protected and the information security controls that have been implemented to protect the information.

Information security awareness, education and training should take place periodically. Initial awareness, education and training can apply to new personnel and to those who transfer to new positions or roles with substantially different information security requirements.

Personnel's understanding should be assessed at the end of an awareness, education or training activity to test knowledge transfer and the effectiveness of the awareness, education and training programme.

#### Awareness

An information security awareness programme should aim to make personnel aware of their responsibilities for information security and the means by which those responsibilities are discharged.

The awareness programme should be planned taking into consideration the roles of personnel in the organization, including internal and external personnel (e.g. external consultants, supplier personnel). The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new personnel. It should also be built on lessons learnt from information security incidents.

The awareness programme should include a number of awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules and e-mails.

Information security awareness should cover general aspects such as:

- a) management's commitment to information security throughout the organization;
- b) familiarity and compliance needs concerning applicable information security rules and obligations, taking into account information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements;
- c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties;
- d) basic information security procedures [e.g. information security event reporting ([6.8](#))] and baseline controls [e.g. password security ([5.17](#))];
- e) contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

### Education and training

The organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. Technical teams should have the skills for configuring and maintaining the required security level for devices, systems, applications and services. If there are missing skills, the organization should take action and acquire them.

The education and training programme should consider different forms [e.g. lectures or self-studies, being mentored by expert staff or consultants (on-the-job training), rotating staff members to follow different activities, recruiting already skilled people and hiring consultants]. It can use different means of delivery including classroom-based, distance learning, web-based, self-paced and others. Technical personnel should keep their knowledge up to date by subscribing to newsletters and magazines or by attending conferences and events aimed at technical and professional improvement.

### **Other information**

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why', when possible. It is important that personnel understand the aim of information security and the potential effect, positive and negative, on the organization of their own behaviour.

Information security awareness, education and training can be part of, or conducted in collaboration with, other activities, for example general information management, ICT, security, privacy or safety training.

## **6.4 Disciplinary process ([FI](#))**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Human_resource_security	#Governance_and_Ecosystem
#Corrective	#Integrity #Availability	#Respond		

### **Control**

A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

### **Purpose**

To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

## Guidance

The disciplinary process should not be initiated without prior verification that an information security policy violation has occurred (see [5.28](#)).

The formal disciplinary process should provide for a graduated response that takes into consideration factors such as:

- a) the nature (who, what, when, how) and gravity of the breach and its consequences;
- b) whether the offence was intentional (malicious) or unintentional (accidental);
- c) whether or not this is a first or repeated offence;
- d) whether or not the violator was properly trained.

The response should take into consideration relevant legal, statutory, regulatory contractual and business requirements as well as other factors as required. The disciplinary process should also be used as a deterrent to prevent personnel and other relevant interested parties from violating the information security policy, topic-specific policies and procedures for information security. Deliberate information security policy violations can require immediate actions.

## Other information

Where possible, the identity of individuals subject to disciplinary action should be protected in line with applicable requirements.

When individuals demonstrate excellent behaviour with regard to information security, they can be rewarded to promote information security and encourage good behaviour.

## 6.5 Responsibilities after termination or change of employment ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem

### Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

### Purpose

To protect the organization's interests as part of the process of changing or terminating employment or contracts.

### Guidance

The process for managing termination or change of employment should define which information security responsibilities and duties should remain valid after termination or change. This can include confidentiality of information, intellectual property and other knowledge obtained, as well as responsibilities contained within any other confidentiality agreement (see [6.6](#)). Responsibilities and duties still valid after termination of employment or contract should be contained in the individual's terms and conditions of employment (see [6.2](#)), contract or agreement. Other contracts or agreements that continue for a defined period after the end of the individual's employment can also contain information security responsibilities.

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual.

A process should be established for the communication of the changes and of operating procedures to personnel, other interested parties and relevant contact persons (e.g. to customers and suppliers).

The process for the termination or change of employment should also be applied to external personnel (i.e. suppliers) when a termination occurs of personnel, the contract or the job with the organization, or when there is a change of the job within the organization.

### Other information

In many organizations, the human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person transitioning to manage the information security aspects of the relevant procedures. In the case of personnel provided through an external party (e.g. through a supplier), this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

## 6.6 Confidentiality or non-disclosure agreements (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

### Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

### Purpose

To maintain confidentiality of information accessible by personnel or external parties.

### Guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to interested parties and personnel of the organization. Based on an organization's information security requirements, the terms in the agreements should be determined by taking into consideration the type of information that will be handled, its classification level, its use and the permissible access by the other party. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

- a) a definition of the information to be protected (e.g. confidential information);
- b) the expected duration of an agreement, including cases where it can be necessary to maintain confidentiality indefinitely or until the information becomes publicly available;
- c) the required actions when an agreement is terminated;
- d) the responsibilities and actions of signatories to avoid unauthorized information disclosure;
- e) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
- f) the permitted use of confidential information and rights of the signatory to use the information;
- g) the right to audit and monitor activities that involve confidential information for highly sensitive circumstances;

- h) the process for notification and reporting of unauthorized disclosure or confidential information leakage;
- i) the terms for information to be returned or destroyed at agreement termination;
- j) the expected actions to be taken in the case of non-compliance with the agreement.

The organization should take into consideration the compliance with confidentiality and non-disclosure agreements for the jurisdiction to which they apply (see [5.31](#), [5.32](#), [5.33](#), [5.34](#)).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

## Other information

Confidentiality and non-disclosure agreements protect the organization's information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

## 6.7 Remote working (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection

### Control

Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

### Purpose

To ensure the security of information when personnel are working remotely.

### Guidance

Remote working occurs whenever personnel of the organization work from a location outside of the organization's premises, accessing information whether in hardcopy or electronically via ICT equipment. Remote working environments include those referred to as "teleworking", "telecommuting", "flexible workplace", "virtual work environments" and "remote maintenance".

**NOTE** It is possible that not all the recommendations in this guidance can be applied due to local legislation and regulations in different jurisdictions.

Organizations allowing remote working activities should issue a topic-specific policy on remote working that defines the relevant conditions and restrictions. Where deemed applicable, the following matters should be considered:

- a) the existing or proposed physical security of the remote working site, taking into account the physical security of the location and the local environment, including the different jurisdictions where personnel are located;
- b) rules and security mechanisms for the remote physical environment such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information and other associated assets, and information security event reporting (see [6.8](#));
- c) the expected physical remote working environments;

- d) the communications security requirements, taking into account the need for remote access to the organization's systems, the sensitivity of the information to be accessed and passed over the communication link and the sensitivity of the systems and applications;
- e) the use of remote access such as virtual desktop access that supports processing and storage of information on privately owned equipment;
- f) the threat of unauthorized access to information or resources from other persons at the remote working site (e.g. family and friends);
- g) the threat of unauthorized access to information or resources from other persons in public places;
- h) the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services;
- i) use of security measures, such as firewalls and protection against malware;
- j) secure mechanisms for deploying and initializing systems remotely;
- k) secure mechanisms for authentication and enablement of access privileges taking into consideration the vulnerability of single-factor authentication mechanisms where remote access to the organization's network is allowed.

The guidelines and measures to be considered should include:

- a) the provision of suitable equipment and storage furniture for the remote working activities, where the use of privately-owned equipment that is not under the control of the organization is not allowed;
- b) a definition of the work permitted, the classification of information that can be held and the internal systems and services that the remote worker is authorized to access;
- c) the provision of training for those working remotely and those providing support. This should include how to conduct business in a secure manner while working remotely;
- d) the provision of suitable communication equipment, including methods for securing remote access, such as requirements on device screen locks and inactivity timers; the enabling of device location tracking; installation of remote wipe capabilities;
- e) physical security;
- f) rules and guidance on family and visitor access to equipment and information;
- g) the provision of hardware and software support and maintenance;
- h) the provision of insurance;
- i) the procedures for backup and business continuity;
- j) audit and security monitoring;
- k) revocation of authority and access rights and the return of equipment when the remote working activities are terminated.

## Other information

No other information.

## 6.8 Information security event reporting [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence

### Control

The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

### Purpose

To support timely, consistent and effective reporting of information security events that can be identified by personnel.

### Guidance

All personnel and users should be made aware of their responsibility to report information security events as quickly as possible in order to prevent or minimize the effect of information security incidents. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. The reporting mechanism should be as easy, accessible and available as possible. Information security events include incidents, breaches and vulnerabilities.

Situations to be considered for information security event reporting include:

- a) ineffective information security controls;
- b) breach of information confidentiality, integrity or availability expectations;
- c) human errors;
- d) non-compliance with the information security policy, topic-specific policies or applicable standards;
- e) breaches of physical security measures;
- f) system changes that have not gone through the change management process;
- g) malfunctions or other anomalous system behaviour of software or hardware;
- h) access violations;
- i) vulnerabilities;
- j) suspected malware infection.

Personnel and users should be advised not to attempt to prove suspected information security vulnerabilities. Testing vulnerabilities can be interpreted as a potential misuse of the system and can also cause damage to the information system or service, and it can corrupt or obscure digital evidence. Ultimately, this can result in legal liability for the individual performing the testing.

### Other information

See the ISO/IEC 27035 series for additional information.

## 7 Physical controls (FI)

### 7.1 Physical security perimeters (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

#### Control

Security perimeters should be defined and used to protect areas that contain information and other associated assets.

#### Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

#### Guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

- a) defining security perimeters and the siting and strength of each of the perimeters in accordance with the information security requirements related to the assets within the perimeter;
- b) having physically sound perimeters for a building or site containing information processing facilities (i.e. there should be no gaps in the perimeter or areas where a break-in can easily occur). The exterior roofs, walls, ceilings and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms (e.g. bars, alarms, locks). Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level; ventilation points should also be considered;
- c) alarming, monitoring and testing all fire doors on a security perimeter in conjunction with the walls to establish the required level of resistance in accordance with suitable standards. They should operate in a failsafe manner.

#### Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities.

A secure area can be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access can be necessary between areas with different security requirements inside the security perimeter. The organization should consider having physical security measures that can be strengthened during increased threat situations.

### 7.2 Physical entry (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection

#### Control

Secure areas should be protected by appropriate entry controls and access points.

## Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs.

## Guidance

### General

Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following guidelines should be considered:

- a) restricting access to sites and buildings to authorized personnel only. The process for the management of access rights to physical areas should include the provision, periodical review, update and revocation of authorizations (see [5.18](#));
- b) securely maintaining and monitoring a physical logbook or electronic audit trail of all access and protecting all logs (see [5.33](#)) and sensitive authentication information;
- c) establishing and implementing a process and technical mechanisms for the management of access to areas where information is processed or stored. Authentication mechanisms include the use of access cards, biometrics or two-factor authentication such as an access card and secret PIN. Double security doors should be considered for access to sensitive areas;
- d) setting up a reception area monitored by personnel, or other means to control physical access to the site or building;
- e) inspecting and examining personal belongings of personnel and interested parties upon entry and exit;  
**NOTE** Local legislation and regulations can exist regarding the possibility of inspecting personal belongings.
- f) requiring all personnel and interested parties to wear some form of visible identification and to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Easily distinguishable badges should be considered to better identify permanent employees, suppliers and visitors;
- g) granting supplier personnel restricted access to secure areas or information processing facilities only when required. This access should be authorized and monitored;
- h) giving special attention to physical access security in the case of buildings holding assets for multiple organizations;
- i) designing physical security measures so that they can be strengthened when the likelihood of physical incidents increases;
- j) securing other entry points such as emergency exits from unauthorized access;
- k) setting up a key management process to ensure the management of the physical keys or authentication information (e.g. lock codes, combination locks to offices, rooms and facilities such as key cabinets) and to ensure a log book or annual key audit and that access to physical keys or authentication information is controlled (see [5.17](#) for further guidance on authentication information).

### Visitors

The following guidelines should be considered:

- a) authenticating the identity of visitors by an appropriate means;
- b) recording the date and time of entry and departure of visitors;

- c) only granting access for visitors for specific, authorized purposes and with instructions on the security requirements of the area and on emergency procedures;
- d) supervising all visitors, unless an explicit exception is granted.

#### Delivery and loading areas and incoming material

The following guidelines should be considered:

- a) restricting access to delivery and loading areas from outside of the building to identified and authorized personnel;
- b) designing the delivery and loading areas so that deliveries can be loaded and unloaded without delivery personnel gaining unauthorized access to other parts of the building;
- c) securing the external doors of delivery and loading areas when doors to restricted areas are opened;
- d) inspecting and examining incoming deliveries for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas;
- e) registering incoming deliveries in accordance with asset management procedures (see [5.9](#) and [7.10](#)) on entry to the site;
- f) physically segregating incoming and outgoing shipments, where possible;
- g) inspecting incoming deliveries for evidence of tampering on the way. If tampering is discovered, it should be immediately reported to security personnel.

#### **Other information**

No other information.

### **7.3 Securing offices, rooms and facilities (FI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

#### **Control**

Physical security for offices, rooms and facilities should be designed and implemented.

#### **Purpose**

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

#### **Guidance**

The following guidelines should be considered to secure offices, rooms and facilities:

- a) siting critical facilities to avoid access by the public;
- b) where applicable, ensuring buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;
- c) configuring facilities to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;
- d) not making directories, internal telephone books and online accessible maps identifying locations of confidential information processing facilities readily available to any unauthorized person.

## Other information

No other information.

## 7.4 Physical security monitoring (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

### Control

Premises should be continuously monitored for unauthorized physical access.

### Purpose

To detect and deter unauthorized physical access.

### Guidance

Physical premises should be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems should be continuously monitored to detect unauthorized access or suspicious behaviour by:

- a) installing video monitoring systems such as closed-circuit television to view and record access to sensitive areas within and outside an organization's premises;
- b) installing, according to relevant applicable standards, and periodically testing contact, sound or motion detectors to trigger an intruder alarm such as:
  - 1) installing contact detectors that trigger an alarm when a contact is made or broken in any place where a contact can be made or broken (such as windows and doors and underneath objects) to be used as a panic alarm;
  - 2) motion detectors based on infra-red technology which trigger an alarm when an object passes through their field of view;
  - 3) installing sensors sensitive to the sound of breaking glass which can be used to trigger an alarm to alert security personnel;
- c) using those alarms to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times; cover should also be provided for other areas (e.g. computer or communications rooms).

The design of monitoring systems should be kept confidential because disclosure can facilitate undetected break-ins.

Monitoring systems should be protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

The alarm system control panel should be placed in an alarmed zone and, for safety alarms, in a place that allows an easy exit route for the person who sets the alarm. The control panel and the detectors should have tamperproof mechanisms. The system should regularly be tested to ensure that it is working as intended, particularly if its components are battery powered.

Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

### Other information

No other information.

## 7.5 Protecting against physical and environmental threats (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

### Control

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

### Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

### Guidance

Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

Physical premises location and construction should take account of:

- a) local topography, such as appropriate elevation, bodies of water and tectonic fault lines;
- b) urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.

Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:

- a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);
- b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;
- c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;
- d) explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.

### Other information

Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

## 7.6 Working in secure areas (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

### Control

Security measures for working in secure areas should be designed and implemented.

### Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

### Guidance

The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

The following guidelines should be considered:

- a) making personnel aware only of the existence of, or activities within, a secure area on a need-to-know basis;
- b) avoiding unsupervised work in secure areas both for safety reasons and to reduce chances for malicious activities;
- c) physically locking and periodically inspecting vacant secure areas;
- d) not allowing photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized;
- e) appropriately controlling the carrying and use of user endpoint devices in secure areas;
- f) posting emergency procedures in a readily visible or accessible manner.

### Other information

No other information.

## 7.7 Clear desk and clear screen (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

### Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

### Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

## Guidance

The organization should establish and communicate a topic-specific policy on clear desk and clear screen to all relevant interested parties.

The following guidelines should be considered:

- a) locking away sensitive or critical business information (e.g. on paper or on electronic storage media) (ideally in a safe, cabinet or other form of security furniture) when not required, especially when the office is vacated;
- b) protecting user endpoint devices by key locks or other security means when not in use or unattended;
- c) leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature;
- d) making the originator collect outputs from printers or multi-function devices immediately. The use of printers with an authentication function, so the originators are the only ones who can get their printouts and only when standing next to the printer;
- e) securely storing documents and removable storage media containing sensitive information and, when no longer required, discarding them using secure disposal mechanisms;
- f) establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);
- g) clearing sensitive or critical information on whiteboards and other types of display when no longer required.

The organization should have procedures in place when vacating facilities including conducting a final sweep prior to leaving to ensure the organization's assets are not left behind (e.g. documents fallen behind drawers or furniture).

## Other information

No other information.

## 7.8 Equipment siting and protection (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

## Control

Equipment should be sited securely and protected.

## Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

## Guidance

The following guidelines should be considered to protect equipment:

- a) siting equipment to minimize unnecessary access into work areas and to avoid unauthorized access;
- b) carefully positioning information processing facilities handling sensitive data to reduce the risk of information being viewed by unauthorized persons during their use;

- c) adopting controls to minimize the risk of potential physical and environmental threats [e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism];
- d) establishing guidelines for eating, drinking and smoking in proximity to information processing facilities;
- e) monitoring environmental conditions, such as temperature and humidity, for conditions which can adversely affect the operation of information processing facilities;
- f) applying lightning protection to all buildings and fitting lightning protection filters to all incoming power and communications lines;
- g) considering the use of special protection methods, such as keyboard membranes, for equipment in industrial environments;
- h) protecting equipment processing confidential information to minimize the risk of information leakage due to electromagnetic emanation;
- i) physically separating information processing facilities managed by the organization from those not managed by the organization.

#### Other information

No other information.

### 7.9 Security of assets off-premises [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

#### Control

Off-site assets should be protected.

#### Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

#### Guidance

Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization [bring your own device (BYOD)] needs protection. The use of these devices should be authorized by management.

The following guidelines should be considered for the protection of devices which store or process information outside the organization's premises:

- a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;
- b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);
- c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to be transferred with the asset should be securely deleted before the transfer;

- d) where necessary and practical, requiring authorization for equipment and media to be removed from the organization's premises and keeping a record of such removals in order to maintain an audit trail (see [5.14](#));
- e) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing;
- f) implementing location tracking and ability for remote wiping of devices.

Permanent installation of equipment outside the organization's premises [such as antennas and automated teller machines (ATMs)] can be subject to higher risk of damage, theft or eavesdropping. These risks can vary considerably between locations and should be taken into account in determining the most appropriate measures. The following guidelines should be considered when siting this equipment outside of the organization's premises:

- a) physical security monitoring (see [7.4](#));
- b) protecting against physical and environmental threats (see [7.5](#));
- c) physical access and tamper proofing controls;
- d) logical access controls.

### Other information

More information about other aspects of protecting information storing and processing equipment and user endpoint devices can be found in [8.1](#) and [6.7](#).

## 7.10 Storage media ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

### Control

Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

### Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

### Guidance

#### Removable storage media

The following guidelines for the management of removable storage media should be considered:

- a) establishing a topic-specific policy on the management of removable storage media and communicating such topic-specific policy to anyone who uses or handles removable storage media;
- b) where necessary and practical, requiring authorization for storage media to be removed from the organization and keeping a record of such removals in order to maintain an audit trail;
- c) storing all storage media in a safe, secure environment according to their information classification and protecting them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications;

- d) if information confidentiality or integrity are important considerations, using cryptographic techniques to protect information on removable storage media;
- e) to mitigate the risk of storage media degrading while stored information is still needed, transferring the information to fresh storage media before becoming unreadable;
- f) storing multiple copies of valuable information on separate storage media to further reduce the risk of coincidental information damage or loss;
- g) considering the registration of removable storage media to limit the chance for information loss;
- h) only enabling removable storage media ports [e.g. secure digital (SD) card slots and universal serial bus (USB) ports] if there is an organizational reason for their use;
- i) where there is a need to use removable storage media, monitoring the transfer of information to such storage media;
- j) information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.

In this control, media includes paper documents. When transferring physical storage media, apply security measures in [5.14](#).

#### Secure reuse or disposal

Procedures for the secure reuse or disposal of storage media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

- a) if storage media containing confidential information need to be reused within the organization, securely deleting data or formatting the storage media before reuse (see [8.10](#));
- b) disposing of storage media containing confidential information securely when not needed anymore (e.g. by destroying, shredding or securely deleting the content);
- c) having procedures in place to identify the items that can require secure disposal;
- d) many organizations offer collection and disposal services for storage media. Care should be taken in selecting a suitable external party supplier with adequate controls and experience;
- e) logging the disposal of sensitive items in order to maintain an audit trail;
- f) when accumulating storage media for disposal, giving consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

A risk assessment should be performed on damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded (see [7.14](#)).

#### **Other information**

When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

### **7.11 Supporting utilities ([FI](#))**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Integrity	#Protect	#Physical_security	#Protection
#Detective	#Availability	#Detect		

## Control

Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

### Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

### Guidance

Organizations depend on utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) to support their information processing facilities. Therefore, the organization should:

- a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;
- b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
- c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;
- d) if necessary, raise alarms to detect utilities malfunctions;
- e) if necessary, ensure utilities have multiple feeds with diverse physical routing;
- f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;
- g) ensure equipment supporting the utilities is connected to the internet only when needed and only in a secure manner.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. Emergency contact details should be recorded and available to personnel in the event of an outage.

### Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

## 7.12 Cabling security (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

## Control

Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

### Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

## Guidance

The following guidelines for cabling security should be considered:

- a) power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, such as floor cable protector and utility pole; if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);
- b) segregating power cables from communications cables to prevent interference;
- c) for sensitive or critical systems, further controls to consider include:
  - 1) installation of armoured conduit and locked rooms or boxes and alarms at inspection and termination points;
  - 2) use of electromagnetic shielding to protect the cables;
  - 3) periodical technical sweeps and physical inspections to detect unauthorized devices being attached to the cables;
  - 4) controlled access to patch panels and cable rooms (e.g. with mechanical keys or PINs);
  - 5) use of fibre-optic cables;
- d) labelling cables at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Specialist advice should be sought on how to manage risks arising from cabling incidents or malfunctions.

## Other information

Sometimes power and telecommunications cabling are shared resources for more than one organization occupying co-located premises.

### 7.13 Equipment maintenance (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

## Control

Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

## Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

## Guidance

The following guidelines for equipment maintenance should be considered:

- a) maintaining equipment in accordance with the supplier's recommended service frequency and specifications;
- b) implementing and monitoring of a maintenance programme by the organization;
- c) only authorized maintenance personnel carrying out repairs and maintenance on equipment;

- d) keeping records of all suspected or actual faults, and of all preventive and corrective maintenance;
- e) implementing appropriate controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; subjecting the maintenance personnel to a suitable confidentiality agreement;
- f) supervising maintenance personnel when carrying out maintenance on site;
- g) authorizing and controlling access for remote maintenance;
- h) applying security measures for assets off-premises (see [7.9](#)) if equipment containing information is taken off premises for maintenance;
- i) complying with all maintenance requirements imposed by insurance;
- j) before putting equipment back into operation after maintenance, inspecting it to ensure that the equipment has not been tampered with and is functioning properly;
- k) applying measures for secure disposal or re-use of equipment (see [7.14](#)) if it is determined that equipment is to be disposed of.

## Other information

Equipment includes technical components of information processing facilities, uninterruptible power supply (UPS) and batteries, power generators, power alternators and converters, physical intrusion detection systems and alarms, smoke detectors, fire extinguishers, air conditioning and lifts.

## 7.14 Secure disposal or re-use of equipment ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

### Control

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

### Purpose

To prevent leakage of information from equipment to be disposed or re-used.

### Guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function. See [7.10](#) for detailed guidance on secure disposal of storage media and [8.10](#) for guidance on information deletion.

Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

The organization should consider the removal of security controls such as access controls or surveillance equipment at the end of lease or when moving out of premises. This depends on factors such as:

- a) its lease agreement to return the facility to original condition;
- b) minimizing the risk of leaving systems with sensitive information on them for the next tenant (e.g. user access lists, video or image files);

- c) the ability to reuse the controls at the next facility.

### Other information

Damaged equipment containing storage media can require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

- the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files);
- the cryptographic keys are long enough to resist brute force attacks;
- the cryptographic keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on cryptography, see [8.24](#).

Techniques for securely overwriting storage media differ according to the storage media technology and the classification level of the information on the storage media. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

See ISO/IEC 27040 for detail on methods for sanitizing storage media.

## 8 Technological controls [\(FI\)](#)

### 8.1 User endpoint devices [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

#### Control

Information stored on, processed by or accessible via user endpoint devices should be protected.

#### Purpose

To protect information against the risks introduced by using user endpoint devices.

#### Guidance

##### General

The organization should establish a topic-specific policy on secure configuration and handling of user endpoint devices. The topic-specific policy should be communicated to all relevant personnel and consider the following:

- the type of information and the classification level that the user endpoint devices can handle, process, store or support;
- registration of user endpoint devices;
- requirements for physical protection;
- restriction of software installation (e.g. remotely controlled by system administrators);
- requirements for user endpoint device software (including software versions) and for applying updates (e.g. active automatic updating);

- f) rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);
- g) access controls;
- h) storage device encryption;
- i) protection against malware;
- j) remote disabling, deletion or lockout;
- k) backups;
- l) usage of web services and web applications;
- m) end user behaviour analytics (see [8.16](#));
- n) the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g. USB ports);
- o) the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organization's information and other associated assets (e.g. software) from other information and other associated assets on the device.

Consideration should be given as to whether certain information is so sensitive that it can only be accessed via user endpoint devices, but not stored on such devices. In such cases, additional technical safeguards can be required on the device. For example, ensuring that downloading files for offline working is disabled and that local storage such as SD card is disabled.

As far as possible, the recommendations on this control should be enforced through configuration management (see [8.9](#)) or automated tools.

#### User responsibility

All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures. Users should be advised to:

- a) log-off active sessions and terminate services when no longer needed;
- b) protect user endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use; not leave devices carrying important, sensitive or critical business information unattended;
- c) use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);
- d) physically protect user endpoint devices against theft (e.g. in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure taking into account legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organization should be established for cases of theft or loss of user endpoint devices.

#### Use of personal devices

Where the organization allows the use of personal devices (sometimes known as BYOD), in addition to the guidance given in this control, the following should be considered:

- a) separation of personal and business use of the devices, including using software to support such separation and protect business data on a private device;
- b) providing access to business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of

- data by the organization in case of theft or loss of the device or when no longer authorized to use the service. In such cases, PII protection legislation should be considered;
- c) topic-specific policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
  - d) access to privately owned equipment (to verify the security of the machine or during an investigation), which can be prevented by legislation;
  - e) software licensing agreements that are such that organizations can become liable for licensing for client software on user endpoint devices owned privately by personnel or external party users.

### Wireless connections

The organization should establish procedures for:

- a) the configuration of wireless connections on devices (e.g. disabling vulnerable protocols);
- b) using wireless or wired connections with appropriate bandwidth in accordance with relevant topic-specific policies (e.g. because backups or software updates are needed).

### **Other information**

Controls to protect information on user endpoint devices depend on whether the user endpoint device is used only inside of the organization's secured premises and network connections, or whether it is exposed to increased physical and network related threats outside of the organization.

The wireless connections for user endpoint devices are similar to other types of network connections but have important differences that should be considered when identifying controls. In particular, back-up of information stored on user endpoint devices can sometimes fail because of limited network bandwidth or because user endpoint devices are not connected at the times when backups are scheduled.

For some USB ports, such as USB-C, disabling the USB port is not possible because it is used for other purposes (e.g. power delivery and display output).

## **8.2 Privileged access rights (FI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

### **Control**

The allocation and use of privileged access rights should be restricted and managed.

### **Purpose**

To ensure only authorized users, software components and services are provided with privileged access rights.

### **Guidance**

The allocation of privileged access rights should be controlled through an authorization process in accordance with the relevant topic-specific policy on access control (see [5.15](#)). The following should be considered:

- a) identifying users who need privileged access rights for each system or process (e.g. operating systems, database management systems and applications);
- b) allocating privileged access rights to users as needed and on an event-by-event basis in line with the topic-specific policy on access control (see [5.15](#)) (i.e. only to individuals with the necessary competence

- to carry out activities that require privileged access and based on the minimum requirement for their functional roles);
- c) maintaining an authorization process (i.e. determining who can approve privileged access rights, or not granting privileged access rights until the authorization process is complete) and a record of all privileges allocated;
  - d) defining and implementing requirements for expiry of privileged access rights;
  - e) taking measures to ensure that users are aware of their privileged access rights and when they are in privileged access mode. Possible measures include using specific user identities, user interface settings or even specific equipment;
  - f) authentication requirements for privileged access rights can be higher than the requirements for normal access rights. Re-authentication or authentication step-up can be necessary before doing work with privileged access rights;
  - g) regularly, and after any organizational change, reviewing users working with privileged access rights in order to verify if their duties, roles, responsibilities and competence still qualify them for working with privileged access rights (see [5.18](#));
  - h) establishing specific rules in order to avoid the use of generic administration user IDs (such as “root”), depending on systems’ configuration capabilities. Managing and protecting authentication information of such identities (see [5.17](#));
  - i) granting temporary privileged access just for the time window necessary to implement approved changes or activities (e.g. for maintenance activities or some critical changes), rather than permanently granting privileged access rights. This is often referred as break glass procedure, and often automated by privilege access management technologies;
  - j) logging all privileged access to systems for audit purposes;
  - k) not sharing or linking identities with privileged access rights to multiple persons, assigning each person a separate identity which allows assigning specific privileged access rights. Identities can be grouped (e.g. by defining an administrator group) in order to simplify the management of privileged access rights;
  - l) only using identities with privileged access rights for undertaking administrative tasks and not for day-to-day general tasks [i.e. checking email, accessing the web (users should have a separate normal network identity for these activities)].

### Other information

Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.

Inappropriate use of system administrator privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

More information related to access management and the secure management of access to information and information and communications technologies resources can be found in ISO/IEC 29146.

### 8.3 Information access restriction ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

## Control

Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

### Purpose

To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

### Guidance

Access to information and other associated assets should be restricted in accordance with the established topic-specific policies. The following should be considered in order to support access restriction requirements:

- a) not allowing access to sensitive information by unknown user identities or anonymously. Public or anonymous access should only be granted to storage locations that do not contain any sensitive information;
- b) providing configuration mechanisms to control access to information in systems, applications and services;
- c) controlling which data can be accessed by a particular user;
- d) controlling which identities or group of identities have which access, such as read, write, delete and execute;
- e) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

Further, dynamic access management techniques and processes to protect sensitive information that has high value to the organization should be considered when the organization:

- a) needs granular control over who can access such information during what period and in what way;
- b) wants to share such information with people outside the organization and maintain control over who can access it;
- c) wants to dynamically manage, in real-time, the use and distribution of such information;
- d) wants to protect such information against unauthorized changes, copying and distribution (including printing);
- e) wants to monitor the use of the information;
- f) wants to record any changes to such information that take place in case a future investigation is required.

Dynamic access management techniques should protect information throughout its life cycle (i.e. creation, processing, storage, transmission and disposal), including:

- a) establishing rules on the management of dynamic access based on specific use cases considering:
  - 1) granting access permissions based on identity, device, location or application;
  - 2) leveraging the classification scheme in order to determine what information needs to be protected with dynamic access management techniques;
- b) establishing operational, monitoring and reporting processes and supporting technical infrastructure.

Dynamic access management systems should protect information by:

- a) requiring authentication, appropriate credentials or a certificate to access information;

- b) restricting access, for example to a specified time frame (e.g. after a given date or until a particular date);
- c) using encryption to protect information;
- d) defining the printing permissions for the information;
- e) recording who accesses the information and how the information is used;
- f) raising alerts if attempts to misuse the information are detected.

### Other information

Dynamic access management techniques and other dynamic information protection technologies can support the protection of information even when data is shared beyond the originating organization, where traditional access controls cannot be enforced. It can be applied to documents, emails or other files containing information to limit who can access the content and in what way. It can be at a granular level and be adapted over the life cycle of the information.

Dynamic access management techniques do not replace classical access management [e.g. using access control lists (ACLs)], but can add more factors for conditionality, real-time evaluation, just-in-time data reduction and other enhancements that can be useful for the most sensitive information. It offers a way to control access outside the organization's environment. Incident response can be supported by dynamic access management techniques as permissions can be modified or revoked at any time.

Additional information on a framework for access management is provided in ISO/IEC 29146.

## 8.4 Access to source code [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection

### Control

Read and write access to source code, development tools and software libraries should be appropriately managed.

### Purpose

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.

### Guidance

Access to source code and associated items (such as designs, specifications, verification plans and validation plans) and development tools (e.g. compilers, builders, integration tools, test platforms and environments) should be strictly controlled.

For source code, this can be achieved by controlling central storage of such code, preferably in source code management system.

Read access and write access to source code can differ based on the personnel's role. For example, read access to source code can be broadly provided inside the organization, but write access to source code is only made available to privileged personnel or designated owners. Where code components are used by several developers within an organization, read access to a centralized code repository should be implemented. Furthermore, if open-source code or third-party code components are used inside an organization, read access to such external code repositories can be broadly provided. However, write access should still be restricted.

The following guidelines should be considered to control access to program source libraries in order to reduce the potential for corruption of computer programs:

- a) managing the access to program source code and the program source libraries according to established procedures;
- b) granting read and write access to source code based on business needs and managed to address risks of alteration or misuse and according to established procedures;
- c) updating of source code and associated items and granting of access to source code in accordance with change control procedures (see [8.32](#)) and only performing it after appropriate authorization has been received;
- d) not granting developers direct access to the source code repository, but through developer tools that control activities and authorizations on the source code;
- e) holding program listings in a secure environment, where read and write access should be appropriately managed and assigned;
- f) maintaining an audit log of all accesses and of all changes to source code.

If the program source code is intended to be published, additional controls to provide assurance on its integrity (e.g. digital signature) should be considered.

## Other information

If access to source code is not properly controlled, source code can be modified or some data in the development environment (e.g. copies of production data, configuration details) can be retrieved by unauthorized persons.

## 8.5 Secure authentication ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

### Control

Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

### Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

### Guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

The strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used.

Authentication information should be accompanied by additional authentication factors for accessing critical information systems (also known as multi-factor authentication). Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorized accesses. Multi-factor authentication can be combined with other techniques to require

additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

Biometric authentication information should be invalidated if it is ever compromised. Biometric authentication can be unavailable depending on the conditions of use (e.g. moisture or aging). To prepare for these issues, biometric authentication should be accompanied with at least one alternative authentication technique.

The procedure for logging into a system or application should be designed to minimize the risk of unauthorized access. Log-on procedures and technologies should be implemented considering the following:

- a) not displaying sensitive system or application information until the log-on process has been successfully completed in order to avoid providing an unauthorized user with any unnecessary assistance;
- b) displaying a general notice warning that the system or the application or the service should only be accessed by authorized users;
- c) not providing help messages during the log-on procedure that would aid an unauthorized user (e.g. if an error condition arises, the system should not indicate which part of the data is correct or incorrect);
- d) validating the log-on information only on completion of all input data;
- e) protecting against brute force log-on attempts on usernames and passwords [e.g. using completely automated public Turing test to tell computers and humans apart (CAPTCHA), requiring password reset after a predefined number of failed attempts or blocking the user after a maximum number of errors];
- f) logging unsuccessful and successful attempts;
- g) raising a security event if a potential attempted or successful breach of log-on controls is detected (e.g. sending an alert to the user and the organization's system administrators when a certain number of wrong password attempts has been reached);
- h) displaying or sending the following information on a separate channel on completion of a successful log-on:
  - 1) date and time of the previous successful log-on;
  - 2) details of any unsuccessful log-on attempts since the last successful log-on;
- i) not displaying a password in clear text when it is being entered; in some cases, it can be required to de-activate this functionality in order to facilitate user log-on (e.g. for accessibility reasons or to avoid blocking users because of repeated errors);
- j) not transmitting passwords in clear text over a network to avoid being captured by a network "sniffer" program;
- k) terminating inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on user endpoint devices;
- l) restricting connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

## Other information

Additional information on entity authentication assurance can be found in ISO/IEC 29115.

## 8.6 Capacity management (E1)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Integrity	#Identify #Protect	#Continuity	#Governance_and_Ecosystem
#Detective	#Availability	#Detect		#Protection

### Control

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

### Purpose

To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

### Guidance

Capacity requirements for information processing facilities, human resources, offices and other facilities should be identified, taking into account the business criticality of the concerned systems and processes.

System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems.

The organization should perform stress-tests of systems and services to confirm that sufficient system capacity is available to meet peak performance requirements.

Detective controls should be put in place to indicate problems in due time.

Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention should be paid to any resources with long procurement lead times or high costs. Therefore, managers, service or product owners should monitor the utilization of key system resources.

Managers should use capacity information to identify and avoid potential resource limitations and dependency on key personnel which can present a threat to system security or services and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. The following should be considered to increase capacity:

- a) hiring new personnel;
- b) obtaining new facilities or space;
- c) acquiring more powerful processing systems, memory and storage;
- d) making use of cloud computing, which has inherent characteristics that directly address issues of capacity. Cloud computing has elasticity and scalability which enable on-demand rapid expansion and reduction in resources available to particular applications and services.

The following should be considered to reduce demand on the organization's resources:

- a) deletion of obsolete data (disk space);
- b) disposal of hardcopy records that have met their retention period (free up shelving space);
- c) decommissioning of applications, systems, databases or environments;
- d) optimizing batch processes and schedules;

- e) optimizing application code or database queries;
- f) denying or restricting bandwidth for resource-consuming services if these are not critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

### Other information

For more detail on the elasticity and scalability of cloud computing, see ISO/IEC TS 23167.

## 8.7 Protection against malware [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

### Control

Protection against malware should be implemented and supported by appropriate user awareness.

### Purpose

To ensure information and other associated assets are protected against malware.

### Guidance

Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls. Use of malware detection and repair software alone is not usually adequate. The following guidance should be considered:

- a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)] (see [8.19](#) and [8.32](#));
- b) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting);
- c) reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management (see [8.8](#) and [8.19](#))];
- d) conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved files or unauthorized amendments;
- e) establishing protective measures against risks associated with obtaining files and software either from or via external networks or on any other medium;
- f) installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:
  - 1) scanning any data received over networks or via any form of electronic storage media, for malware before use;
  - 2) scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization;

- 3) scanning webpages for malware when accessed;
- g) determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:
- 1) defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices and servers;
  - 2) the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;
- h) taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;
- i) implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date. This can be necessary when the protection against malware causes disruption to normal operations;
- j) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery measures (see [8.13](#));
- k) isolating environments where catastrophic consequences can occur;
- l) defining procedures and responsibilities to deal with protection against malware on systems, including training in their use, reporting and recovering from malware attacks;
- m) providing awareness or training (see [6.3](#)) to all users on how to identify and potentially mitigate the receipt, sending or installation of malware infected emails, files or programs [the information collected in n) and o) can be used to ensure awareness and training are kept up-to-date];
- n) implementing procedures to regularly collect information about new malware, such as subscribing to mailing lists or reviewing relevant websites;
- o) verifying that information relating to malware, such as warning bulletins, comes from qualified and reputable sources (e.g. reliable internet sites or suppliers of malware detection software) and is accurate and informative.

## Other information

It is not always possible to install software that protects against malware on some systems (e.g. some industrial control systems). Some forms of malware infect computer operating systems and computer firmware such that common malware controls cannot clean the system and a full reimaging of the operating system software and sometimes the computer firmware is necessary to return to a secure state.

## 8.8 Management of technical vulnerabilities ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_vulnerability_management	#Governance_and_Ecosystem #Protection #Defence

### Control

Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

## Purpose

To prevent exploitation of technical vulnerabilities.

## Guidance

### Identifying technical vulnerabilities

The organization should have an accurate inventory of assets (see [5.9](#) to [5.14](#)) as a prerequisite for effective technical vulnerability management; the inventory should include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

To identify technical vulnerabilities, the organization should consider:

- a) defining and establishing the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, updating, asset tracking and any coordination responsibilities required;
- b) for software and other technologies (based on the asset inventory list, see [5.9](#)), identifying information resources that will be used for identifying relevant technical vulnerabilities and maintaining awareness about them. Updating the list of information resources based on changes in the inventory or when other new or useful resources are found;
- c) requiring suppliers of information system (including their components) to ensure vulnerability reporting, handling and disclosure, including the requirements in applicable contracts (see [5.20](#));
- d) using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;
- e) conducting planned, documented and repeatable penetration tests or vulnerability assessments by competent and authorized persons to support the identification of vulnerabilities. Exercising caution as such activities can lead to a compromise of the security of the system;
- f) tracking the usage of third-party libraries and source code for vulnerabilities. This should be included in secure coding (see [8.28](#)).

The organization should develop procedures and capabilities to:

- a) detect the existence of vulnerabilities in its products and services including any external component used in these;
- b) receive vulnerability reports from internal or external sources.

The organization should provide a public point of contact as part of a topic-specific policy on vulnerability disclosure so that researchers and others are able to report issues. The organization should establish vulnerability reporting procedures, online reporting forms and making use of appropriate threat intelligence or information sharing forums. The organization should also consider bug bounty programs where rewards are offered as an incentive to assist organizations in identifying vulnerabilities in order to appropriately remediate them. The organization should also share information with competent industry bodies or other interested parties.

### Evaluating technical vulnerabilities

To evaluate identified technical vulnerabilities, the following guidance should be considered:

- a) analyse and verify reports to determine what response and remediation activity is needed;
- b) once a potential technical vulnerability has been identified, identifying the associated risks and the actions to be taken. Such actions can involve updating vulnerable systems or applying other controls.

### Taking appropriate measures to address technical vulnerabilities

A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. If changes are necessary, the original software should be retained and the changes applied to a designated copy. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

The following guidance should be considered to address technical vulnerabilities:

- a) taking appropriate and timely action in response to the identification of potential technical vulnerabilities; defining a timeline to react to notifications of potentially relevant technical vulnerabilities;
- b) depending on how urgently a technical vulnerability needs to be addressed, carrying out the action according to the controls related to change management (see [8.32](#)) or by following information security incident response procedures (see [5.26](#));
- c) only using updates from legitimate sources (which can be internal or external to the organization);
- d) testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated [i.e. if an update is available, assessing the risks associated with installing the update (the risks posed by the vulnerability should be compared with the risk of installing the update)];
- e) addressing systems at high risk first;
- f) develop remediation (typically software updates or patches);
- g) test to confirm if the remediation or mitigation is effective;
- h) provide mechanisms to verify the authenticity of remediation;
- i) if no update is available or the update cannot be installed, considering other controls, such as:
  - 1) applying any workaround suggested by the software vendor or other relevant sources;
  - 2) turning off services or capabilities related to the vulnerability;
  - 3) adapting or adding access controls (e.g. firewalls) at network borders (see [8.20](#) to [8.22](#));
  - 4) shielding vulnerable systems, devices or applications from attack through deployment of suitable traffic filters (sometimes called virtual patching);
  - 5) increasing monitoring to detect actual attacks;
  - 6) raising awareness of the vulnerability.

For acquired software, if the vendors regularly release information about security updates for their software and provide a facility to install such updates automatically, the organization should decide whether to use the automatic update or not.

### Other considerations

An audit log should be kept for all steps undertaken in technical vulnerability management.

The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out in case an incident occurs.

Where the organization uses a cloud service supplied by a third-party cloud service provider, technical vulnerability management of cloud service provider resources should be ensured by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management should be part of the cloud service agreement and this should include processes for reporting the cloud service provider's actions relating to technical vulnerabilities (see [5.23](#)). For some cloud services, there are respective responsibilities for the cloud service provider and the cloud service customer. For example, the cloud service customer is responsible for vulnerability management of its own assets used for the cloud services.

## Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see [8.32](#)).

There is a possibility that an update does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling an update cannot be easily achieved once the update has been applied.

If adequate testing of the updates is not possible (e.g. because of costs or lack of resources) a delay in updating can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031 can be beneficial.

Where software patches or updates are produced, the organization can consider providing an automated update process where these updates are installed on affected systems or products without the need for intervention by the customer or the user. If an automated update process is offered, it can allow the customer or user to choose an option to turn off the automatic update or control the timing of the installation of the update.

Where the vendor provides an automated update process and the updates can be installed on affected systems or products without the need for intervention, the organization determines if it applies the automated process or not. One reason for not electing for automated update is to retain control over when the update is performed. For example, a software used for a business operation cannot be updated until the operation has completed.

A weakness with vulnerability scanning is that it is possible it does not fully account for defence in depth: two countermeasures that are always invoked in sequence can have vulnerabilities that are masked by strengths in the other. The composite countermeasure is not vulnerable, whereas a vulnerability scanner can report that both components are vulnerable. The organization should therefore take care in reviewing and acting on vulnerability reports.

Many organizations supply software, systems, products and services not only within the organization but also to interested parties such as customers, partners or other users. These software, systems, products and services can have information security vulnerabilities that affect the security of users.

Organizations can release remediation and disclose information about vulnerabilities to users (typically through a public advisory) and provide appropriate information for software vulnerability database services.

For more information relating to the management of technical vulnerabilities when using cloud computing, see the ISO/IEC 19086 series and ISO/IEC 27017.

ISO/IEC 29147 provides detailed information on receiving vulnerability reports and publishing vulnerability advisories. ISO/IEC 30111 provides detailed information about handling and resolving reported vulnerabilities.

## 8.9 Configuration management ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

## Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

## Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

## Guidance

### General

The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Roles, responsibilities and procedures should be in place to ensure satisfactory control of all configuration changes.

### Standard templates

Standard templates for the secure configuration of hardware, software, services and networks should be defined:

- a) using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations);
- b) considering the level of protection needed in order to determine a sufficient level of security;
- c) supporting the organization's information security policy, topic-specific policies, standards and other security requirements;
- d) considering the feasibility and applicability of security configurations in the organization's context.

The templates should be reviewed periodically and updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced.

The following should be considered for establishing standard templates for the secure configuration of hardware, software, services and networks:

- a) minimizing the number of identities with privileged or administrator level access rights;
- b) disabling unnecessary, unused or insecure identities;
- c) disabling or restricting unnecessary functions and services;
- d) restricting access to powerful utility programs and host parameter settings;
- e) synchronizing clocks;
- f) changing vendor default authentication information such as default passwords immediately after installation and reviewing other important default security-related parameters;
- g) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity;
- h) verifying that licence requirements have been met (see [5.32](#)).

### Managing configurations

Established configurations of hardware, software, services and networks should be recorded and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see [8.32](#)).

Configuration records can contain as relevant:

- a) up-to-date owner or point of contact information for the asset;
- b) date of the last change of configuration;
- c) version of configuration template;
- d) relation to configurations of other assets.

### Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

### **Other information**

Documentation for systems often records details about the configuration of both hardware and software.

System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling.

Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).

Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

## **8.10 Information deletion (FI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

### **Control**

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

### **Purpose**

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

### **Guidance**

#### General

Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.

When deleting information on systems, applications and services, the following should be considered:

- a) selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations;
- b) recording the results of deletion as evidence;
- c) when using service suppliers of information deletion, obtaining evidence of information deletion from them.

Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

#### Deletion methods

In accordance with the organization's topic-specific policy on data retention and taking into consideration relevant legislation and regulations, sensitive information should be deleted when no longer required, by:

- a) configuring systems to securely destroy information when no longer required (e.g. after a defined period subject to the topic-specific policy on data retention or by subject access request);
- b) deleting obsolete versions, copies and temporary files wherever they are located;
- c) using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools;
- d) using approved, certified providers of secure disposal services;
- e) using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives and other magnetic storage media).

Where cloud services are used, the organization should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, the organization should use it, or request that the cloud service provider delete the information. These deletion processes should be automated in accordance with topic-specific policies, when available and applicable. Depending on the sensitivity of information deleted, logs can track or verify that these deletion processes have happened.

To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information should be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises.

Considering that the secure deletion of some devices (e.g. smartphones) can only be achieved through destruction or using the functions embedded in these devices (e.g. "restore factory settings"), the organization should choose the appropriate method according to the classification of information handled by such devices.

Control measures described in [7.14](#) should be applied to physically destroy the storage device and simultaneously delete the information it contains.

An official record of information deletion is useful when analysing the cause of a possible information leakage event.

#### **Other information**

Information on user data deletion in cloud services can be found in ISO/IEC 27017.

Information on deletion of PII can be found in ISO/IEC 27555.

## 8.11 Data masking (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

### Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

### Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

### Guidance

Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as data masking, pseudonymization or anonymization.

Pseudonymization or anonymization techniques can hide PII, disguise the true identity of PII principals or other sensitive information, and disconnect the link between PII and the identity of the PII principal or the link between other sensitive information.

When using pseudonymization or anonymization techniques, it should be verified that data has been adequately pseudonymized or anonymized. Data anonymization should consider all the elements of the sensitive information to be effective. As an example, if not considered properly, a person can be identified even if the data that can directly identify that person is anonymised, by the presence of further data which allows the person to be identified indirectly.

Additional techniques for data masking include:

- a) encryption (requiring authorized users to have a key);
- b) nulling or deleting characters (preventing unauthorized users from seeing full messages);
- c) varying numbers and dates;
- d) substitution (changing one value for another to hide sensitive data);
- e) replacing values with their hash.

The following should be considered when implementing data masking techniques:

- a) not granting all users access to all data, therefore designing queries and masks in order to show only the minimum required data to the user;
- b) there are cases where some data should not be visible to the user for some records out of a set of data; in this case, designing and implementing a mechanism for obfuscation of data (e.g. if a patient does not want hospital staff to be able to see all of their records, even in case of emergency, then the hospital staff are presented with partially obfuscated data and data can only be accessed by staff with specific roles if it contains useful information for appropriate treatment);
- c) when data are obfuscated, giving the PII principal the possibility to require that users cannot see if the data are obfuscated (obfuscation of the obfuscation; this is used in health facilities, for example if the patient does not want personnel to see that sensitive information such as pregnancies or results of blood exams has been obfuscated);
- d) any legal or regulatory requirements (e.g. requiring the masking of payment cards' information during processing or storage).

The following should be considered when using data masking, pseudonymization or anonymization:

- a) level of strength of data masking, pseudonymization or anonymization according to the usage of the processed data;
- b) access controls to the processed data;
- c) agreements or restrictions on usage of the processed data;
- d) prohibiting collating the processed data with other information in order to identify the PII principal;
- e) keeping track of providing and receiving the processed data.

### Other information

Anonymization irreversibly alters PII in such a way that the PII principal can no longer be identified directly or indirectly.

Pseudonymization replaces the identifying information with an alias. Knowledge of the algorithm (sometimes referred to as the “additional information”) used to perform the pseudonymization allows for at least some form of identification of the PII principal. Such “additional information” should therefore be kept separate and protected.

While pseudonymization is therefore weaker than anonymization, pseudonymized datasets can be more useful in statistical research.

Data masking is a set of techniques to conceal, substitute or obfuscate sensitive data items. Data masking can be static (when data items are masked in the original database), dynamic (using automation and rules to secure data in real-time) or on-the-fly (with data masked in an application’s memory).

Hash functions can be used in order to anonymize PII. In order to prevent enumeration attacks, they should always be combined with a salt function.

PII in resource identifiers and their attributes [e.g. file names, uniform resource locators (URLs)] should be either avoided or appropriately anonymized.

Additional controls concerning the protection of PII in public clouds are given in ISO/IEC 27018.

Additional information on de-identification techniques is available in ISO/IEC 20889.

## 8.12 Data leakage prevention [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence
#Detective				

### Control

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

### Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

## Guidance

The organization should consider the following to reduce the risk of data leakage:

- a) identifying and classifying information to protect against leakage (e.g. personal information, pricing models and product designs);
- b) monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);
- c) acting to prevent information from leaking (e.g. quarantine emails containing sensitive information).

Data leakage prevention tools should be used to:

- a) identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);
- b) detect the disclosure of sensitive information (e.g. when information is uploaded to untrusted third-party cloud services or sent via email);
- c) block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

The organization should determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of the organization. If that is the case, the organization should implement technology such as data leakage prevention tools or the configuration of existing tools that allow users to view and manipulate data held remotely but prevent copy and paste outside of the organization's control.

If data export is required, the data owner should be allowed to approve the export and hold users accountable for their actions.

Taking screenshots or photographs of the screen should be addressed through terms and conditions of use, training and auditing.

Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

Data leakage prevention should also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial, scientific or any other) which can be of interest for espionage or can be critical for the community. The data leakage prevention actions should be oriented to confuse the adversary's decisions for example by replacing authentic information with false information, either as an independent action or as response to the adversary's intelligence actions. Examples of these kinds of actions are reverse social engineering or the use of honeypots to attract attackers.

## Other information

Data leakage prevention tools are designed to identify data, monitor data usage and movement, and take actions to prevent data from leaking (e.g. alerting users to their risky behaviour and blocking the transfer of data to portable storage devices).

Data leakage prevention inherently involves monitoring personnel's communications and online activities, and by extension external party messages, which raises legal concerns that should be considered prior to deploying data leakage prevention tools. There is a variety of legislation relating to privacy, data protection, employment, interception of data and telecommunications that is applicable to monitoring and data processing in the context of data leakage prevention.

Data leakage prevention can be supported by standard security controls, such as topic-specific policies on access control and secure document management (see [5.12](#) and [5.15](#)).

## 8.13 Information backup [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

### Control

Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

### Purpose

To enable recovery from loss of data or systems.

### Guidance

A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.

Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.

When designing a backup plan, the following items should be taken into consideration:

- a) producing accurate and complete records of the backup copies and documented restoration procedures;
- b) reflecting the business requirements of the organization (e.g. the recovery point objective, see [5.30](#)), the security requirements of the information involved and the criticality of the information to the continued operation of the organization in the extent (e.g. full or differential backup) and frequency of backups;
- c) storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- d) giving backup information an appropriate level of physical and environmental protection (see [Clause 7](#) and [8.1](#)) consistent with the standards applied at the main site;
- e) regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss;
- f) protecting backups by means of encryption according to the identified risks (e.g. in situations where confidentiality is of importance);
- g) taking care to ensure that inadvertent data loss is detected before backup is taken.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.

Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans (see [5.30](#)). This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan. In the case of critical systems and services, backup measures should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of the organization's information, applications and systems in the cloud service environment should be taken. The organization should determine if and

how requirements for backup are fulfilled when using the information backup service provided as part of the cloud service.

The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires and should take into consideration legislation and regulations.

### Other information

For further information on storage security including retention consideration, see ISO/IEC 27040.

## 8.14 Redundancy of information processing facilities [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

### Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

### Purpose

To ensure the continuous operation of information processing facilities.

### Guidance

The organization should identify requirements for the availability of business services and information systems. The organization should design and implement systems architecture with appropriate redundancy to meet these requirements.

Redundancy can be introduced by duplicating information processing facilities in part or in their entirety (i.e. spare components or having two of everything). The organization should plan and implement procedures for the activation of the redundant components and processing facilities. The procedures should establish if the redundant components and processing activities are always activated, or in case of emergency, automatically or manually activated. The redundant components and information processing facilities should ensure the same security level as the primary ones.

Mechanisms should be in place to alert the organization to any failure in the information processing facilities, enable executing the planned procedure and allow continued availability while the information processing facilities are repaired or replaced.

The organization should consider the following when implementing redundant systems:

- a) contracting with two or more suppliers of network and critical information processing facilities such as internet service providers;
- b) using redundant networks;
- c) using two geographically separate data centres with mirrored systems;
- d) using physically redundant power supplies or sources;
- e) using multiple parallel instances of software components, with automatic load balancing between them (between instances in the same data centre or in different data centres);
- f) having duplicated components in systems (e.g. CPU, hard disks, memories) or in networks (e.g. firewalls, routers, switches).

Where applicable, preferably in production mode, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

## Other information

There is a strong relationship between redundancy and ICT readiness for business continuity (see [5.30](#)) especially if short recovery times are required. Many of the redundancy measures can be part of the ICT continuity strategies and solutions.

The implementation of redundancies can introduce risks to the integrity (e.g. processes of copying data to duplicated components can introduce errors) or confidentiality (e.g. weak security control of duplicated components can lead to compromise) of information and information systems, which need to be considered when designing information systems.

Redundancy in information processing facilities does not usually address application unavailability due to faults within an application.

With the use of public cloud computing, it is possible to have multiple live versions of information processing facilities, existing in multiple separate physical locations with automatic failover and load balancing between them.

Some of the technologies and techniques for providing redundancy and automatic fail-over in the context of cloud services are discussed in ISO/IEC TS 23167.

## 8.15 Logging ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence

### Control

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.

### Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

### Guidance

#### General

The organization should determine the purpose for which logs are created, what data is collected and logged, and any log-specific requirements for protecting and handling the log data. This should be documented in a topic-specific policy on logging.

Event logs should include for each event, as applicable:

- a) user IDs;
- b) system activities;
- c) dates, times and details of relevant events (e.g. log-on and log-off);
- d) device identity, system identifier and location;
- e) network addresses and protocols.

The following events should be considered for logging:

- a) successful and rejected system access attempts;
- b) successful and rejected data and other resource access attempts;
- c) changes to system configuration;
- d) use of privileges;
- e) use of utility programs and applications;
- f) files accessed and the type of access, including deletion of important data files;
- g) alarms raised by the access control system;
- h) activation and de-activation of security systems, such as anti-virus systems and intrusion detection systems;
- i) creation, modification or deletion of identities;
- j) transactions executed by users in applications. In some cases, the applications are a service or product provided or run by a third party.

It is important for all systems to have synchronized time sources (see [8.17](#)) as this allows for correlation of logs between systems for analysis, alerting and investigation of an incident.

#### Protection of logs

Users, including those with privileged access rights, should not have permission to delete or de-activate logs of their own activities. They can potentially manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

- a) alterations to the message types that are recorded;
- b) log files being edited or deleted;
- c) failure to record events or over-writing of past recorded events if the storage media holding a log file is exceeded.

For protection of logs, the use of the following techniques should be considered: cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file.

Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence (see [5.28](#)).

Where the organization needs to send system or application logs to a vendor to assist with debugging or troubleshooting errors, logs should be de-identified where possible using data masking techniques (see [8.11](#)) for information such as usernames, internet protocol (IP) addresses, hostnames or organization name, before sending to the vendor.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see [5.34](#)).

#### Log analysis

Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behaviour, which can represent indicators of compromise.

Analysis of events should be performed by taking into account:

- a) the necessary skills for the experts performing the analysis;
- b) determining the procedure of log analysis;
- c) the required attributes of each security-related event;
- d) exceptions identified through the use of predetermined rules [e.g. security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures];
- e) known behaviour patterns and standard network traffic compared to anomalous activity and behaviour [user and entity behaviour analytics (UEBA)];
- f) results of trend or pattern analysis (e.g. as a result of using data analytics, big data techniques and specialized analysis tools);
- g) available threat intelligence.

Log analysis should be supported by specific monitoring activities to help identify and analyse anomalous behaviour, which includes:

- a) reviewing successful and unsuccessful attempts to access protected resources [e.g. domain name system (DNS) servers, web portals and file shares];
- b) checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers;
- c) examining usage reports from service providers (e.g. invoices or service reports) for unusual activity within systems and networks (e.g. by reviewing patterns of activity);
- d) including event logs of physical monitoring such as entrance and exit to ensure more accurate detection and incident analysis;
- e) correlating logs to enable efficient and highly accurate analysis.

Suspected and actual information security incidents should be identified (e.g. malware infection or probing of firewalls) and be subject to further investigation (e.g. as part of an information security incident management process, see [5.25](#)).

## Other information

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the use of suitable utility programs or audit tools to perform file interrogation can be considered.

Event logging sets the foundation for automated monitoring systems (see [8.16](#)) which are capable of generating consolidated reports and alerts on system security.

A SIEM tool or equivalent service can be used to store, correlate, normalize and analyse log information, and to generate alerts. SIEMs tend to require careful configuration to optimize their benefits.

Configurations to consider include identification and selection of appropriate log sources, tuning and testing of rules and development of use cases.

Public transparency files for the recording of logs are used, for example, in certificate transparency systems. Such files can provide an additional detection mechanism useful for guarding against log tampering.

In cloud environments, log management responsibilities can be shared between the cloud service customer and the cloud service provider. Responsibilities vary depending on the type of cloud service being used. Further guidance can be found in ISO/IEC 27017.

## 8.16 Monitoring activities [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

### Control

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

### Purpose

To detect anomalous behaviour and potential information security incidents.

### Guidance

The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.

The following should be considered for inclusion within the monitoring system:

- a) outbound and inbound network, system and application traffic;
- b) access to systems, servers, networking equipment, monitoring system, critical applications, etc.;
- c) critical or admin level system and network configuration files;
- d) logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention];
- e) event logs relating to system and network activity;
- f) checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code);
- g) use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance.

The organization should establish a baseline of normal behaviour and monitor against this baseline for anomalies. When establishing a baseline, the following should be considered:

- a) reviewing utilization of systems at normal and peak periods;
- b) usual time of access, location of access, frequency of access for each user or group of users.

The monitoring system should be configured against the established baseline to identify anomalous behaviour, such as:

- a) unplanned termination of processes or applications;
- b) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers);
- c) known attack characteristics (e.g. denial of service and buffer overflows);
- d) unusual system behaviour (e.g. keystroke logging, process injection and deviations in use of standard protocols);
- e) bottlenecks and overloads (e.g. network queuing, latency levels and network jitter);
- f) unauthorized access (actual or attempted) to systems or information;
- g) unauthorized scanning of business applications, systems and networks;

- 
- h) successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems);
  - i) unusual user and system behaviour in relation to expected behaviour.

Continuous monitoring via a monitoring tool should be used. Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. Monitoring tools should include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools should also be able to recognize specific signatures and data or network or application behaviour patterns.

Automated monitoring software should be configured to generate alerts (e.g. via management consoles, email messages or instant messaging systems) based on predefined thresholds. The alerting system should be tuned and trained on the organization's baseline to minimize false positives. Personnel should be dedicated to respond to alerts and should be properly trained to accurately interpret potential incidents. There should be redundant systems and processes in place to receive and respond to alert notifications.

Abnormal events should be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring (see [5.25](#)). Procedures should be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events (see [5.26](#)) on information security. Procedures should also be established to identify and address false positives including tuning the monitoring software to reduce the number of future false positives.

## Other information

Security monitoring can be enhanced by:

- a) leveraging threat intelligence systems (see [5.7](#));
- b) leveraging machine learning and artificial intelligence capabilities;
- c) using blocklists or allowlists;
- d) undertaking a range of technical security assessments (e.g. vulnerability assessments, penetration testing, cyber-attack simulations and cyber response exercises), and using the results of these assessments to help determine baselines or acceptable behaviour;
- e) using performance monitoring systems to help establish and detect anomalous behaviour;
- f) leveraging logs in combination with monitoring systems.

Monitoring activities are often conducted using specialist software, such as intrusion detection systems. These can be configured to a baseline of normal, acceptable and expected system and network activities.

Monitoring for anomalous communications helps in the identification of botnets (i.e. set of devices under the malicious control of the botnet owner, usually used for mounting distributed denial of service attacks on other computers of other organizations). If the computer is being controlled by an external device, there is a communication between the infected device and the controller. The organization should therefore employ technologies to monitor for anomalous communications and take such action as necessary.

## 8.17 Clock synchronization ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

### Control

The clocks of information processing systems used by the organization should be synchronized to approved time sources.

## Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

## Guidance

External and internal requirements for time representation, reliable synchronization and accuracy should be documented and implemented. Such requirements can be from legal, statutory, regulatory, contractual, standards and internal monitoring needs. A standard reference time for use within the organization should be defined and considered for all systems, including building management systems, entry and exit systems and others that can be used to aid investigations.

A clock linked to a radio time broadcast from a national atomic clock or global positioning system (GPS) should be used as the reference clock for logging systems; a consistent, trusted date and time source to ensure accurate time-stamps. Protocols such as network time protocol (NTP) or precision time protocol (PTP) should be used to keep all networked systems in synchronization with a reference clock.

The organization can use two external time sources at the same time in order to improve the reliability of external clocks, and appropriately manage any variance.

Clock synchronization can be difficult when using multiple cloud services or when using both cloud and on-premises services. In this case, the clock of each service should be monitored and the difference recorded in order to mitigate risks arising from discrepancies.

## Other information

The correct setting of computer clocks is important to ensure the accuracy of event logs, which can be required for investigations or as evidence in legal and disciplinary cases. Inaccurate audit logs can hinder such investigations and damage the credibility of such evidence.

## 8.18 Use of privileged utility programs ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

## Control

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

## Purpose

To ensure the use of utility programs does not harm system and application controls for information security.

## Guidance

The following guidelines for the use of utility programs that can be capable of overriding system and application controls should be considered:

- a) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see [8.2](#));
- b) use of identification, authentication and authorization procedures for utility programs, including unique identification of the person who uses the utility program;
- c) defining and documenting of authorization levels for utility programs;

- d) authorization for ad hoc use of utility programs;
- e) not making utility programs available to users who have access to applications on systems where segregation of duties is required;
- f) removing or disabling all unnecessary utility programs;
- g) at a minimum, logical segregation of utility programs from application software. Where practical, segregating network communications for such programs from application traffic;
- h) limitation of the availability of utility programs (e.g. for the duration of an authorized change);
- i) logging of all use of utility programs.

### Other information

Most information systems have one or more utility programs that can be capable of overriding system and application controls, for example diagnostics, patching, antivirus, disk defragmenters, debuggers, backup and network tools.

## 8.19 Installation of software on operational systems ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection

### Control

Procedures and measures should be implemented to securely manage software installation on operational systems.

### Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

### Guidance

The following guidelines should be considered to securely manage changes and installation of software on operational systems:

- a) performing updates of operational software only by trained administrators upon appropriate management authorization (see [8.5](#));
- b) ensuring that only approved executable code and no development code or compilers is installed on operational systems;
- c) only installing and updating software after extensive and successful testing (see [8.29](#) and [8.31](#));
- d) updating all corresponding program source libraries;
- e) using a configuration control system to keep control of all operational software as well as the system documentation;
- f) defining a rollback strategy before changes are implemented;
- g) maintaining an audit log of all updates to operational software;
- h) archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release (e.g. the introduction of new information security functionality or the number and severity of information security vulnerabilities affecting the current version). Software patches should be applied when they can help to remove or reduce information security vulnerabilities (see [8.8](#) and [8.19](#)).

Computer software can rely on externally supplied software and packages (e.g. software programs using modules which are hosted on external sites), which should be monitored and controlled to avoid unauthorized changes, because they can introduce information security vulnerabilities.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software. Open source software used in operational systems should be maintained to the latest appropriate release of the software. Over time, open source code can cease to be maintained but is still available in an open source software repository. The organization should also consider the risks of relying on unmaintained open source software when used in operational systems.

When suppliers are involved in installing or updating software, physical or logical access should only be given when necessary and with appropriate authorization. The supplier's activities should be monitored (see [5.22](#)).

The organization should define and enforce strict rules on which types of software users can install.

The principle of least privilege should be applied to software installation on operational systems. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted based on the roles of the users concerned.

### Other information

No other information.

## 8.20 Networks security ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

### Control

Networks and network devices should be secured, managed and controlled to protect information in systems and applications.

### Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network.

### Guidance

Controls should be implemented to ensure the security of information in networks and to protect connected services from unauthorized access. In particular, the following items should be considered:

- a) the type and classification level of information that the network can support;
- b) establishing responsibilities and procedures for the management of networking equipment and devices;

- c) maintaining up to date documentation including network diagrams and configuration files of devices (e.g. routers, switches);
- d) separating operational responsibility for networks from ICT system operations where appropriate (see [5.3](#));
- e) establishing controls to safeguard the confidentiality and integrity of data passing over public networks, third-party networks or over wireless networks and to protect the connected systems and applications (see [5.22](#), [8.24](#), [5.14](#) and [6.6](#)). Additional controls can also be required to maintain the availability of the network services and computers connected to the network;
- f) appropriately logging and monitoring to enable recording and detection of actions that can affect, or are relevant to, information security (see [8.16](#) and [8.15](#));
- g) closely coordinating network management activities both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;
- h) authenticating systems on the network;
- i) restricting and filtering systems connection to the network (e.g. using firewalls);
- j) detecting, restricting and authenticating the connection of equipment and devices to the network;
- k) hardening of network devices;
- l) segregating network administration channels from other network traffic;
- m) temporarily isolating critical subnetworks (e.g. with drawbridges) if the network is under attack;
- n) disabling vulnerable network protocols.

The organization should ensure that appropriate security controls are applied to the use of virtualized networks. Virtualized networks also cover software-defined networking (SDN, SD-WAN). Virtualized networks can be desirable from a security viewpoint, since they can permit logical separation of communication taking place over physical networks, particularly for systems and applications that are implemented using distributed computing.

### Other information

Additional information on network security can be found in the ISO/IEC 27033 series.

More information concerning virtualized networks can be found in ISO/IEC TS 23167.

## 8.21 Security of network services [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

### Control

Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.

### Purpose

To ensure security in the use of network services.

## Guidance

The security measures necessary for particular services, such as security features, service levels and service requirements, should be identified and implemented (by internal or external network service providers). The organization should ensure that network service providers implement these measures.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored. The right to audit should be agreed between the organization and the provider. The organization should also consider third-party attestations provided by service providers to demonstrate they maintain appropriate security measures.

Rules on the use of networks and network services should be formulated and implemented to cover:

- a) the networks and network services which are allowed to be accessed;
- b) authentication requirements for accessing various network services;
- c) authorization procedures for determining who is allowed to access which networks and networked services;
- d) network management and technological controls and procedures to protect access to network connections and network services;
- e) the means used to access networks and network services [e.g. use of virtual private network (VPN) or wireless network];
- f) time, location and other attributes of the user at the time of the access;
- g) monitoring of the use of network services.

The following security features of network services should be considered:

- a) technology applied for security of network services, such as authentication, encryption and network connection controls;
- b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
- c) caching (e.g. in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements;
- d) procedures for the network service usage to restrict access to network services or applications, where necessary.

## Other information

Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

More guidance on a framework for access management is given in ISO/IEC 29146.

### 8.22 Segregation of networks [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

## Control

Groups of information services, users and information systems should be segregated in the organization's networks.

### Purpose

To split the network in security boundaries and to control traffic between them based on business needs.

### Guidance

The organization should consider managing the security of large networks by dividing them into separate network domains and separating them from the public network (i.e. internet). The domains can be chosen based on levels of trust, criticality and sensitivity (e.g. public access domain, desktop domain, server domain, low- and high-risk systems), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks.

The perimeter of each domain should be well-defined. If access between network domains is allowed, it should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the topic-specific policy on access control (see [5.15](#)), access requirements, value and classification of information processed and take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly-defined network perimeter. Radio coverage adjustment should be considered for segregation of wireless networks. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls (see [8.20](#)) before granting access to internal systems. Wireless access network for guests should be segregated from those for personnel if personnel only use controlled user endpoint devices compliant to the organization's topic-specific policies. WiFi for guests should have at least the same restrictions as WiFi for personnel, in order to discourage the use of guest WiFi by personnel.

### Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

## 8.23 Web filtering (EI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

## Control

Access to external websites should be managed to reduce exposure to malicious content.

### Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

## Guidance

The organization should reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material. A technique for achieving this works by blocking the IP address or domain of the website(s) concerned. Some browsers and anti-malware technologies do this automatically or can be configured to do so.

The organization should identify the types of websites to which personnel should or should not have access. The organization should consider blocking access to the following types of websites:

- a) websites that have an information upload function unless permitted for valid business reasons;
- b) known or suspected malicious websites (e.g. those distributing malware or phishing contents);
- c) command and control servers;
- d) malicious website acquired from threat intelligence (see [5.7](#));
- e) websites sharing illegal content.

Prior to deploying this control, the organization should establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. The rules should be kept up-to-date.

Training should be given to personnel on the secure and appropriate use of online resources including access to the web. The training should include the organization's rules, contact point for raising security concerns, and exception process when restricted web resources need to be accessed for legitimate business reasons. Training should also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.

## Other information

Web filtering can include a range of techniques including signatures, heuristics, list of acceptable websites or domains, list of prohibited websites or domains and bespoke configuration to help prevent malicious software and other malicious activity from attacking the organization's network and systems.

### 8.24 Use of cryptography ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

## Control

Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

## Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

## Guidance

### General

When using cryptography, the following should be considered:

- a) the topic-specific policy on cryptography defined by the organization, including the general principles for the protection of information. A topic-specific policy on the use of cryptography is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use;
- b) identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms required;
- c) the use of cryptography for protection of information held on mobile user endpoint devices or storage media and transmitted over networks to such devices or storage media;
- d) the approach to key management, including methods to deal with the generation and protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;
- e) roles and responsibilities for:
  - 1) the implementation of the rules for the effective use of cryptography;
  - 2) the key management, including key generation (see [8.24](#));
- f) the standards to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices that are approved or required for use in the organization;
- g) the impact of using encrypted information on controls that rely on content inspection (e.g. malware detection or content filtering).

When implementing the organization's rules for effective use of cryptography, the regulations and national restrictions that can apply to the use of cryptographic techniques in different parts of the world should be taken into consideration as well as the issues of trans-border flow of encrypted information (see [5.31](#)).

The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g. with a certification authority) should cover issues of liability, reliability of services and response times for the provision of services (see [5.22](#)).

### Key management

Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

- a) generating keys for different cryptographic systems and different applications;
- b) issuing and obtaining public key certificates;
- c) distributing keys to intended entities, including how to activate keys when received;
- d) storing keys, including how authorized users obtain access to keys;
- e) changing or updating keys including rules on when to change keys and how this will be done;
- f) dealing with compromised keys;
- g) revoking keys including how to withdraw or deactivate keys [e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived)];
- h) recovering keys that are lost or corrupted;

- i) backing up or archiving keys;
- j) destroying keys;
- k) logging and auditing of key management related activities;
- l) setting activation and deactivation dates for keys so that the keys can only be used for the period of time according to the organization's rules on key management;
- m) handling legal requests for access to cryptographic keys (e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case).

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

In addition to integrity, for many use cases, the authenticity of public keys should also be considered.

### Other information

The authenticity of public keys is usually addressed by public key management processes using certificate authorities and public key certificates, but it is also possible to address it by using technologies such as applying manual processes for small number keys.

Cryptography can be used to achieve different information security objectives, for example:

- a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;
- c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
- d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

The ISO/IEC 11770 series provides further information on key management.

## 8.25 Secure development life cycle (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

### Control

Rules for the secure development of software and systems should be established and applied.

### Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

## Guidance

Secure development is a requirement to build up a secure service, architecture, software and system. To achieve this, the following aspects should be considered:

- a) separation of development, test and production environments (see [8.31](#));
- b) guidance on the security in the software development life cycle:
  - 1) security in the software development methodology (see [8.28](#) and [8.27](#));
  - 2) secure coding guidelines for each programming language used (see [8.28](#));
- c) security requirements in the specification and design phase (see [5.8](#));
- d) security checkpoints in projects (see [5.8](#));
- e) system and security testing, such as regression testing, code scan and penetration tests (see [8.29](#));
- f) secure repositories for source code and configuration (see [8.4](#) and [8.9](#));
- g) security in the version control (see [8.32](#));
- h) required application security knowledge and training (see [8.28](#));
- i) developers' capability for preventing, finding and fixing vulnerabilities (see [8.28](#));
- j) licensing requirements and alternatives to ensure cost-effective solutions while avoiding future licensing issues (See [5.32](#)).

If development is outsourced, the organization should obtain assurance that the supplier complies with the organization's rules for secure development (see [8.30](#)).

## Other information

Development can also take place inside applications, such as office applications, scripting, browsers and databases.

## 8.26 Application security requirements ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence

## Control

Information security requirements should be identified, specified and approved when developing or acquiring applications.

## Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications.

## Guidance

### General

Application security requirements should be identified and specified. These requirements are usually determined through a risk assessment. The requirements should be developed with the support of information security specialists.

Application security requirements can cover a wide range of topics, depending on the purpose of the application.

Application security requirements should include, as applicable:

- a) level of trust in identity of entities [e.g. through authentication (see [5.17](#), [8.2](#) and [8.5](#))];
- b) identifying the type of information and classification level to be processed by the application;
- c) need for segregation of access and level of access to data and functions in the application;
- d) resilience against malicious attacks or unintentional disruptions [e.g. protection against buffer overflow or structured query language (SQL) injections];
- e) legal, statutory and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed or stored;
- f) need for privacy associated with all parties involved;
- g) the protection requirements of any confidential information;
- h) protection of data while being processed, in transit and at rest;
- i) need to securely encrypt communications between all involved parties;
- j) input controls, including integrity checks and input validation;
- k) automated controls (e.g. approval limits or dual approvals);
- l) output controls, also considering who can access outputs and its authorization;
- m) restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data (e.g. personal data);
- n) requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements;
- o) requirements mandated by other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
- p) error message handling.

#### Transactional services

Additionally, for applications offering transactional services between the organization and a partner, the following should be considered when identifying information security requirements:

- a) the level of trust each party requires in each other's claimed identity;
- b) the level of trust required in the integrity of information exchanged or processed and the mechanisms for identification of lack of integrity (e.g. cyclic redundancy check, hashing, digital signatures);
- c) authorization processes associated with who can approve contents of, issue or sign key transactional documents;
- d) confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation (e.g. contracts associated with tendering and contract processes);
- e) the confidentiality and integrity of any transactions (e.g. orders, delivery address details and confirmation of receipts);
- f) requirements on how long to maintain a transaction confidential;
- g) insurance and other contractual requirements.

### Electronic ordering and payment applications

Additionally, for applications involving electronic ordering and payment, the following should be considered:

- a) requirements for maintaining the confidentiality and integrity of order information;
- b) the degree of verification appropriate to verify payment information supplied by a customer;
- c) avoidance of loss or duplication of transaction information;
- d) storing transaction details outside of any publicly accessible environment (e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on electronic storage media directly accessible from the internet);
- e) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate or signature management process.

Several of the above considerations can be addressed by the application of cryptography (see [8.24](#)), taking into consideration legal requirements (see [5.31](#) to [5.36](#), especially see [5.31](#) for cryptography legislation).

### **Other information**

Applications accessible via networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public; incomplete transmission, mis-routing, unauthorized message alteration, duplication or replay. Therefore, detailed risk assessments and careful determination of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Further information on application security can be found in the ISO/IEC 27034 series.

## **8.27 Secure system architecture and engineering principles (FI)**

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

### **Control**

Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.

### **Purpose**

To ensure information systems are securely designed, implemented and operated within the development life cycle.

### **Guidance**

Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology). New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

Secure engineering principles provide guidance on user authentication techniques, secure session control and data validation and sanitisation.

Secure system engineering principles should include analysis of:

- a) the full range of security controls required to protect information and systems against identified threats;
- b) the capabilities of security controls to prevent, detect or respond to security events;
- c) specific security controls required by particular business processes (e.g. encryption of sensitive information, integrity checking and digitally signing information);
- d) where and how security controls are to be applied (e.g. by integrating with a security architecture and the technical infrastructure);
- e) how individual security controls (manual and automated) work together to produce an integrated set of controls.

Security engineering principles should take account of:

- a) the need to integrate with a security architecture;
- b) technical security infrastructure [e.g. public key infrastructure (PKI), identity and access management (IAM), data leakage prevention and dynamic access management];
- c) capability of the organization to develop and support the chosen technology;
- d) cost, time and complexity of meeting security requirements;
- e) current good practices.

Secure system engineering should involve:

- a) the use of security architecture principles, such as "security by design", "defence in depth", "security by default", "default deny", "fail securely", "distrust input from external applications", "security in deployment", "assume breach", "least privilege", "usability and manageability" and "least functionality";
- b) a security-oriented design review to help identify information security vulnerabilities, ensure security controls are specified and meet security requirements;
- c) documentation and formal acknowledgement of security controls that do not fully meet requirements (e.g. due to overriding safety requirements);
- d) hardening of systems.

The organization should consider "zero trust" principles such as:

- a) assuming the organization's information systems are already breached and thus not be reliant on network perimeter security alone;
- b) employing a "never trust and always verify" approach for access to information systems;
- c) ensuring that requests to information systems are encrypted end-to-end;
- d) verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e. not automatically trusting anything inside or outside its perimeters);
- e) using "least privilege" and dynamic access control techniques (see [5.15](#), [5.18](#) and [8.2](#)). This includes authenticating and authorizing requests for information or to systems based on contextual information such as authentication information (see [5.17](#)), user identities (see [5.16](#)), data about the user endpoint device, and data classification (see [5.12](#));
- f) always authenticating requesters and always validating authorization requests to information systems based on information including authentication information (see [5.17](#)) and user identities ([5.16](#)), data about the user endpoint device, and data classification (see [5.12](#)), for example enforcing strong authentication (e.g. multi-factor, see [8.5](#)).

The established security engineering principles should be applied, where applicable, to outsourced development of information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should ensure that suppliers' security engineering practices align with the organization's needs.

The security engineering principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up-to-date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

## Other information

Secure engineering principles can be applied to the design or configuration of a range of techniques, such as:

- fault tolerance and other resilience techniques;
- segregation (e.g. through virtualization or containerization);
- tamper resistance.

Secure virtualization techniques can be used to prevent interference between applications running on the same physical device. If a virtual instance of an application is compromised by an attacker, only that instance is affected. The attack has no effect on any other application or data.

Tamper resistance techniques can be used to detect tampering of information containers, whether physical (e.g. a burglar alarm) or logical (e.g. a data file). A characteristic of such techniques is that there is a record of the attempt to tamper with the container. In addition, the control can prevent the successful extraction of data through its destruction (e.g. device memory can be deleted).

## 8.28 Secure coding (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

### Control

Secure coding principles should be applied to software development.

### Purpose

To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

### Guidance

#### General

The organization should establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied. Additionally, such processes and governance should be extended to cover software components from third parties and open source software.

The organization should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the organization's secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape.

### Planning and before coding

Secure coding principles should be used both for new developments and in reuse scenarios. These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others. Planning and prerequisites before coding should include:

- a) organization-specific expectations and approved principles for secure coding to be used for both in-house and outsourced code developments;
- b) common and historical coding practices and defects that lead to information security vulnerabilities;
- c) configuring development tools, such as integrated development environments (IDE), to help enforce the creation of secure code;
- d) following guidance issued by the providers of development tools and execution environments as applicable;
- e) maintenance and use of updated development tools (e.g. compilers);
- f) qualification of developers in writing secure code;
- g) secure design and architecture, including threat modelling;
- h) secure coding standards and where relevant mandating their use;
- i) use of controlled environments for development.

### During coding

Considerations during coding should include:

- a) secure coding practices specific to the programming languages and techniques being used;
- b) using secure programming techniques, such as pair programming, refactoring, peer review, security iterations and test-driven development;
- c) using structured programming techniques;
- d) documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;
- e) prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords, unapproved code samples and unauthenticated web services).

Testing should be conducted during and after development (see [8.29](#)). Static application security testing (SAST) processes can identify security vulnerabilities in software.

Before software is made operational, the following should be evaluated:

- a) attack surface and the principle of least privilege;
- b) conducting an analysis of the most common programming errors and documenting that these have been mitigated.

### Review and maintenance

After code has been made operational:

- a) updates should be securely packaged and deployed;
- b) reported information security vulnerabilities should be handled (see [8.8](#));
- c) errors and suspected attacks should be logged and logs regularly reviewed to make adjustments to the code as necessary;

- d) source code should be protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control).

If using external tools and libraries, the organization should consider:

- a) ensuring that external libraries are managed (e.g. by maintaining an inventory of libraries used and their versions) and regularly updated with release cycles;
- b) selection, authorization and reuse of well-vetted components, particularly authentication and cryptographic components;
- c) the licence, security and history of external components;
- d) ensuring that software is maintainable, tracked and originates from proven, reputable sources;
- e) sufficiently long-term availability of development resources and artefacts.

Where a software package needs to be modified the following points should be considered:

- a) the risk of built-in controls and integrity processes being compromised;
- b) whether to obtain the consent of the vendor;
- c) the possibility of obtaining the required changes from the vendor as standard program updates;
- d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes;
- e) compatibility with other software in use.

## Other information

A guiding principle is to ensure security-relevant code is invoked when necessary and is tamper-resistant. Programs installed from compiled binary code also have these properties but only for data held within the application. For interpreted languages, the concept only works when the code is executed on a server that is otherwise inaccessible by the users and processes that use it, and that its data is held in a similarly protected database. For example, the interpreted code can be run on a cloud service where access to the code itself requires administrator privileges. Such administrator access should be protected by security mechanisms such as just-in-time administration principles and strong authentication. If the application owner can access scripts by direct remote access to the server, so in principle can an attacker. Webservers should be configured to prevent directory browsing in such cases.

Application code is best designed on the assumption that it is always subject to attack, through error or malicious action. In addition, critical applications can be designed to be tolerant of internal faults. For example, the output from a complex algorithm can be checked to ensure that it lies within safe bounds before the data is used in an application such as a safety or financial critical application. The code that performs the boundary checks is simple and therefore much easier to prove correctness.

Some web applications are susceptible to a variety of vulnerabilities that are introduced by poor design and coding, such as database injection and cross-site scripting attacks. In these attacks, requests can be manipulated to abuse the webserver functionality.

More information on ICT security evaluation can be found in the ISO/IEC 15408 series.

## 8.29 Security testing in development and acceptance [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection

### Control

Security testing processes should be defined and implemented in the development life cycle.

### Purpose

To validate if information security requirements are met when applications or code are deployed to the production environment.

### Guidance

New information systems, upgrades and new versions should be thoroughly tested and verified during the development processes. Security testing should be an integral part of the testing for systems or components.

Security testing should be conducted against a set of requirements, which can be expressed as functional or non-functional. Security testing should include testing of:

- a) security functions [e.g. user authentication (see [8.5](#)), access restriction (see [8.3](#)) and use of cryptography (see [8.24](#))];
- b) secure coding (see [8.28](#));
- c) secure configurations (see [8.9](#), [8.20](#) and [8.22](#)) including that of operating systems, firewalls and other security components.

Test plans should be determined using a set of criteria. The extent of testing should be in proportion to the importance, nature of the system and the potential impact of the change being introduced. The test plan should include:

- a) detailed schedule of activities and tests;
- b) inputs and expected outputs under a range of conditions;
- c) criteria to evaluate the results;
- d) decision for further actions as necessary.

The organization can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken to ensure that the system works as expected and only as expected (see [5.8](#)). The following should be considered:

- a) performing code review activities as a relevant element for testing for security flaws, including unanticipated inputs and conditions;
- b) performing vulnerability scanning to identify insecure configurations and system vulnerabilities;
- c) performing penetration testing to identify insecure code and design.

For outsourced development and purchasing components, an acquisition process should be followed. Contracts with the supplier should address the identified security requirements (see [5.20](#)). Products and services should be evaluated against these criteria before acquisition.

Testing should be performed in a test environment that matches the target production environment as closely as possible to ensure that the system does not introduce vulnerabilities to the organization's environment and that the tests are reliable (see [8.31](#)).

## Other information

Multiple test environments can be established, which can be used for different kinds of testing (e.g. functional and performance testing). These different environments can be virtual, with individual configurations to simulate a variety of operating environments.

Testing and monitoring of test environments, tools and technologies also needs to be considered to ensure effective testing. The same considerations apply to monitoring of the monitoring systems deployed in development, test and production settings. Judgement is needed, guided by the sensitivity of the systems and data, to determine how many layers of meta-testing are useful.

## 8.30 Outsourced development (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection

### Control

The organization should direct, monitor and review the activities related to outsourced system development.

### Purpose

To ensure information security measures required by the organization are implemented in outsourced system development.

### Guidance

Where system development is outsourced, the organization should communicate and agree requirements and expectations, and continually monitor and review whether the delivery of outsourced work meets these expectations. The following points should be considered across the organization's entire external supply chain:

- a) licensing agreements, code ownership and intellectual property rights related to the outsourced content (see [5.32](#));
- b) contractual requirements for secure design, coding and testing practices (see [8.25](#) to [8.29](#));
- c) provision of the threat model to consider by external developers;
- d) acceptance testing for the quality and accuracy of the deliverables (see [8.29](#));
- e) provision of evidence that minimum acceptable levels of security and privacy capabilities are established (e.g. assurance reports);
- f) provision of evidence that sufficient testing has been applied to guard against the presence of malicious content (both intentional and unintentional) upon delivery;
- g) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

- h) escrow agreements for the software source code (e.g. if the supplier goes out of business);
- i) contractual right to audit development processes and controls;
- jj) security requirements for the development environment (see [8.31](#));
- k) taking consideration of applicable legislation (e.g. on protection of personal data).

#### Other information

Further information on supplier relationships can be found in the ISO/IEC 27036 series.

### 8.31 Separation of development, test and production environments ([FI](#))

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

#### Control

Development, testing and production environments should be separated and secured.

#### Purpose

To protect the production environment and data from compromise by development and test activities.

#### Guidance

The level of separation between production, testing and development environments that is necessary to prevent production problems should be identified and implemented.

The following items should be considered:

- a) adequately separating development and production systems and operating them in different domains (e.g. in separate virtual or physical environments);
- b) defining, documenting and implementing rules and authorization for the deployment of software from development to production status;
- c) testing changes to production systems and applications in a testing or staging environment prior to being applied to production systems (see [8.29](#));
- d) not testing in production environments except in circumstances that have been defined and approved;
- e) compilers, editors and other development tools or utility programs not being accessible from production systems when not required;
- f) displaying appropriate environment identification labels in menus to reduce the risk of error;
- g) not copying sensitive information into the development and testing system environments unless equivalent controls are provided for the development and testing systems.

In all cases, development and testing environments should be protected considering:

- a) patching and updating of all the development, integration and testing tools (including builders, integrators, compilers, configuration systems and libraries);
- b) secure configuration of systems and software;
- c) control of access to the environments;
- d) monitoring of change to the environment and code stored therein;

- e) secure monitoring of the environments;
- f) taking backups of the environments.

A single person should not have the ability to make changes to both development and production without prior review and approval. This can be achieved for example through segregation of access rights or through rules that are monitored. In exceptional situations, additional measures such as detailed logging and real-time monitoring should be implemented in order to detect and act on unauthorized changes.

### Other information

Without adequate measures and procedures, developers and testers having access to production systems can introduce significant risks (e.g. unwanted modification of files or system environment, system failure, running unauthorized and untested code in production systems, disclosure of confidential data, data integrity and availability issues). There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the production environment.

Measures and procedures include carefully designed roles in conjunction with implementing segregation of duty requirements and having adequate monitoring processes in place.

Development and testing personnel also pose a threat to the confidentiality of production information. Development and testing activities can cause unintended changes to software or information if they share the same computing environment. Separating development, testing and production environments is therefore desirable to reduce the risk of accidental change or unauthorized access to production software and business data (see [8.33](#) for the protection of test information).

In some cases, the distinction between development, test and production environments can be deliberately blurred and testing can be carried out in a development environment or through controlled rollouts to live users or servers (e.g. small population of pilot users). In some cases, product testing can occur through live use of the product inside the organization. Furthermore, to reduce downtime of live deployments, two identical production environments can be supported where only one is live at any one time.

Supporting processes for the use of production data in development and testing environments ([8.33](#)) are necessary.

Organizations can also consider the guidance provided in this section for training environments when conducting end user training.

## 8.32 Change management [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

### Control

Changes to information processing facilities and information systems should be subject to change management procedures.

### Purpose

To preserve information security when executing changes.

### Guidance

Introduction of new systems and major changes to existing systems should follow agreed rules and a formal process of documentation, specification, testing, quality control and managed implementation. Management responsibilities and procedures should be in place to ensure satisfactory control of all changes.

Change control procedures should be documented and enforced to ensure the confidentiality, integrity and availability of information in information processing facilities and information systems, for the entire system development life cycle from the early design stages through all subsequent maintenance efforts.

Wherever practicable, change control procedures for ICT infrastructure and software should be integrated.

The change control procedures should include:

- a) planning and assessing the potential impact of changes considering all dependencies;
- b) authorization of changes;
- c) communicating changes to relevant interested parties;
- d) tests and acceptance of tests for the changes (see [8.29](#));
- e) implementation of changes including deployment plans;
- f) emergency and contingency considerations including fall-back procedures;
- g) maintaining records of changes that include all of the above;
- h) ensuring that operating documentation (see [5.37](#)) and user procedures are changed as necessary to remain appropriate;
- i) ensuring that ICT continuity plans and response and recovery procedures (see [5.30](#)) are changed as necessary to remain appropriate.

### Other information

Inadequate control of changes to information processing facilities and information systems is a common cause of system or security failures. Changes to the production environment, especially when transferring software from development to operational environment, can impact on the integrity and availability of applications.

Changing software can impact the production environment and vice versa.

Good practice includes the testing of ICT components in an environment segregated from both the production and development environments (see [8.31](#)). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Production environment includes operating systems, databases and middleware platforms. The control should be applied for changes of applications and infrastructures.

### 8.33 Test information [\(FI\)](#)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

#### Control

Test information should be appropriately selected, protected and managed.

#### Purpose

To ensure relevance of testing and protection of operational information used for testing.

## Guidance

Test information should be selected to ensure the reliability of tests results and the confidentiality of the relevant operational information. Sensitive information (including personally identifiable information) should not be copied into the development and testing environments (see [8.31](#)).

The following guidelines should be applied to protect the copies of operational information, when used for testing purposes, whether the test environment is built in-house or on a cloud service:

- a) applying the same access control procedures to test environments as those applied to operational environments;
- b) having a separate authorization each time operational information is copied to a test environment;
- c) logging the copying and use of operational information to provide an audit trail;
- d) protecting sensitive information by removal or masking (see [8.11](#)) if used for testing;
- e) properly deleting (see [8.10](#)) operational information from a test environment immediately after the testing is complete to prevent unauthorized use of test information.

Test information should be securely stored (to prevent tampering, which can otherwise lead to invalid results) and only used for testing purposes.

## Other information

System and acceptance testing can require substantial volumes of test information that are as close as possible to operational information.

## 8.34 Protection of information systems during audit testing (FI)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

### Control

Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.

### Purpose

To minimize the impact of audit and other assurance activities on operational systems and business processes.

## Guidance

The following guidelines should be observed:

- a) agreeing audit requests for access to systems and data with appropriate management;
- b) agreeing and controlling the scope of technical audit tests;
- c) limiting audit tests to read-only access to software and data. If read-only access is not available to obtain the necessary information, executing the test by an experienced administrator who has the necessary access rights on behalf of the auditor;
- d) if access is granted, establishing and verifying the security requirements (e.g. antivirus and patching) of the devices used for accessing the systems (e.g. laptops or tablets) before allowing the access;
- e) only allowing access other than read-only for isolated copies of system files, deleting them when the audit is completed, or giving them appropriate protection if there is an obligation to keep such files under audit documentation requirements;
- f) identifying and agreeing on requests for special or additional processing, such as running audit tools;
- g) running audit tests that can affect system availability outside business hours;
- h) monitoring and logging all access for audit and test purposes.

## Other information

Audit tests and other assurance activities can also happen on development and test systems, where such tests can impact for example the integrity of code or lead to disclosure of any sensitive information held in such environments.

## Annex A (informative) Using attributes [\(FI\)](#)

### A.1 General [\(FI\)](#)

This annex provides a table to demonstrate the use of attributes as a way of creating different views of the controls. The five examples of attributes are (see [4.2](#)):

- a) Control types (#Preventive, #Detective, #Corrective)
- b) Information security properties (#Confidentiality, #Integrity, #Availability)
- c) Cybersecurity concepts (#Identify, #Protect, #Detect, #Respond, #Recover)
- d) Operational capabilities (#Governance, #Asset\_management, #Information\_protection, #Human\_resource\_security, #Physical\_security, #System\_and\_network\_security, #Application\_security, #Secure\_configuration, #Identity\_and\_access\_management, #Threat\_and\_vulnerability\_management, #Continuity, #Supplier\_relationships\_security, #Legal\_and\_compliance, #Information\_security\_event\_management, #Information\_security\_assurance)
- e) Security domains (#Governance\_and\_Ecosystem, #Protection, #Defence, #Resilience)

[Table A.1](#) contains a matrix of all controls in this document with their given attribute values.

The filtering or sorting of the matrix can be achieved by using a tool such as a simple spreadsheet or a database, which can include more information like control text, guidance, organization-specific guidance or attributes (see [A.2](#)).

**Table A.1 Matrix of controls and attribute values**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.1</a>	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
<a href="#">5.2</a>	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
<a href="#">5.3</a>	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem
<a href="#">5.4</a>	Management responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem
<a href="#">5.5</a>	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
<a href="#">5.6</a>	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.7</a>	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
<a href="#">5.8</a>	Information security in project management	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection
<a href="#">5.9</a>	Inventory of information and other associated assets	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection
<a href="#">5.10</a>	Acceptable use of information and other associated assets	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection
<a href="#">5.11</a>	Return of assets	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection
<a href="#">5.12</a>	Classification of information	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence
<a href="#">5.13</a>	Labelling of information	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_protection	#Defence #Protection
<a href="#">5.14</a>	Information transfer	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
<a href="#">5.15</a>	Access control	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">5.16</a>	Identity management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">5.17</a>	Authentication information	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">5.18</a>	Access rights	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">5.19</a>	Information security in supplier relationships	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
<a href="#">5.20</a>	Addressing information security within supplier agreements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
<a href="#">5.21</a>	Managing information security in the ICT supply chain	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.22</a>	Monitoring, review and change management of supplier services	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence
<a href="#">5.23</a>	Information security for use of cloud services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
<a href="#">5.24</a>	Information security incident management planning and preparation	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
<a href="#">5.25</a>	Assessment and decision on information security events	#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
<a href="#">5.26</a>	Response to information security incidents	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
<a href="#">5.27</a>	Learning from information security incidents	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence
<a href="#">5.28</a>	Collection of evidence	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
<a href="#">5.29</a>	Information security during disruption	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
<a href="#">5.30</a>	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience
<a href="#">5.31</a>	Legal, statutory, regulatory and contractual requirements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection
<a href="#">5.32</a>	Intellectual property rights	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem
<a href="#">5.33</a>	Protection of records	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.34</a>	Privacy and protection of PII	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection
<a href="#">5.35</a>	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
<a href="#">5.36</a>	Compliance with policies, rules and standards for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem
<a href="#">5.37</a>	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
<a href="#">6.1</a>	Screening	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
<a href="#">6.2</a>	Terms and conditions of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
<a href="#">6.3</a>	Information security awareness, education and training	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
<a href="#">6.4</a>	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem
<a href="#">6.5</a>	Responsibilities after termination or change of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">6.6</a>	Confidentiality or non-disclosure agreements	#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem
<a href="#">6.7</a>	Remote working	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection
<a href="#">6.8</a>	Information security event reporting	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence
<a href="#">7.1</a>	Physical security perimeters	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
<a href="#">7.2</a>	Physical entry	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection
<a href="#">7.3</a>	Securing offices, rooms and facilities	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
<a href="#">7.4</a>	Physical security monitoring	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence
<a href="#">7.5</a>	Protecting against physical and environmental threats	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
<a href="#">7.6</a>	Working in secure areas	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
<a href="#">7.7</a>	Clear desk and clear screen	#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection
<a href="#">7.8</a>	Equipment siting and protection	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
<a href="#">7.9</a>	Security of assets off-premises	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
<a href="#">7.10</a>	Storage media	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">7.11</a>	Supporting utilities	#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection
<a href="#">7.12</a>	Cabling security	#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection
<a href="#">7.13</a>	Equipment maintenance	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience
<a href="#">7.14</a>	Secure disposal or re-use of equipment	#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection
<a href="#">8.1</a>	User endpoint devices	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
<a href="#">8.2</a>	Privileged access rights	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">8.3</a>	Information access restriction	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">8.4</a>	Access to source code	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection
<a href="#">8.5</a>	Secure authentication	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
<a href="#">8.6</a>	Capacity management	#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_Ecosystem #Protection
<a href="#">8.7</a>	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence
<a href="#">8.8</a>	Management of technical vulnerabilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_vulnerability_management	#Governance_and_Ecosystem #Protection #Defence
<a href="#">8.9</a>	Configuration management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
<a href="#">8.10</a>	Information deletion	#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection
<a href="#">8.11</a>	Data masking	#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">8.12</a>	Data leakage prevention	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence
<a href="#">8.13</a>	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
<a href="#">8.14</a>	Redundancy of information processing facilities	#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience
<a href="#">8.15</a>	Logging	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence
<a href="#">8.16</a>	Monitoring activities	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
<a href="#">8.17</a>	Clock synchronization	#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence
<a href="#">8.18</a>	Use of privileged utility programs	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection
<a href="#">8.19</a>	Installation of software on operational systems	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection
<a href="#">8.20</a>	Networks security	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection
<a href="#">8.21</a>	Security of network services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
<a href="#">8.22</a>	Segregation of networks	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
<a href="#">8.23</a>	Web filtering	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
<a href="#">8.24</a>	Use of cryptography	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
<a href="#">8.25</a>	Secure development life cycle	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
<a href="#">8.26</a>	Application security requirements	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence

**Table A.1 (continued)**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">8.27</a>	Secure system architecture and engineering principles	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
<a href="#">8.28</a>	Secure coding	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
<a href="#">8.29</a>	Security testing in development and acceptance	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection
<a href="#">8.30</a>	Outsourced development	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection
<a href="#">8.31</a>	Separation of development, test and production environments	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
<a href="#">8.32</a>	Change management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
<a href="#">8.33</a>	Test information	#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection
<a href="#">8.34</a>	Protection of information systems during audit testing	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

[Table A.2](#) shows an example of how to create a view by filtering by a particular attribute value, in this case #Corrective.

**Table A.2 View of #Corrective controls**

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.5</a>	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
<a href="#">5.6</a>	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
<a href="#">5.7</a>	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
<a href="#">5.24</a>	Information security incident management planning and preparation	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
<a href="#">5.26</a>	Response to information security incidents	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
<a href="#">5.28</a>	Collection of evidence	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
<a href="#">5.29</a>	Information security during disruption	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
<a href="#">5.30</a>	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience
<a href="#">5.35</a>	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
<a href="#">5.37</a>	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
<a href="#">6.4</a>	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem

**Table A.2 (continued)**

<b>ISO/IEC 27002 control identifier</b>	<b>Control name</b>	<b>Control type</b>	<b>Information security properties</b>	<b>Cybersecurity concepts</b>	<b>Operational capabilities</b>	<b>Security domains</b>
<a href="#">8.7</a>	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence
<a href="#">8.13</a>	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
<a href="#">8.16</a>	Monitoring activities	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

## A.2 Organizational views (FI)

Since attributes are used to create different views of controls, organizations can discard the examples of attributes proposed in this document and create their own attributes with different values to address specific needs in the organization. In addition, the values assigned to each attribute can differ between organizations since organizations can have different views on the use or applicability of the control or of the values associated to the attribute (when the values are specific to the context of the organization). The first step is to understand why an organizational-specific attribute is desirable. For example, if an organization has constructed its risk treatment plans [see ISO/IEC 27001:2013, 6.1.3 e)] based on events, it can wish to associate a risk scenario attribute to each control in this document.

The benefit of such an attribute is to speed up the process of fulfilment of ISO/IEC 27001 requirement related to risk treatment, which is to compare the controls determined through the process of risk treatment (referred to as “necessary” controls), with those in ISO/IEC 27001:2013, Annex A (which are issued from in this document) to ensure that no necessary control has been overlooked.

Once the purpose and benefits are known, the next step is to determine the attribute values. For example, the organization might identify 9 events:

- 1) loss or theft of mobile device;
- 2) loss or theft from organization's premises;
- 3) force majeure, vandalism and terrorism;
- 4) failure of software, hardware, power, internet and communications;
- 5) fraud;
- 6) hacking;
- 7) disclosure;
- 8) breach of the law;
- 9) social engineering.

The second step can therefore be accomplished by assigning identifiers to each event (e.g. E1, E2, ..., E9).

The third step is to copy the control identifiers and control names from this document into a spreadsheet or database and associate the attribute values with each control, remembering that each control can have more than one attribute value.

The final step is to sort the spreadsheet or query the database to extract the required information.

Other examples of organizational attributes (and possible values) include:

- a) maturity (values from the ISO/IEC 33000 series or other maturity models);
- b) implementation state (to do, in progress, partially implemented, fully implemented);
- c) priority (1, 2, 3, etc.);
- d) organizational areas involved (security, ICT, human resources, top management, etc.);
- e) events;
- f) assets involved;
- e) build and run, to differentiate controls used in the different steps of the service life cycle;
- g) other frameworks the organization works with or can be transitioning from.

**Annex B**  
(informative)  
**Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013 (FI)**

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27002:2013 for organizations that are currently using that standard and now wish to transition to this edition.

**Table B.1** provides the correspondence of the controls specified in [Clauses 5 to 8](#) with those in ISO/IEC 27002:2013.

**Table B.1 Correspondence between controls in this document and controls in ISO/IEC 27002:2013**

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
<a href="#">5.1</a>	05.1.1, 05.1.2	Policies for information security
<a href="#">5.2</a>	06.1.1	Information security roles and responsibilities
<a href="#">5.3</a>	06.1.2	Segregation of duties
<a href="#">5.4</a>	07.2.1	Management responsibilities
<a href="#">5.5</a>	06.1.3	Contact with authorities
<a href="#">5.6</a>	06.1.4	Contact with special interest groups
<a href="#">5.7</a>	New	Threat intelligence
<a href="#">5.8</a>	06.1.5, 14.1.1	Information security in project management
<a href="#">5.9</a>	08.1.1, 08.1.2	Inventory of information and other associated assets
<a href="#">5.10</a>	08.1.3, 08.2.3	Acceptable use of information and other associated assets
<a href="#">5.11</a>	08.1.4	Return of assets
<a href="#">5.12</a>	08.2.1	Classification of information
<a href="#">5.13</a>	08.2.2	Labelling of information
<a href="#">5.14</a>	13.2.1, 13.2.2, 13.2.3	Information transfer
<a href="#">5.15</a>	09.1.1, 09.1.2	Access control
<a href="#">5.16</a>	09.2.1	Identity management
<a href="#">5.17</a>	09.2.4, 09.3.1, 09.4.3	Authentication information
<a href="#">5.18</a>	09.2.2, 09.2.5, 09.2.6	Access rights
<a href="#">5.19</a>	15.1.1	Information security in supplier relationships
<a href="#">5.20</a>	15.1.2	Addressing information security within supplier agreements
<a href="#">5.21</a>	15.1.3	Managing information security in the ICT supply chain
<a href="#">5.22</a>	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
<a href="#">5.23</a>	New	Information security for use of cloud services
<a href="#">5.24</a>	16.1.1	Information security incident management planning and preparation
<a href="#">5.25</a>	16.1.4	Assessment and decision on information security events
<a href="#">5.26</a>	16.1.5	Response to information security incidents
<a href="#">5.27</a>	16.1.6	Learning from information security incidents
<a href="#">5.28</a>	16.1.7	Collection of evidence
<a href="#">5.29</a>	17.1.1, 17.1.2, 17.1.3	Information security during disruption
<a href="#">5.30</a>	New	ICT readiness for business continuity
<a href="#">5.31</a>	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
<a href="#">5.32</a>	18.1.2	Intellectual property rights

**Table B.1 (continued)**

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
<a href="#">5.33</a>	18.1.3	Protection of records
<a href="#">5.34</a>	18.1.4	Privacy and protection of PII
<a href="#">5.35</a>	18.2.1	Independent review of information security
<a href="#">5.36</a>	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
<a href="#">5.37</a>	12.1.1	Documented operating procedures
<a href="#">6.1</a>	07.1.1	Screening
<a href="#">6.2</a>	07.1.2	Terms and conditions of employment
<a href="#">6.3</a>	07.2.2	Information security awareness, education and training
<a href="#">6.4</a>	07.2.3	Disciplinary process
<a href="#">6.5</a>	07.3.1	Responsibilities after termination or change of employment
<a href="#">6.6</a>	13.2.4	Confidentiality or non-disclosure agreements
<a href="#">6.7</a>	06.2.2	Remote working
<a href="#">6.8</a>	16.1.2, 16.1.3	Information security event reporting
<a href="#">7.1</a>	11.1.1	Physical security perimeters
<a href="#">7.2</a>	11.1.2, 11.1.6	Physical entry
<a href="#">7.3</a>	11.1.3	Securing offices, rooms and facilities
<a href="#">7.4</a>	New	Physical security monitoring
<a href="#">7.5</a>	11.1.4	Protecting against physical and environmental threats
<a href="#">7.6</a>	11.1.5	Working in secure areas
<a href="#">7.7</a>	11.2.9	Clear desk and clear screen
<a href="#">7.8</a>	11.2.1	Equipment siting and protection
<a href="#">7.9</a>	11.2.6	Security of assets off-premises
<a href="#">7.10</a>	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
<a href="#">7.11</a>	11.2.2	Supporting utilities
<a href="#">7.12</a>	11.2.3	Cabling security
<a href="#">7.13</a>	11.2.4	Equipment maintenance
<a href="#">7.14</a>	11.2.7	Secure disposal or re-use of equipment
<a href="#">8.1</a>	06.2.1, 11.2.8	User endpoint devices
<a href="#">8.2</a>	09.2.3	Privileged access rights
<a href="#">8.3</a>	09.4.1	Information access restriction
<a href="#">8.4</a>	09.4.5	Access to source code
<a href="#">8.5</a>	09.4.2	Secure authentication
<a href="#">8.6</a>	12.1.3	Capacity management
<a href="#">8.7</a>	12.2.1	Protection against malware
<a href="#">8.8</a>	12.6.1, 18.2.3	Management of technical vulnerabilities
<a href="#">8.9</a>	New	Configuration management
<a href="#">8.10</a>	New	Information deletion
<a href="#">8.11</a>	New	Data masking
<a href="#">8.12</a>	New	Data leakage prevention
<a href="#">8.13</a>	12.3.1	Information backup
<a href="#">8.14</a>	17.2.1	Redundancy of information processing facilities
<a href="#">8.15</a>	12.4.1, 12.4.2, 12.4.3	Logging

**Table B.1 (continued)**

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
<a href="#">8.16</a>	New	Monitoring activities
<a href="#">8.17</a>	12.4.4	Clock synchronization
<a href="#">8.18</a>	09.4.4	Use of privileged utility programs
<a href="#">8.19</a>	12.5.1, 12.6.2	Installation of software on operational systems
<a href="#">8.20</a>	13.1.1	Networks security
<a href="#">8.21</a>	13.1.2	Security of network services
<a href="#">8.22</a>	13.1.3	Segregation of networks
<a href="#">8.23</a>	New	Web filtering
<a href="#">8.24</a>	10.1.1, 10.1.2	Use of cryptography
<a href="#">8.25</a>	14.2.1	Secure development life cycle
<a href="#">8.26</a>	14.1.2, 14.1.3	Application security requirements
<a href="#">8.27</a>	14.2.5	Secure system architecture and engineering principles
<a href="#">8.28</a>	New	Secure coding
<a href="#">8.29</a>	14.2.8, 14.2.9	Security testing in development and acceptance
<a href="#">8.30</a>	14.2.7	Outsourced development
<a href="#">8.31</a>	12.1.4, 14.2.6	Separation of development, test and production environments
<a href="#">8.32</a>	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
<a href="#">8.33</a>	14.3.1	Test information
<a href="#">8.34</a>	12.7.1	Protection of information systems during audit testing

[Table B.2](#) provides the correspondence of controls specified in ISO/IEC 27002:2013 with those in this document.

**Table B.2 Correspondence between controls in ISO/IEC 27002:2013 and controls in this document**

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
5		Information security policies
5.1		Management direction for information security
5.1.1	<a href="#">5.1</a>	Policies for information security
5.1.2	<a href="#">5.1</a>	Review of the policies for information security
6		Organization of information security
6.1		Internal organization
6.1.1	<a href="#">5.2</a>	Information security roles and responsibilities
6.1.2	<a href="#">5.3</a>	Segregation of duties
6.1.3	<a href="#">5.5</a>	Contact with authorities
6.1.4	<a href="#">5.6</a>	Contact with special interest groups
6.1.5	<a href="#">5.8</a>	Information security in project management
6.2		Mobile devices and teleworking
6.2.1	<a href="#">8.1</a>	Mobile device policy
6.2.2	<a href="#">6.7</a>	Teleworking
7		Human resource security

**Table B.2 (continued)**

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
7.1		Prior to employment
7.1.1	<a href="#">6.1</a>	Screening
7.1.2	<a href="#">6.2</a>	Terms and conditions of employment
7.2		During employment
7.2.1	<a href="#">5.4</a>	Management responsibilities
7.2.2	<a href="#">6.3</a>	Information security awareness, education and training
7.2.3	<a href="#">6.4</a>	Disciplinary process
7.3		Termination and change of employment
7.3.1	<a href="#">6.5</a>	Termination or change of employment responsibilities
8		Asset management
8.1		Responsibility for assets
8.1.1	<a href="#">5.9</a>	Inventory of assets
8.1.2	<a href="#">5.9</a>	Ownership of assets
8.1.3	<a href="#">5.10</a>	Acceptable use of assets
8.1.4	<a href="#">5.11</a>	Return of assets
8.2		Information classification
8.2.1	<a href="#">5.12</a>	Classification of information
8.2.2	<a href="#">5.13</a>	Labelling of information
8.2.3	<a href="#">5.10</a>	Handling of assets
8.3		Media handling
8.3.1	<a href="#">7.10</a>	Management of removable media
8.3.2	<a href="#">7.10</a>	Disposal of media
8.3.3	<a href="#">7.10</a>	Physical media transfer
9		Access control
9.1		Business requirements of access control
9.1.1	<a href="#">5.15</a>	Access control policy
9.1.2	<a href="#">5.15</a>	Access to networks and network services
9.2		User access management
9.2.1	<a href="#">5.16</a>	User registration and de-registration
9.2.2	<a href="#">5.18</a>	User access provisioning
9.2.3	<a href="#">8.2</a>	Management of privileged access rights
9.2.4	<a href="#">5.17</a>	Management of secret authentication information of users
9.2.5	<a href="#">5.18</a>	Review of user access rights
9.2.6	<a href="#">5.18</a>	Removal or adjustment of access rights
9.3		User responsibilities
9.3.1	<a href="#">5.17</a>	Use of secret authentication information
9.4		System and application access control
9.4.1	<a href="#">8.3</a>	Information access restriction
9.4.2	<a href="#">8.5</a>	Secure log-on procedures
9.4.3	<a href="#">5.17</a>	Password management system
9.4.4	<a href="#">8.18</a>	Use of privileged utility programs
9.4.5	<a href="#">8.4</a>	Access control to program source code

**Table B.2 (continued)**

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
10		Cryptography
10.1		Cryptographic controls
10.1.1	<a href="#">8.24</a>	Policy on the use of cryptographic controls
10.1.2	<a href="#">8.24</a>	Key management
11		Physical and environmental security
11.1		Secure areas
11.1.1	<a href="#">7.1</a>	Physical security perimeter
11.1.2	<a href="#">7.2</a>	Physical entry controls
11.1.3	<a href="#">7.3</a>	Securing offices, rooms and facilities
11.1.4	<a href="#">7.5</a>	Protecting against external and environmental threats
11.1.5	<a href="#">7.6</a>	Working in secure areas
11.1.6	<a href="#">7.2</a>	Delivery and loading areas
11.2		Equipment
11.2.1	<a href="#">7.8</a>	Equipment siting and protection
11.2.2	<a href="#">7.11</a>	Supporting utilities
11.2.3	<a href="#">7.12</a>	Cabling security
11.2.4	<a href="#">7.13</a>	Equipment maintenance
11.2.5	<a href="#">7.10</a>	Removal of assets
11.2.6	<a href="#">7.9</a>	Security of equipment and assets off-premises
11.2.7	<a href="#">7.14</a>	Secure disposal or reuse of equipment
11.2.8	<a href="#">8.1</a>	Unattended user equipment
11.2.9	<a href="#">7.7</a>	Clear desk and clear screen policy
12		Operations security
12.1		Operational procedures and responsibilities
12.1.1	<a href="#">5.37</a>	Documented operating procedures
12.1.2	<a href="#">8.32</a>	Change management
12.1.3	<a href="#">8.6</a>	Capacity management
12.1.4	<a href="#">8.31</a>	Separation of development, testing and operational environments
12.2		Protection from malware
12.2.1	<a href="#">8.7</a>	Controls against malware
12.3		Backup
12.3.1	<a href="#">8.13</a>	Information backup
12.4		Logging and monitoring
12.4.1	<a href="#">8.15</a>	Event logging
12.4.2	<a href="#">8.15</a>	Protection of log information
12.4.3	<a href="#">8.15</a>	Administrator and operator logs
12.4.4	<a href="#">8.17</a>	Clock synchronization
12.5		Control of operational software
12.5.1	<a href="#">8.19</a>	Installation of software on operational systems
12.6		Technical vulnerability management
12.6.1	<a href="#">8.8</a>	Management of technical vulnerabilities
12.6.2	<a href="#">8.19</a>	Restrictions on software installation

**Table B.2 (continued)**

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
12.7		Information systems audit considerations
12.7.1	<a href="#">8.34</a>	Information systems audit controls
13		Communications security
13.1		Network security management facilities.
13.1.1	<a href="#">8.20</a>	Network controls
13.1.2	<a href="#">8.21</a>	Security of network services
13.1.3	<a href="#">8.22</a>	Segregation in networks
13.2		Information transfer
13.2.1	<a href="#">5.14</a>	Information transfer policies and procedures
13.2.2	<a href="#">5.14</a>	Agreements on information transfer
13.2.3	<a href="#">5.14</a>	Electronic messaging
13.2.4	<a href="#">6.6</a>	Confidentiality or nondisclosure agreements
14		System acquisition, development and maintenance
14.1		Security requirements of information systems
14.1.1	<a href="#">5.8</a>	Information security requirements analysis and specification
14.1.2	<a href="#">8.26</a>	Securing application services on public networks
14.1.3	<a href="#">8.26</a>	Protecting application services transactions
14.2		Security in development and support processes
14.2.1	<a href="#">8.25</a>	Secure development policy
14.2.2	<a href="#">8.32</a>	System change control procedures
14.2.3	<a href="#">8.32</a>	Technical review of applications after operating platform changes
14.2.4	<a href="#">8.32</a>	Restrictions on changes to software packages
14.2.5	<a href="#">8.27</a>	Secure system engineering principles
14.2.6	<a href="#">8.31</a>	Secure development environment
14.2.7	<a href="#">8.30</a>	Outsourced development
14.2.8	<a href="#">8.29</a>	System security testing
14.2.9	<a href="#">8.29</a>	System acceptance testing
14.3		Test data
14.3.1	<a href="#">8.33</a>	Protection of test data
15		Supplier relationships
15.1		Information security in supplier relationships
15.1.1	<a href="#">5.19</a>	Information security policy for supplier relationships
15.1.2	<a href="#">5.20</a>	Addressing security within supplier agreements
15.1.3	<a href="#">5.21</a>	Information and communication technology supply chain
15.2		Supplier service delivery management
15.2.1	<a href="#">5.22</a>	Monitoring and review of supplier services
15.2.2	<a href="#">5.22</a>	Managing changes to supplier services
16		Information security incident management
16.1		Management of information security incidents and improvements
16.1.1	<a href="#">5.24</a>	Responsibilities and procedures
16.1.2	<a href="#">6.8</a>	Reporting information security events
16.1.3	<a href="#">6.8</a>	Reporting information security weaknesses

**Table B.2 (continued)**

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
16.1.4	<a href="#">5.25</a>	Assessment of and decision on information security events
16.1.5	<a href="#">5.26</a>	Response to information security incidents
16.1.6	<a href="#">5.27</a>	Learning from information security incidents
16.1.7	<a href="#">5.28</a>	Collection of evidence
17		Information security aspects of business continuity management
17.1		Information security continuity
17.1.1	<a href="#">5.29</a>	Planning information security continuity
17.1.2	<a href="#">5.29</a>	Implementing information security continuity
17.1.3	<a href="#">5.29</a>	Verify, review and evaluate information security continuity
17.2		Redundancies
17.2.1	<a href="#">8.14</a>	Availability of information processing facilities
18		Compliance
18.1		Compliance with legal and contractual requirements
18.1.1	<a href="#">5.31</a>	Identification of applicable legislation and contractual requirements
18.1.2	<a href="#">5.32</a>	Intellectual property rights
18.1.3	<a href="#">5.33</a>	Protection of records
18.1.4	<a href="#">5.34</a>	Privacy and protection of personally identifiable information
18.1.5	<a href="#">5.31</a>	Regulation of cryptographic controls
18.2		Information security reviews
18.2.1	<a href="#">5.35</a>	Independent review of information security
18.2.2	<a href="#">5.36</a>	Compliance with security policies and standards
18.2.3	<a href="#">5.36, 8.8</a>	Technical compliance review

## Bibliography [\(FI\)](#)

- [1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO 55001, *Asset management — Management systems — Requirements*
- [3] ISO/IEC 11770 (all parts), *Information security — Key management*
- [4] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*
- [5] ISO 15489 (all parts), *Information and documentation — Records management*
- [6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
- [7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
- [8] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*
- [9] ISO/IEC 19770 (all parts), *Information technology — IT asset management*
- [10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- [11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
- [12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
- [13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
- [14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
- [15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
- [16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
- [17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
- [18] ISO/IEC TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
- [19] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
- [20] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*
- [21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
- [22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
- [23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
- [24] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*
- [25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*

- [26] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
- [27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
- [30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [31] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*
- [32] ISO/IEC 27034 (all parts), *Information technology — Application security*
- [33] ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information security incident management*
- [34] ISO/IEC 27036 (all parts), *Information technology — Security techniques — Information security for supplier relationships*
- [35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [37] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*
- [38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
- [39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
- [40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
- [41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
- [42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
- [43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*
- [44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
- [45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
- [46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
- [47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
- [48] ISO 31000:2018, *Risk management — Guidelines*
- [49] IEC 31010, *Risk management — Risk assessment techniques*
- [50] ISO/IEC 22123 (all parts), *Information technology — Cloud computing*
- [51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

- 
- [52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at <https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/>
  - [53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076
  - [54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-37r2>
  - [55] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at [https://owasp.org/www-project-top-ten/OWASP\\_Top\\_Ten\\_2017/](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/)
  - [56] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at <https://github.com/OWASP/DevGuide>
  - [57] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-63b>
  - [58] OASIS. Structured Threat Information Expression. Available at <https://www.oasis-open.org/standards#stix2.0>
  - [59] OASIS. Trusted Automated Exchange of Indicator Information. Available at <https://www.oasis-open.org/standards#taxii2.0>