SFS

Suomen Standardisoimisliitto

# SFS-EN ISO/IEC 27001:2023

## Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset

Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

SFS Standardi

SFS-EN ISO/IEC 27001:2023

Vahvistettu 2023-08-04 1 (46)

2. painos
Korvaa standardien ISO/IEC 27001:2022:fi painoksen 1 ja SFS-EN ISO/IEC 27001:2017 painoksen 1

2nd edition
Replaces standards ISO/IEC 27001:2022:fi edition 1 and SFS-EN ISO/IEC 27001:2017 edition 1

Ristiriitatapauksissa pätee englanninkielinen teksti.
Suomenkielisen käännöksen päivämäärä 2023-09-01

In case of interpretation disputes the English text applies.
Date of translation into Finnish 2023-09-01

# Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset

## Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)

Tämä standardi sisältää eurooppalaisen standardin EN ISO/IEC 27001:2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)" englanninkielisen tekstin.

This standard consists of the English text of the European Standard EN ISO/IEC 27001:2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)".

Standardi sisältää myös englanninkielisen tekstin suomenkielisen käännöksen.

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

Eurooppalainen standardi EN ISO/IEC 27001:2023 on vahvistettu suomalaiseksi kansalliseksi standardiksi.

The European Standard EN ISO/IEC 27001:2023 has the status of a Finnish national standard.



Standardista vastaava toimialayhteisö:
Suomen Standardisoimisliitto SFS ry

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

**Suomen Standardisoimisliitto SFS ry**
Malminkatu 34, PL 130, 00101 Helsinki
p. 09 149 9331, www.sfs.fi, sales@sfs.fi

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

Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

## Monta tapaa tilata

### Pysy ajan tasalla

Tietopalvelumme tarjoaa monia helppoja tapoja pysyä ajan tasalla toimialaasi kuuluvista standardeista. Lue lisää www.sfs.fi/tietopalvelu.

Haluatko tietoa uusista julkaisuista sähköpostilla?
Tilaa sähköinen uutiskirje haluamastasi aiheesta www.sfs.fi/uutiskirjetilaus.

### Asiakaspalvelu auttaa

SFS:n asiakaspalvelusta voit tilata kaikki tarvitsemasi julkaisut.
Ota yhteyttä 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.

### SFS Online

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

facebook.com/Standardeista
@standardeista
Suomen Standardisoimisliitto SFS ry



# SFS-EN ISO/IEC 27001:2023

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

Julkaistu: SFS 2023-09



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Sisällys

Sivu





Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

## Eurooppalainen esipuhe (CEN) (EN)

Standardin ISO/IEC 27001:2022 on laatinut ISOn (International Organization for Standardization) ja IEC:n (International Electrotechnical Commission) yhteinen tekninen komitea ISO/IEC JTC 1 *Information technology*. CENin ja CENELECin yhteinen tekninen komitea CEN-CENELEC/JTC 13 *Cybersecurity and Data Protection*, jonka sihteeristönä toimii DIN, on hyväksynyt sen eurooppalaiseksi standardiksi EN ISO/IEC 27001:2023.

Tälle eurooppalaiselle standardille on annettava kansallisen standardin asema joko julkaisemalla standardin kanssa yhtäpitävä teksti tai vahvistamalla asiakirja kansalliseksi standardiksi tammikuun 2024 loppuun mennessä. Lisäksi tämän standardin kanssa ristiriitaiset kansalliset standardit on kumottava tammikuun 2024 loppuun mennessä.

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

Tämä asiakirja korvaa standardin EN ISO/IEC 27001:2017.

Tästä asiakirjasta voi lähettää palautetta tai kysymyksiä kunkin maan kansalliselle standardointijärjestölle. Järjestöt on lueteltu CENin ja CENELECin verkkosivuilla.

CENin ja CENELECin sääntöjen mukaan seuraavien maiden standardointijärjestöt 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 27001:2022 eurooppalaiseksi standardiksi EN ISO/IEC 27001:2023 sellaisenaan.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

## Esipuhe (ISO)

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostavat maailmanlaajuiseen standardisointiin erikoistuneen järjestelmän. ISOn tai IEC:n kansalliset jäsenjärjestöt osallistuvat kansainvälisten 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 tarkoitetut 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 tai www.iec.ch/members_experts/refdocs).

Jotkin tämän asiakirjan yksityiskohdat saattavat olla patenttioikeuksin suojattuja. 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) tai IEC:n ylläpitämässä patentointia koskevien ilmoitusten luettelossa (https://patents.iec.ch).

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

Standardien käytön vapaaehtoisuudesta, vaatimustenmukaisuuden arviointiin liittyvien ISOn käyttämien termien ja ilmaisujen merkityksestä sekä kaupan teknisiä esteitä koskevan WTO:n sopimuksen periaatteiden noudattamisesta ISOn toiminnassa on tietoa osoitteessa www.iso.org/iso/foreword.html. IEC:n vastaavista käytännöistä on tietoa osoitteessa 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 27001:2013), jota on uudistettu teknisesti. Tämä koskee myös teknisiä korjauksia ISO/IEC 27001:2013/Cor. 1:2014 ja ISO/IEC 27001:2013/Cor. 2:2015.

Suurimmat muutokset edelliseen painokseen ovat seuraavat:

— Teksti on yhdenmukaistettu hallintajärjestelmästandardien rakenteen ja standardin ISO/IEC 27002:2022 kanssa.

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



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Johdanto (EN)

## 0.1 Yleistä

Tässä asiakirjassa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Tietoturvallisuuden hallintajärjestelmän käyttöönotto on organisaation strateginen päätös. Organisaation tietoturvallisuuden hallintajärjestelmän luomiseen ja toteuttamiseen vaikuttavat organisaation tarpeet ja tavoitteet, turvallisuusvaatimukset, käytettävät organisaatioprosessit sekä organisaation koko ja rakenne. Kaikkien näiden asiaan vaikuttavien tekijöiden odotetaan muuttuvan ajan kuluessa.

Tietoturvallisuuden hallintajärjestelmä suojaa tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla sekä vahvistaa sidosryhmien luottamusta siihen, että riskejä hallitaan asianmukaisesti.

On tärkeää, että tietoturvallisuuden hallintajärjestelmä on osa organisaation prosesseja ja yleisiä johtamis- ja hallintarakenteita ja että se on yhdistetty niihin. Lisäksi on tärkeää, että tietoturvallisuus otetaan huomioon prosessien, tietojärjestelmien ja hallintakeinojen suunnittelussa. Tietoturvallisuuden hallintajärjestelmän toteutuksen oletetaan olevan organisaation tarpeiden mukainen.

Tätä asiakirjaa voivat käyttää sekä sisäiset että ulkoiset sidosryhmät, kun ne arvioivat organisaation kykyä täyttää sen omat tietoturvavaatimukset.

Järjestys, jossa vaatimukset esitetään tässä asiakirjassa, ei ole niiden tärkeysjärjestys tai niiden suositeltu toteuttamisjärjestys. Kohdat on numeroitu vain viittaustarkoituksessa.

Standardissa ISO/IEC 27000 esitetään tietoturvallisuuden hallintajärjestelmien yleiskuvaus ja sanasto keskittyen eritoten tietoturvallisuuden hallintajärjestelmästandardisarjaan (johon kuuluvat myös standardit ISO/IEC 27003[2], ISO/IEC 27004[3] ja ISO/IEC 27005[4]) sekä esitetään aihealueeseen liittyvät termit ja määritelmät.

## 0.2 Yhteensopivuus muiden hallintajärjestelmästandardien kanssa

Tässä asiakirjassa noudatetaan ISOn ja IEC:n sääntöjen osan 1 liitteessä SL (ISOn konsolidoitu lisäys) määriteltyä yleisrakennetta ja määriteltyjä alakohtien otsikkoja, vakiotekstejä, yhteisiä termejä sekä keskeisiä määritelmiä. Näin tämä asiakirja säilyy yhteensopivana muiden liitteen SL mukaisten hallintajärjestelmästandardien kanssa.

Tästä liitteen SL mukaisesta yhtenäistämisestä on hyötyä organisaatioille, jotka haluavat, että niiden johtamisjärjestelmä täyttää kahden tai useamman hallintajärjestelmästandardin vaatimukset.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 1 Soveltamisala (EN)

Tässä asiakirjassa määritellään vaatimukset, jotka koskevat tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista organisaation toimintaympäristössä. Tämä asiakirja sisältää myös organisaation tarpeisiin mukautettua tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. Asiakirjassa esitetyt vaatimukset ovat yleisluonteisia, ja tarkoitus on, että ne soveltuvat kaikille organisaatioille niiden tyypistä, koosta tai luonteesta riippumatta. Jos organisaatio ilmoittaa noudattavansa tämän asiakirjan vaatimuksia, ei mitään kohdissa 4–10 esitetyistä vaatimuksista voida rajata tarkastelun ulkopuolelle.

# 2 Velvoittavat viittaukset (EN)

Osa tämän asiakirjan vaatimuksista esitetään muissa asiakirjoissa, joihin viitataan tekstissä. Viittaus voi koskea asiakirjan koko sisältöä tai sen osaa. Jos viittaus on päivätty, sovelletaan vain kyseistä painosta. Jos viittaus on päiväämätön, sovelletaan viimeisintä painosta sekä mahdollisia muutoksia.

ISO/IEC 27000[1)], *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

# 3 Termit ja määritelmät (EN)

Tässä asiakirjassa käytetään standardissa ISO/IEC 27000 esitettyjä 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/.

# 4 Organisaation toimintaympäristö (EN)

## 4.1 Organisaation ja sen toimintaympäristön ymmärtäminen (EN)

Organisaation on määritettävä ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta ja vaikuttavat sen kykyyn saavuttaa tietoturvallisuuden hallintajärjestelmältä halutut tulokset.

HUOM. Näiden asioiden määrittämisellä tarkoitetaan organisaation ulkoisen ja sisäisen toimintaympäristön määrittelemistä, jota käsitellään standardin ISO 31000:2018[5] kohdassa 5.4.1.

## 4.2 Sidosryhmien tarpeiden ja odotusten ymmärtäminen (EN)

Organisaation on määritettävä

a) tietoturvallisuuden hallintajärjestelmän kannalta olennaiset sidosryhmät

b) näiden sidosryhmien olennaiset vaatimukset

c) mihin näistä vaatimuksista tietoturvallisuuden hallintajärjestelmällä vastataan.

HUOM. Sidosryhmien vaatimukset saattavat sisältää lakisääteisiä vaatimuksia ja viranomaisten vaatimuksia sekä sopimusvelvoitteita.

1) Vastaava suomenkielinen SFS-standardi: SFS-EN ISO/IEC 27000:2020 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 4.3 Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen (EN)

Organisaation on päätettävä tietoturvallisuuden hallintajärjestelmän rajauksista ja soveltamisesta, jotta järjestelmän soveltamisalan voi määritellä.

Kun organisaatio päättää tietoturvallisuuden hallintajärjestelmänsä soveltamisalasta, sen on otettava huomioon

a) kohdassa 4.1 mainitut ulkoiset ja sisäiset asiat

b) kohdassa 4.2 mainitut vaatimukset

c) organisaation ja muiden organisaatioiden suorittamien toimintojen rajapinnat ja riippuvuudet.

Soveltamisalan on oltava saatavilla dokumentoituna tietona.

### 4.4 Tietoturvallisuuden hallintajärjestelmä (EN)

Organisaation on luotava ja toteutettava tietoturvallisuuden hallintajärjestelmä, johon sisältyvät tarvittavat prosessit ja niiden keskinäiset vaikutukset, sekä ylläpidettävä ja parannettava sitä jatkuvasti tässä asiakirjassa esitettyjen vaatimusten mukaisesti.

## 5 Johtajuus (EN)

### 5.1 Johtajuus ja sitoutuminen (EN)

Ylimmän johdon on osoitettava johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmään

a) varmistamalla, että tietoturvapolitiikka laaditaan ja tietoturvatavoitteet asetetaan ja että ne ovat yhdenmukaisia organisaation strategian kanssa

b) varmistamalla, että tietoturvallisuuden hallintajärjestelmän vaatimukset yhdistetään organisaation prosesseihin

c) varmistamalla, että tietoturvallisuuden hallintajärjestelmää varten tarvittavat resurssit ovat saatavilla

d) viestimällä siitä, miten tärkeää on, että tietoturvallisuuden hallinta on vaikuttavaa ja että tietoturvallisuuden hallintajärjestelmää koskevia vaatimuksia noudatetaan

e) varmistamalla, että tietoturvallisuuden hallintajärjestelmä saavuttaa halutut tulokset

f) ohjaamalla ihmisiä lisäämään tietoturvallisuuden hallintajärjestelmän vaikuttavuutta ja tukemalla heitä siinä

g) edistämällä jatkuvaa parantamista

h) tukemalla muiden johtoon kuuluvien johtajuutta heidän vastuualueillaan.

HUOM. Tässä asiakirjassa ”liiketoiminnalla” tarkoitetaan yleisesti niitä toimintoja, jotka ovat organisaation olemassaolon tarkoituksen kannalta keskeisiä.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 5.2 Tietoturvapolitiikka (EN)

Ylimmän johdon on laadittava tietoturvapolitiikka, joka

a) sopii organisaation tarkoitukseen

b) sisältää tietoturvatavoitteet (ks. kohta 6.2) tai muodostaa perustan tietoturvatavoitteiden asettamiselle

c) sisältää sitoutumisen tietoturvallisuutta koskevien vaatimusten täyttämiseen

d) sisältää sitoutumisen tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen.

Tietoturvapolitiikan on oltava

e) saatavilla dokumentoituna tietona

f) koko organisaation tiedossa

g) tarvittaessa sidosryhmien saatavilla.

### 5.3 Organisaation roolit, vastuut ja valtuudet (EN)

Ylimmän johdon on varmistettava, että tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet määritellään ja että niistä viestitään organisaatiossa.

Ylimmän johdon on määriteltävä, kenellä tai keillä on vastuu ja valtuudet

a) varmistaa, että tietoturvallisuuden hallintajärjestelmä on tässä asiakirjassa esitettyjen vaatimusten mukainen

b) raportoida ylimmälle johdolle tietoturvallisuuden hallintajärjestelmän suorituskyvystä.

HUOM. Ylin johto voi myös määritellä, kenellä tai keillä on vastuu ja valtuudet raportoida tietoturvallisuuden hallintajärjestelmän suorituskyvystä organisaation sisällä.

## 6 Suunnittelu (EN)

### 6.1 Riskien ja mahdollisuuksien käsittely (EN)

#### 6.1.1 Yleistä (EN)

Tietoturvallisuuden hallintajärjestelmää suunnitellessaan organisaation on otettava huomioon kohdassa 4.1 mainitut asiat ja kohdassa 4.2 esitetyt vaatimukset sekä määritettävä riskit ja mahdollisuudet, joita on käsiteltävä, jotta voidaan

a) varmistaa, että tietoturvallisuuden hallintajärjestelmä voi saavuttaa halutut tulokset

b) estää tai vähentää ei-toivottuja vaikutuksia

c) saada aikaan jatkuvaa parantamista.

Organisaation on suunniteltava

d) näihin riskeihin ja mahdollisuuksiin kohdistuvat toimenpiteet

e) kuinka

1) nämä toimenpiteet yhdistetään sen tietoturvallisuuden hallintajärjestelmän prosesseihin ja toteutetaan

2) näiden toimenpiteiden vaikuttavuus arvioidaan.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 6.1.2 Tietoturvariskien arviointi (EN)

Organisaation on määriteltävä ja toteutettava tietoturvariskien arviointiprosessi, jossa

a) laaditaan ja ylläpidetään tietoturvariskikriteerejä, joihin kuuluvat

   1) riskien hyväksymiskriteerit

   2) tietoturvariskien arvioinnin suorittamista koskevat kriteerit

b) varmistetaan, että toistuvat tietoturvariskien arvioinnit tuottavat yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia.

c) tunnistetaan tietoturvariskit

   1) toteuttamalla tietoturvariskien arviointiprosessi, jolla tunnistetaan tämän tietoturvallisuuden hallintajärjestelmän soveltamisalaan kuuluvan tiedon luottamuksellisuuden, eheyden ja saatavuuden menettämiseen liittyvät riskit

   2) tunnistamalla riskien omistajat

d) analysoidaan tietoturvariskit

   1) arvioimalla kohdassa 6.1.2 c) 1) tunnistettujen riskien toteutumisen mahdolliset seuraukset

   2) arvioimalla kohdassa 6.1.2 c) 1) tunnistettujen riskien toteutumisen realistinen todennäköisyys

   3) määrittämällä riskin taso

e) arvioidaan tietoturvariskit

   1) vertaamalla riskianalyysin tuloksia kohdassa 6.1.2 a) laadittuihin riskikriteereihin

   2) priorisoimalla analysoidut riskit riskien käsittelyyn.

Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien arviointiprosessista.

### 6.1.3 Tietoturvariskien käsittely (EN)

Organisaation on määriteltävä ja toteutettava tietoturvariskien käsittelyprosessi, jossa

a) valitaan soveltuvat tietoturvariskien käsittelyvaihtoehdot ottaen huomioon riskien arvioinnin tulokset

b) määritetään kaikki hallintakeinot, joita tarvitaan valittujen tietoturvariskien käsittelyvaihtoehtojen toteuttamiseen

   HUOM. 1 Organisaatiot voivat tarpeen mukaan suunnitella hallintakeinot itse tai yksilöidä ne muista lähteistä.

c) verrataan kohdassa 6.1.3 b) määritettyjä hallintakeinoja liitteessä A oleviin ja todennetaan, ettei yhtäkään tarvittavaa hallintakeinoa ole jätetty pois

   HUOM. 2 Liite A sisältää luettelon mahdollisista hallintakeinoista. Tämän asiakirjan käyttäjiä kehotetaan käyttämään liitettä A, jotta he voivat varmistaa, ettei mitään tarvittavia tietoturvallisuuden hallintakeinoja jätetä huomioimatta.

   HUOM. 3 Liitteen A luettelo tietoturvallisuuden hallintakeinoista ei ole täydellinen, vaan siinä esitettyjen lisäksi voidaan tarvittaessa toteuttaa muitakin tietoturvallisuuden hallintakeinoja.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

d) laaditaan soveltuvuuslausunto, joka sisältää

— tarvittavat hallintakeinot (ks. kohdat 6.1.3 b) ja c))

— perustelut niiden käyttämiselle

— sen, onko tarvittavat hallintakeinot toteutettu vai ei

— perustelut liitteessä A esitettyjen hallintakeinojen käyttämättä jättämiselle

e) laaditaan tietoturvariskien käsittelysuunnitelma

f) hankitaan riskien omistajalta hyväksyntä tietoturvariskien käsittelysuunnitelmalle ja jäljelle jääville tietoturvariskeille.

Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien käsittelyprosessista.

HUOM. 4 Tässä asiakirjassa esitetyt tietoturvariskien arviointi- ja käsittelyprosessit ovat yhdensuuntaisia standardissa ISO 31000[5] esitettyjen periaatteiden ja yleisten ohjeiden kanssa.

## 6.2 Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu (EN)

Organisaation on asetettava tietoturvatavoitteet asiaankuuluville toiminnoille ja tasoille.

Tietoturvatavoitteiden on täytettävä seuraavat vaatimukset:

a) Niiden on oltava yhdenmukaisia tietoturvapolitiikan kanssa.

b) Niiden on oltava mitattavissa (jos mahdollista).

c) Niissä on otettava huomioon soveltuvat tietoturvavaatimukset sekä riskien arvioinnin ja käsittelyn tulokset.

d) Niitä on seurattava.

e) Niistä on viestittävä.

f) Niitä on päivitettävä tarvittaessa.

g) Niiden on oltava saatavilla dokumentoituna tietona

Organisaation on säilytettävä dokumentoitua tietoa tietoturvatavoitteista.

Kun organisaatio suunnittelee, kuinka se voi saavuttaa tietoturvatavoitteensa, sen on määritettävä

h) mitä tehdään

i) mitä resursseja tarvitaan

j) kuka tai ketkä ovat vastuussa

k) milloin tarvittavat toimet saadaan valmiiksi

l) kuinka tuloksia arvioidaan.

## 6.3 Muutosten suunnittelu (EN)

Kun organisaatio havaitsee tietoturvallisuuden hallintajärjestelmään liittyviä muutostarpeita, muutokset on toteutettava suunnitelmallisesti.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 7 Tukitoiminnot (EN)

## 7.1 Resurssit (EN)

Organisaation on määritettävä ja varattava tietoturvallisuuden hallintajärjestelmän luomiseen, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit.

## 7.2 Pätevyys (EN)

Organisaation on

a) määritettävä, millainen pätevyys niillä sen ohjauksessa työskentelevillä henkilöillä täytyy olla, joiden työ vaikuttaa sen tietoturvallisuuden tasoon

b) varmistettava, että nämä henkilöt ovat päteviä soveltuvan koulutuksen, harjoittelun tai kokemuksen perusteella

c) hankittava tarvittaessa vaadittava pätevyys eri toimenpitein sekä arvioitava tehtyjen toimenpiteiden vaikuttavuutta

d) säilytettävä asianmukaista dokumentoitua tietoa näyttönä pätevyydestä.

HUOM. Eri keinoja voivat olla esimerkiksi nykyisten työntekijöiden kouluttaminen, mentorointi tai siirtäminen toisiin tehtäviin tai pätevien henkilöiden palkkaaminen tai vuokraaminen.

## 7.3 Tietoisuus (EN)

Organisaation ohjauksessa työskentelevien henkilöiden on oltava tietoisia

a) tietoturvapolitiikasta

b) siitä, miten he voivat osaltaan lisätä tietoturvallisuuden hallintajärjestelmän vaikuttavuutta ja millaista hyötyä tietoturvallisuuden tason parantamisesta on

c) seurauksista, joita tietoturvallisuuden hallintajärjestelmää koskevien vaatimusten noudattamatta jättämisellä voi olla.

## 7.4 Viestintä (EN)

Organisaation on määritettävä, millaista tietoturvallisuuden hallintajärjestelmän kannalta olennaista sisäistä ja ulkoista viestintää tarvitaan, mihin sisältyy se

a) mistä viestitään

b) milloin viestitään

c) keiden kanssa viestitään

d) kuinka viestitään.

## 7.5 Dokumentoitu tieto (EN)

### 7.5.1 Yleistä (EN)

Organisaation tietoturvallisuuden hallintajärjestelmän on sisällettävä

a) tässä asiakirjassa edellytetty dokumentoitu tieto

b) dokumentoitu tieto, jonka organisaatio on määrittänyt tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömäksi.

HUOM. Tietoturvallisuuden hallintajärjestelmän dokumentoidun tiedon laajuus voi olla erilainen eri organisaatioissa, koska siihen vaikuttavat.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

1) organisaation koko sekä sen toimintojen, prosessien, tuotteiden ja palveluiden tyyppi

2) prosessien monimutkaisuus ja niiden välinen vuorovaikutus

3) henkilöiden pätevyys.

### 7.5.2 Dokumentoidun tiedon luominen ja päivittäminen (EN)

Organisaation on dokumentoitua tietoa luodessaan ja päivittäessään varmistettava sen asianmukainen

a) yksilöinti ja tunnistus (esim. otsikko, päiväys, laatija, viitenumero)

b) tallennusmuoto (esim. kieli, ohjelmistoversio, kuvat) ja tallennusväline (esim. paperi, sähköinen)

c) soveltuvuuden ja tarkoituksenmukaisuuden tarkistaminen ja hyväksyminen.

### 7.5.3 Dokumentoidun tiedon hallinta (EN)

Tietoturvallisuuden hallintajärjestelmän ja tämän asiakirjan edellyttämää dokumentoitua tietoa on hallittava, jotta voidaan varmistaa, että

a) se on aina tarvittaessa saatavilla käyttötarkoitukseen sopivassa muodossa

b) se on suojattu asianmukaisesti (esimerkiksi luottamuksellisia tietoja ei luovuteta luvatta, tietojen asiaton käyttö on estetty ja tiedot pysyvät muuttumattomana kokonaisuutena).

Organisaation dokumentoidun tiedon hallinnan on katettava soveltuvin osin seuraavat kohdat:

c) jakelu, pääsy tietoihin, esillesaanti ja käyttö

d) varastointi ja säilytys, johon kuuluu myös luettavuuden säilyttäminen

e) muutostenhallinta (esim. versionhallinta)

f) säilyttäminen ja hävittäminen.

Ulkopuolista alkuperää oleva dokumentoitu tieto, jonka organisaatio on määrittänyt tarpeelliseksi tietoturvallisuuden hallintajärjestelmän suunnittelun ja toiminnan kannalta, on yksilöitävä tarvittavalla tavalla, ja sitä on hallittava.

HUOM. Pääsyllä tietoihin voidaan tarkoittaa päätöstä siitä, kenellä on lupa tarkastella dokumentoitua tietoa tai lupa ja valtuudet tarkastella ja muuttaa sitä.

## 8 Toiminta (EN)

### 8.1 Toiminnan suunnittelu ja ohjaus (EN)

Organisaation on suunniteltava ja toteutettava prosessit, joita tarvitaan vaatimusten täyttämiseen ja kohdassa 6 määritettyjen toimenpiteiden toteuttamiseen, sekä ohjattava niitä. Tätä varten sen on

— määriteltävä kriteerit näille prosesseille

— toteutettava prosessien ohjaus kriteerien mukaisesti

Organisaation on säilytettävä dokumentoitua tietoa tarvittavassa laajuudessa voidakseen luottaa siihen, että prosessit on toteutettu suunnitellusti.

Organisaation on hallittava suunniteltuja muutoksia ja arvioitava tahattomien muutosten seurauksia sekä pyrittävä lieventämään mahdollisia haittavaikutuksia tarpeen mukaan.

Organisaation on varmistettava, että tietoturvallisuuden hallintajärjestelmän kannalta olennaisia ulkoisesti tuotettuja prosesseja, tuotteita tai palveluja hallitaan.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 8.2 Tietoturvariskien arviointi (EN)

Organisaation on suoritettava tietoturvariskien arviointi suunnitelluin aikavälein tai kun merkittäviä muutoksia ehdotetaan tai kun tällaisia muutoksia tapahtuu. Arvioinnissa on otettava huomioon kohdassa 6.1.2 a) laaditut kriteerit.

Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien arviointien tuloksista.

### 8.3 Tietoturvariskien käsittely (EN)

Organisaation on otettava käyttöön tietoturvariskien käsittelysuunnitelma.

Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien käsittelyn tuloksista.

## 9 Suorituskyvyn arviointi (EN)

### 9.1 Seuranta, mittaus, analysointi ja arviointi (EN)

Organisaation on määritettävä

a) mitä täytyy seurata ja mitata, mukaan lukien tietoturvaprosessit ja hallintakeinot

b) millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä varmistetaan kelvolliset tulokset tarvittaessa; valituilla menetelmillä pitäisi saada vertailtavissa ja toistettavissa olevia tuloksia, jotta niitä voidaan pitää kelvollisina

c) milloin seuranta ja mittaus on toteutettava

d) ketkä toteuttavat seurannan ja mittaamisen

e) milloin seurannan ja mittauksen tuloksia on analysoitava ja arvioitava

f) ketkä analysoivat ja arvioivat saadut tulokset.

Dokumentoitua tietoa on säilytettävänä näyttönä tuloksista.

Organisaation on arvioitava tietoturvan toteutumista ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta.

### 9.2 Sisäinen auditointi (EN)

#### 9.2.1 Yleistä (EN)

Organisaation on tehtävä sisäisiä auditointeja suunnitelluin aikavälein, jotta niistä saatujen tietojen perusteella voidaan määrittää

a) onko tietoturvallisuuden hallintajärjestelmä

   1) organisaation omien tietoturvallisuuden hallintajärjestelmää koskevien vaatimusten mukainen

   2) tässä asiakirjassa esitettyjen vaatimusten mukainen

b) onko tietoturvallisuuden hallintajärjestelmä toteutettu ja ylläpidetty vaikuttavasti.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 9.2.2 Sisäinen auditointiohjelma (EN)

Organisaation on suunniteltava, laadittava, toteutettava ja ylläpidettävä auditointiohjelmia, joissa määritellään muun muassa auditointien taajuus, menetelmät, vastuut, suunnitteluvaatimukset ja raportointi.

Sisäisiä auditointiohjelmia laatiessaan organisaation on otettava huomioon kyseisten prosessien tärkeys sekä edellisten auditointien tulokset.

Organisaation on

a) määriteltävä kussakin auditoinnissa käytettävät auditointikriteerit ja soveltamisala

b) valittava auditoijat ja suoritettava auditoinnit siten, että auditointiprosessin objektiivisuus ja puolueettomuus voidaan varmistaa

c) varmistettava, että auditointien tuloksista raportoidaan asiaankuuluville johtoon kuuluville henkilöille.

Dokumentoitua tietoa on säilytettävä näyttönä auditointiohjelmien toteuttamisesta ja auditointien tuloksista.

## 9.3 Johdon katselmus (EN)

### 9.3.1 Yleistä (EN)

Ylimmän johdon on katselmoitava organisaation tietoturvallisuuden hallintajärjestelmä suunnitelluin aikavälein varmistaakseen, että se on edelleen soveltuva, tarkoituksenmukainen ja vaikuttava.

### 9.3.2 Johdon katselmusten lähtötiedot (EN)

Johdon katselmuksessa on otettava huomioon

a) aiempien johdon katselmusten vuoksi käynnistettyjen toimenpiteiden tilanne

b) tietoturvallisuuden hallintajärjestelmän kannalta olennaisten ulkoisten ja sisäisten asioiden muutokset

c) tietoturvallisuuden hallintajärjestelmän kannalta olennaisten sidosryhmien tarpeet ja odotukset

d) tietoturvan tasoa koskeva palaute, johon sisältyvät seuraavat kehityssuunnat:

   1) poikkeamat ja korjaavat toimenpiteet

   2) seurannan ja mittauksen tulokset

   3) auditointien tulokset

   4) tietoturvatavoitteiden täyttyminen

e) sidosryhmien antama palaute

f) riskien arvioinnin tulokset sekä riskinkäsittelysuunnitelman tilanne

g) jatkuvan parantamisen mahdollisuudet.

### 9.3.3 Johdon katselmusten tulokset (EN)

Johdon katselmuksen tuloksiin on sisällyttävä päätökset jatkuvan parantamisen mahdollisuuksista sekä tietoturvallisuuden hallintajärjestelmän mahdollisista muutostarpeista.

Dokumentoitua tietoa on säilytettävänä näyttönä johdon katselmusten tuloksista.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 10 Parantaminen (EN)

## 10.1 Jatkuva parantaminen (EN)

Organisaation on parannettava jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuutta, tarkoituksenmukaisuutta ja vaikuttavuutta.

## 10.2 Poikkeamat ja korjaavat toimenpiteet (EN)

Kun havaitaan poikkeama, organisaation on

a) reagoitava poikkeamaan ja tilanteesta riippuen

   1) ryhdyttävä toimiin sen hallitsemiseksi ja korjaamiseksi

   2) käsiteltävä sen seurauksia

b) arvioitava, tarvitaanko toimenpiteitä, joilla poistetaan poikkeaman syyt, jotta poikkeama ei toistu tai esiinny muualla. Tällaisia ovat esimerkiksi

   1) poikkeaman katselmointi

   2) poikkeaman syiden selvittäminen

   3) vastaavien poikkeamien tai niiden mahdollisuuksien etsiminen

c) toteutettava tarvittavat toimenpiteet

d) arvioitava suoritettujen korjaavien toimenpiteiden vaikuttavuus

e) tehtävä muutoksia tietoturvallisuuden hallintajärjestelmään, jos se on tarpeellista.

Korjaavien toimenpiteiden on oltava tarkoituksenmukaisia poikkeamien aiheuttamiin vaikutuksiin nähden.

Organisaation on säilytettävä dokumentoitua tietoa todisteena

f) poikkeamien luonteesta sekä niiden johdosta tehdyistä toimenpiteistä

g) tehtyjen korjaavien toimenpiteiden tuloksista.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Liite A
(velvoittava)
# Tietoturvallisuuden hallintakeinojen viiteluettelo (EN)

Taulukossa A.1 luetellut tietoturvallisuuden hallintakeinot on otettu suoraan standardin ISO/IEC 27002:2022[1] kohdista 5–8. Ne ovat yhteneviä kyseisten kohtien kanssa, ja niitä on käytettävä tämän standardin kohdan 6.1.3 yhteydessä.

**Taulukko A.1 Tietoturvallisuuden hallintakeinot**

| **5** | **Organisaatioon liittyvät hallintakeinot** | |
|---|---|---|
| 5.1 | Tietoturvallisuutta koskevat toimintaperiaatteet | **Hallintakeino**<br>Tietoturvapolitiikka ja kohdennetut toimintaperiaatteet on määriteltävä, ylimmän johdon on hyväksyttävä ne, ne on julkaistava, niistä on viestittävä asiaankuuluville henkilöstön jäsenille ja sidosryhmille, näiltä on saatava kuittaus tietojen vastaanottamisesta ja ne on katselmoitava suunnitelluin aikavälein ja aina kun tapahtuu merkittäviä muutoksia. |
| 5.2 | Tietoturvaroolit ja -vastuut | **Hallintakeino**<br>Tietoturvaroolit ja -vastuut on määriteltävä organisaation tarpeiden mukaisesti. |
| 5.3 | Tehtävien eriyttäminen | **Hallintakeino**<br>Keskenään ristiriitaiset tehtävät ja vastuualueet on eriytettävä toisistaan. |
| 5.4 | Johdon vastuut | **Hallintakeino**<br>Johdon on edellytettävä, että koko henkilöstö toteuttaa tietoturvallisuutta organisaation turvallisuuspolitiikan, kohdennettujen toimintaperiaatteiden ja tietoturvamenettelyjen mukaisesti. |
| 5.5 | Yhteydet viranomaisiin | **Hallintakeino**<br>Organisaation on luotava yhteydet toimivaltaisiin viranomaisiin sekä ylläpidettävä näitä yhteyksiä. |
| 5.6 | Yhteydet osaamisyhteisöihin | **Hallintakeino**<br>Organisaation on luotava ja ylläpidettävä yhteyksiä asiantuntijaryhmiin tai muihin foorumeihin sekä ammatillisiin yhteisöihin. |
| 5.7 | Uhkatiedon seuranta | **Hallintakeino**<br>Tietoturvauhkiin liittyvää tietoa on kerättävä ja analysoitava, jotta kyetään tuottamaan uhkia koskevaa tietoa. |
| 5.8 | Tietoturvallisuus projektinhallinnassa | **Hallintakeino**<br>Tietoturvallisuus on integroitava osaksi projektinhallintaa. |
| 5.9 | Tietojen ja niihin liittyvien omaisuuserien luettelo | **Hallintakeino**<br>On laadittava omaisuusluettelo tieto-omaisuudesta ja muihin niihin liittyvistä omaisuuseristä sekä tieto näiden omistajista. Luetteloa on ylläpidettävä. |
| 5.10 | Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö | **Hallintakeino**<br>Tietojen ja niihin liittyvien omaisuuserien hyväksyttävän käytön säännöt ja menettelyt on yksilöitävä, dokumentoitava ja vietävä käytäntöön. |
| 5.11 | Omaisuuden palauttaminen | **Hallintakeino**<br>Henkilöstön ja muiden sidosryhmien on palautettava kaikki hallussaan oleva organisaation omaisuus työsuhteen tai sopimuksen päättyessä tai muuttuessa. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| | | |
|---|---|---|
| 5.12 | Tiedon luokittelu | **Hallintakeino**<br>Tieto on luokiteltava organisaation tietoturvatarpeiden mukaisesti perustuen luottamuksellisuuteen, eheyteen, saatavuuteen ja keskeisten sidosryhmien vaatimuksiin. |
| 5.13 | Tiedon merkintä | **Hallintakeino**<br>Tiedon merkitsemistä koskevat menettelyt on laadittava ja otettava käyttöön organisaation määrittelemien tiedon luokitteluperiaatteiden mukaisesti. |
| 5.14 | Tietojen siirtäminen | **Hallintakeino**<br>Kaiken tyyppisellä organisaation sisäisellä, organisaatioiden välisellä ja sidosryhmille tapahtuvalla tietojen siirtämisellä on oltava säännöt, menettelyt tai sopimukset. |
| 5.15 | Pääsynhallinta | **Hallintakeino**<br>Säännöt, joilla hallitaan fyysistä ja ohjelmallista pääsyä tietoihin ja niihin liittyviin omaisuuseriin, on laadittava ja toteutettava liiketoimintaa ja tietoturvallisuutta koskevien vaatimusten mukaisesti. |
| 5.16 | Identiteetin hallinta | **Hallintakeino**<br>Identiteettien koko elinkaarta on hallittava. |
| 5.17 | Tunnistautumistiedot | **Hallintakeino**<br>Tunnistautumistietojen osoittamista ja hallintaa on ohjattava hallintaprosessilla, johon sisältyy henkilöstön perehdyttäminen tunnistautumistietojen asianmukaiseen käsittelyyn. |
| 5.18 | Pääsyoikeudet | **Hallintakeino**<br>Pääsyoikeuksia tietoihin ja niihin liittyviin omaisuuseriin on myönnettävä, katselmoitava, muokattava ja poistettava organisaation pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden ja sääntöjen mukaisesti. |
| 5.19 | Tietoturvallisuus toimittajasuhteissa | **Hallintakeino**<br>On määriteltävä ja toteutettava prosessit ja menettelyt, joilla hallitaan toimittajan tuotteiden tai palveluiden käyttöön liittyviä tietoturvariskejä. |
| 5.20 | Toimittajasopimusten tietoturvallisuus | **Hallintakeino**<br>Kunkin toimittajan kanssa on laadittava ja sovittava asianmukaiset tietoturvavaatimukset, jotka perustuvat kyseisen toimittajasuhteen tyyppiin. |
| 5.21 | Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa | **Hallintakeino**<br>On määriteltävä ja toteutettava prosesseja ja menettelyjä, joilla hallitaan tieto- ja viestintäteknisten tuotteiden ja palveluiden toimitusketjuihin liittyviä tietoturvariskejä. |
| 5.22 | Toimittajien palvelujen seuranta, katselmointi ja muutoksenhallinta | **Hallintakeino**<br>Organisaation on säännöllisesti seurattava, katselmoitava, arvioitava toimittajan tietoturvallisuuskäytäntöjä ja palveluiden toimittamista ja hallittava niihin kohdistuvia muutoksia. |
| 5.23 | Pilvipalvelujen tietoturvallisuus | **Hallintakeino**<br>Pilvipalvelujen hankinnan, käytön ja hallinnan sekä käytön lopettamisen prosessit on laadittava organisaation tietoturvavaatimusten mukaisesti. |
| 5.24 | Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu | **Hallintakeino**<br>Organisaation on suunniteltava ja valmistauduttava tietoturvahäiriöiden hallintaan laatimalla tietoturvahäiriöiden hallinnan prosessit, roolit ja vastuut sekä viestimällä niistä. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| | | |
|---|---|---|
| 5.25 | Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen | **Hallintakeino**<br>Organisaation on arvioitava tietoturvatapahtumat ja päätettävä, luokitellaanko ne tietoturvahäiriöiksi. |
| 5.26 | Tietoturvahäiriöihin reagointi | **Hallintakeino**<br>Tietoturvahäiriöihin on reagoitava dokumentoitujen menettelytapojen mukaisesti. |
| 5.27 | Tietoturvahäiriöistä oppiminen | **Hallintakeino**<br>Tietoturvahäiriöistä saatua tietämystä on hyödynnettävä tietoturvallisuuden hallintakeinojen vahvistamisessa ja parantamisessa. |
| 5.28 | Todisteiden kerääminen | **Hallintakeino**<br>Organisaation on laadittava ja toteutettava menettelyt tietoturvatapahtumiin liittyvien todisteiden yksilöimiseen, keräämiseen, muuhun hankkimiseen ja säilyttämiseen. |
| 5.29 | Tietoturvallisuus häiriötilanteessa | **Hallintakeino**<br>Organisaation on suunniteltava, miten se ylläpitää riittävää tietoturvallisuustasoa häiriön aikana. |
| 5.30 | Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa | **Hallintakeino**<br>Tieto- ja viestintätekniikan valmius on suunniteltava, toteutettava, ylläpidettävä ja testattava liiketoiminnan jatkuvuustavoitteiden ja tieto- ja viestintätekniikalle asetettujen jatkuvuusvaatimusten perusteella. |
| 5.31 | Lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset | **Hallintakeino**<br>Lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin perustuvat tietoturvallisuuden kannalta tärkeät vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä, dokumentoitava ja pidettävä ajantalla. |
| 5.32 | Immateriaalioikeudet | **Hallintakeino**<br>Organisaation on toteutettava asianmukaiset menettelyt immateriaalioikeuksien suojaamiseen. |
| 5.33 | Tallenteiden suojaaminen | **Hallintakeino**<br>Tallenteet on suojattava katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta käytöltä ja luvattomalta levittämiseltä. |
| 5.34 | Tietosuoja ja henkilötietojen suojaaminen | **Hallintakeino**<br>Organisaation on tunnistettava ja täytettävä vaatimukset, jotka koskevat tietosuojan ylläpitämistä ja henkilötietojen suojaamista, sisältäen sovellettavat lait ja viranomaismääräykset ja sopimusvaatimukset. |
| 5.35 | Tietoturvallisuuden riippumaton katselmointi | **Hallintakeino**<br>Organisaation tietoturvallisuuden johtamisen toimintamalli ja sen toteutus, johon kuuluu henkilöstö, prosessit ja teknologiat, on katselmoitava riippumattomasti ja suunnitelluin aikavälein tai kun tapahtuu merkittäviä muutoksia. |
| 5.36 | Tietoturvallisuutta koskevien toimintaperiaatteiden, sääntöjen ja standardien noudattaminen | **Hallintakeino**<br>Vaatimustenmukaisuutta suhteessa organisaation tietoturvapolitiikkaan, kohdennettuihin toimintaperiaatteisiin, sääntöihin ja standardeihin on katselmoitava säännöllisesti. |
| 5.37 | Dokumentoidut toimintaohjeet | **Hallintakeino**<br>Tietojenkäsittelypalveluita koskevat toimintaohjeet on dokumentoitava ja niiden on oltava kaikkien niitä tarvitsevien henkilöstön jäsenten saatavilla. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| **6** | **Henkilöstöön liittyvät hallintakeinot** | |
|---|---|---|
| 6.1 | Taustatarkistus | **Hallintakeino**<br>Kaikkien työnhakijoiden taustat on tarkistettava ennen heidän palkkaamistaan organisaatioon sekä jatkuvana prosessina lakien, määräysten ja eettisten normien mukaisesti. Tarkistukset on suhteutettava liiketoiminnallisiin vaatimuksiin, käsiteltävän tiedon luokitukseen ja arvioituihin riskeihin. |
| 6.2 | Työsuhteen ehdot | **Hallintakeino**<br>Työsuhteeseen liittyvissä sopimuksissa on eriteltävä henkilöstön ja organisaation tietoturvallisuutta koskevat vastuut. |
| 6.3 | Tietoturvatietoisuus, -opastus ja -koulutus | **Hallintakeino**<br>Organisaation ja tärkeimpien sidosryhmien henkilöstön on saatava tietoturvaopastusta ja -koulutusta, ja heidän tietojaan organisaation tietoturvapolitiikan, kohdennettujen toimintaperiaatteiden ja menettelyjen muutoksista on päivitettävä säännöllisesti, siinä laajuudessa kuin se on heidän toimenkuvansa kannalta merkityksellistä. |
| 6.4 | Kurinpitoprosessi | **Hallintakeino**<br>Organisaatiolla on oltava muodollinen ja tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, kun henkilöstön tai sidosryhmän edustaja on syyllistynyt tietoturvapolitiikan rikkomukseen. |
| 6.5 | Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut | **Hallintakeino**<br>On määritettävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä on viestittävä olennaisille henkilöille ja sidosryhmille, ja niiden noudattaminen on varmistettava. |
| 6.6 | Salassapito- ja vaitiolositoumukset | **Hallintakeino**<br>Organisaation tiedonsuojaustarpeita kuvastavat salassapito- ja vaitiolositoumukset on yksilöitävä, dokumentoitava ja katselmoitava säännöllisesti, ja niihin on saatava henkilöstön ja muiden olennaisten sidosryhmien hyväksyntä. |
| 6.7 | Etätyöskentely | **Hallintakeino**<br>Tilanteisiin, joissa henkilöstö työskentelee etänä, on toteutettava turvallisuusratkaisut, joilla suojataan organisaation tilojen ulkopuolella käytettyjä, käsiteltyjä tai varastoituja tietoja. |
| 6.8 | Tietoturvatapahtumista raportointi | **Hallintakeino**<br>Organisaation on tarjottava henkilöstölle mekanismi havaittujen tai epäiltyjen tietoturvatapahtumien välittömään raportointiin asianmukaisten kanavien kautta. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| **7** | **Fyysiset hallintakeinot** | |
|---|---|---|
| 7.1 | Fyysiset turva-alueet | **Hallintakeino**<br>Turva-alueet on määriteltävä, ja niitä on käytettävä, mikäli tiedon ja siihen liittyvien omaisuuserien suojaaminen edellyttää turva-alueita. |
| 7.2 | Kulunvalvonta | **Hallintakeino**<br>Turva-alueet on suojattava asianmukaisella kulunvalvonnalla ja sisäänkäynneillä. |
| 7.3 | Toimistojen, tilojen ja laitteistojen suojaus | **Hallintakeino**<br>Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltava ja toteutettava. |
| 7.4 | Fyysisen turvallisuuden valvonta | **Hallintakeino**<br>Toimitiloja on valvottava jatkuvasti luvattoman fyysisen pääsyn varalta. |
| 7.5 | Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan | **Hallintakeino**<br>On suunniteltava ja toteutettava suojaus fyysisiä ja ympäristön aiheuttamia uhkia, kuten luonnonkatastrofeja ja muita infrastruktuuriin kohdistuvia tahallisia tai tahattomia fyysisiä uhkia, vastaan. |
| 7.6 | Turva-alueilla työskentely | **Hallintakeino**<br>On suunniteltava ja toteutettava menettelyt, joiden mukaisesti turva-alueilla työskennellään. |
| 7.7 | Puhdas pöytä ja puhdas näyttö | **Hallintakeino**<br>On määriteltävä ja täytäntöönpantava papereita ja siirrettäviä tallennusvälineitä koskevat puhtaan pöydän säännöt sekä tietojenkäsittelypalveluja koskevat puhtaan näytön säännöt. |
| 7.8 | Laitteiden sijoitus ja suojaus | **Hallintakeino**<br>Laitteet on sijoitettava turvallisesti, ja niitä on suojattava. |
| 7.9 | Toimitilojen ulkopuolelle viedyn omaisuuden turvallisuus | **Hallintakeino**<br>Toimitilojen ulkopuolella olevaa omaisuutta on suojattava. |
| 7.10 | Tallennusvälineet | **Hallintakeino**<br>Tallennusvälineitä on hallittava koko niiden elinkaaren ajan aina hankinnasta, käyttöön, kuljettamiseen ja hävittämiseen organisaation luokitteluperiaatteiden ja käsittelyvaatimusten mukaisesti. |
| 7.11 | Tukipalvelut | **Hallintakeino**<br>Tietojenkäsittelypalvelut on suojattava sähkökatkoilta ja muilta tukipalveluiden vikojen aiheuttamilta häiriöiltä. |
| 7.12 | Kaapeloinnin turvallisuus | **Hallintakeino**<br>Sähkökaapelointi sekä tietoa siirtävä tai tietotekniikkapalveluita tukeva tietoliikennekaapelointi on suojattava salakuuntelulta, häirinnältä ja vahingoittumiselta. |
| 7.13 | Laitteiden huolto | **Hallintakeino**<br>Laitteita on huollettava asianmukaisesti, jotta tietojen saatavuus, eheys ja luottamuksellisuus voidaan varmistaa. |
| 7.14 | Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen | **Hallintakeino**<br>Laitteiden tallennettua tietoa sisältävät osat on tarkistettava, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmistot on poistettu tai tuhottu turvallisesti ennen laitteen käytöstä poistamista tai kierrättämistä. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| **8** | **Teknologiset hallintakeinot** | |
|---|---|---|
| 8.1 | Käyttäjien päätelaitteet | **Hallintakeino**<br>Käyttäjien päätelaitteille tallennetut, niillä käsiteltävät tai niiden kautta käytettävät tiedot on suojattava. |
| 8.2 | Ylläpito-oikeudet | **Hallintakeino**<br>Ylläpito-oikeuksien jakamista ja käyttöä on rajoitettava ja hallittava. |
| 8.3 | Tietoihin pääsyn rajoittaminen | **Hallintakeino**<br>Pääsyä tietoihin ja muihin niihin liittyviin omaisuuseriin on rajoitettava pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden mukaisesti. |
| 8.4 | Pääsy lähdekoodiin | **Hallintakeino**<br>Lähdekoodien, kehittämistyökalujen ja ohjelmistokirjastojen luku- ja kirjoitusoikeuksia on hallittava asianmukaisesti. |
| 8.5 | Turvallinen todentaminen | **Hallintakeino**<br>On toteutettava turvallisen pääsyn teknologiat ja menettelyt, jotka perustuvat tietoja koskeviin pääsyrajoituksiin ja pääsynhallintaa koskeviin kohdennettuihin toimintaperiaatteisiin. |
| 8.6 | Kapasiteetinhallinta | **Hallintakeino**<br>Resurssien käyttöä on seurattava, ja se on mukautettava senhetkisten ja odotettujen kapasiteettivaatimusten mukaisesti. |
| 8.7 | Haittaohjelmilta suojautuminen | **Hallintakeino**<br>Haittaohjelmilta suojautuminen on toteutettava, ja sitä on tuettava käyttäjien haittaohjelmia koskevan tietoisuuden parantamisella. |
| 8.8 | Teknisten haavoittuvuuksien hallinta | **Hallintakeino**<br>Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista on hankittava tietoa. Organisaation altistuminen näille haavoittuvuuksille on arvioitava, ja niihin liittyviin riskeihin on vastattava asianmukaisilla toimenpiteillä. |
| 8.9 | Konfiguraationhallinta | **Hallintakeino**<br>Laitteistojen, ohjelmistojen, palveluiden ja verkkojen konfiguraatiot, mukaan lukien turvallisuuskonfiguraatiot, on laadittava, dokumentoitava ja toteutettava, ja niitä on seurattava ja katselmoitava. |
| 8.10 | Tietojen poistaminen | **Hallintakeino**<br>Tietojärjestelmiin, laitteisiin tai mihin tahansa muuhun tallennusvälineeseen varastoidut tiedot on poistettava, kun niitä ei enää tarvita. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| | | |
|---|---|---|
| 8.11 | Tietojen peittäminen | **Hallintakeino**<br>Tietojen peittämistä on käytettävä organisaation pääsynhallintaa koskevien ja muiden asiaan liittyvien kohdennettujen toimintaperiaatteiden sekä liiketoiminnallisten vaatimusten mukaisesti ottaen huomioon olennainen lainsäädäntö. |
| 8.12 | Tietovuotojen estäminen | **Hallintakeino**<br>Tietovuotojen estämistoimia on sovellettava järjestelmiin, verkkoihin ja muihin laitteisiin, joissa käsitellään, varastoidaan tai siirretään arkaluonteisia tietoja. |
| 8.13 | Tietojen varmuuskopiointi | **Hallintakeino**<br>Tiedoista, ohjelmistoista ja järjestelmistä on otettava varmuuskopiot ja ne on testattava säännöllisesti varmuuskopiointia koskevien kohdennettujen toimintaperiaatteiden mukaisesti. |
| 8.14 | Tietojenkäsittelypalvelujen vikasietoisuus | **Hallintakeino**<br>Tietojenkäsittelypalvelut on toteutettava niin vikasietoisina, että saatavuusvaatimukset täyttyvät. |
| 8.15 | Lokikirjaukset | **Hallintakeino**<br>On luotava tapahtumalokeja, joihin tallennetaan toiminnot, poikkeamat, vikaantumiset ja muut olennaiset tapahtumat. Nämä lokit on säilytettävä, ja niitä on suojattava ja analysoitava. |
| 8.16 | Valvontatoiminnot | **Hallintakeino**<br>Verkkoja, järjestelmiä ja sovelluksia on valvottava poikkeavan käyttäytymisen varalta, ja mahdollisia tietoturvahäiriöitä on arvioitava asianmukaisin toimenpitein. |
| 8.17 | Kellojen synkronointi | **Hallintakeino**<br>Organisaatiossa käytettävien tietojenkäsittelyjärjestelmien kellojen on oltava synkronoituja hyväksyttävien aikalähteiden kanssa. |
| 8.18 | Ylläpito- ja hallintasovellukset | **Hallintakeino**<br>Järjestelmän ja sovellusten hallintakeinot ohittamaan kykenevien apuohjelmien käyttöä on rajoitettava, ja niitä on hallittava tarkasti. |
| 8.19 | Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin | **Hallintakeino**<br>On toteutettava menettelyt ja toimet, joilla hallitaan turvallisesti ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin. |
| 8.20 | Verkkoturvallisuus | **Hallintakeino**<br>Verkkoja ja verkossa olevia laitteita on suojattava, hallittava ja valvottava, jotta voidaan suojata järjestelmissä ja sovelluksissa oleva tieto. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Taulukko A.1** *(jatkuu)*

| | | |
|---|---|---|
| 8.21 | Verkkopalvelujen turvaaminen | **Hallintakeino**<br>Kaikkien verkkopalvelujen turvamekanismit, palvelutasot ja palveluvaatimukset on yksilöitävä ja toteutettava, ja niitä on seurattava. |
| 8.22 | Verkkojen eriyttäminen | **Hallintakeino**<br>Tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät on eriytettävä toisistaan organisaation verkoissa. |
| 8.23 | Verkkosuodatus | **Hallintakeino**<br>Pääsyä ulkoisiin verkkosivustoihin on hallittava, jotta voidaan vähentää altistumista haitallisille sisällöille. |
| 8.24 | Salauksen käyttö | **Hallintakeino**<br>Säännöt salauksen vaikuttavaan käyttöön, sisältäen salausavainten hallinnan, on määriteltävä ja toteutettava. |
| 8.25 | Turvallinen kehittämisen elinkaari | **Hallintakeino**<br>Ohjelmistojen ja järjestelmien turvallista kehittämistä koskevat säännöt on laadittava, ja niitä on sovellettava. |
| 8.26 | Sovelluksia koskevat turvallisuusvaatimukset | **Hallintakeino**<br>Tietoturvavaatimukset on tunnistettava, määriteltävä ja hyväksyttävä, kun suunnitellaan tai hankitaan sovelluksia. |
| 8.27 | Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet | **Hallintakeino**<br>Turvallisen järjestelmäarkkitehtuurin ja -suunnittelun periaatteet on laadittava ja dokumentoitava. Niitä on ylläpidettävä, ja niitä on sovellettava kaikkiin tietojärjestelmien kehitystoimiin. |
| 8.28 | Turvallinen ohjelmointi | **Hallintakeino**<br>Ohjelmistokehityksessä on sovellettava turvallisen ohjelmoinnin periaatteita. |
| 8.29 | Tietoturvatestaus kehitys- ja hyväksyntävaiheissa | **Hallintakeino**<br>Kehittämisen elinkaareen liittyvät turvallisuuden testiprosessit on määriteltävä ja toteutettava. |
| 8.30 | Ulkoistettu kehittäminen | **Hallintakeino**<br>Organisaation on ohjattava, valvottava ja katselmoitava toimintoja, jotka liittyvät ulkoistettuun järjestelmäkehitykseen. |
| 8.31 | Kehitys-, testaus- ja tuotantoympäristöjen erottaminen | **Hallintakeino**<br>Kehitys-, testaus- ja tuotantoympäristöt on erotettava, ja niitä on suojattava. |
| 8.32 | Muutoksenhallinta | **Hallintakeino**<br>Tietojenkäsittelypalveluihin ja tietojärjestelmiin tehtäviä muutoksia on hallittava muutoksenhallintamenettelyillä. |
| 8.33 | Testauksessa käytettävät tiedot | **Hallintakeino**<br>Testauksessa käytettävät tiedot on valittava, suojattava ja hallittava asianmukaisesti. |
| 8.34 | Tietojärjestelmien suojaus auditointitestauksen aikana | **Hallintakeino**<br>Testaajan ja asiaankuuluvan johdon on suunniteltava ja sovittava auditointitestauksista ja muista käytössä olevien järjestelmien arvioinnin sisältävistä varmennustoiminnoista. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Kirjallisuus (EN)

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# SFS-EN ISO/IEC 27001:2023

*Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022)*

## Contents

Page





Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

## Foreword (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 or 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) or the IEC list of patent declarations received (see https://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. In the IEC, see 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 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

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 and www.iec.ch/national-committees.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Introduction (FI)

## 0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

## 0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 1 Scope (FI)

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

# 2 Normative references (FI)

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies.
For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

# 3 Terms and definitions (FI)

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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/

# 4 Context of the organization (FI)

## 4.1 Understanding the organization and its context (FI)

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

## 4.2 Understanding the needs and expectations of interested parties (FI)

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 4.3 Determining the scope of the information security management system (FI)

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

### 4.4 Information security management system (FI)

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

## 5 Leadership (FI)

### 5.1 Leadership and commitment (FI)

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 5.2 Policy (FI)

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

### 5.3 Organizational roles, responsibilities and authorities (FI)

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management.

NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

## 6 Planning (FI)

### 6.1 Actions to address risks and opportunities (FI)

#### 6.1.1 General (FI)

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 6.1.2 Information security risk assessment (FI)

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

   1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

   2) identify the risk owners;

d) analyses the information security risks:

   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

   3) determine the levels of risk;

e) evaluates the information security risks:

   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

### 6.1.3 Information security risk treatment (FI)

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

   NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

   NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

   NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

d) produce a Statement of Applicability that contains:

— the necessary controls (see 6.1.3 b) and c));

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].

## 6.2 Information security objectives and planning to achieve them (FI)

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed; and

l) how the results will be evaluated.

## 6.3 Planning of changes (FI)

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 7 Support (FI)

## 7.1 Resources (FI)

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

## 7.2 Competence (FI)

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

## 7.3 Awareness (FI)

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

## 7.4 Communication (FI)

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

## 7.5 Documented information (FI)

### 7.5.1 General (FI)

The organization's information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

### 7.5.2 Creating and updating (FI)

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

### 7.5.3 Control of documented information (FI)

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

## 8 Operation (FI)

### 8.1 Operational planning and control (FI)

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 8.2 Information security risk assessment (FI)

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

### 8.3 Information security risk treatment (FI)

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

## 9 Performance evaluation (FI)

### 9.1 Monitoring, measurement, analysis and evaluation (FI)

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

### 9.2 Internal audit (FI)

#### 9.2.1 General (FI)

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

   1) the organization's own requirements for its information security management system;

   2) the requirements of this document;

b) is effectively implemented and maintained.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

### 9.2.2 Internal audit programme (FI)

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

## 9.3 Management review (FI)

### 9.3.1 General (FI)

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

### 9.3.2 Management review inputs (FI)

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

   1) nonconformities and corrective actions;

   2) monitoring and measurement results;

   3) audit results;

   4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

### 9.3.3 Management review results (FI)

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# 10 Improvement (FI)

## 10.1 Continual improvement (FI)

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

## 10.2 Nonconformity and corrective action (FI)

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

   1) take action to control and correct it;

   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity; and

   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Annex A
(normative)
# Information security controls reference (FI)

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

**Table A.1 Information security controls**

| **5** | **Organizational controls** | |
|---|---|---|
| 5.1 | Policies for information security | **Control**<br>Information security policy and topic-specific policies shall 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. |
| 5.2 | Information security roles and responsibilities | **Control**<br>Information security roles and responsibilities shall be defined and allocated according to the organization needs. |
| 5.3 | Segregation of duties | **Control**<br>Conflicting duties and conflicting areas of responsibility shall be segregated. |
| 5.4 | Management responsibilities | **Control**<br>Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization. |
| 5.5 | Contact with authorities | **Control**<br>The organization shall establish and maintain contact with relevant authorities. |
| 5.6 | Contact with special interest groups | **Control**<br>The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. |
| 5.7 | Threat intelligence | **Control**<br>Information relating to information security threats shall be collected and analysed to produce threat intelligence. |
| 5.8 | Information security in project management | **Control**<br>Information security shall be integrated into project management. |
| 5.9 | Inventory of information and other associated assets | **Control**<br>An inventory of information and other associated assets, including owners, shall be developed and maintained. |
| 5.10 | Acceptable use of information and other associated assets | **Control**<br>Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. |
| 5.11 | Return of assets | **Control**<br>Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement. |
| 5.12 | Classification of information | **Control**<br>Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| 5.13 | Labelling of information | **Control**<br>An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |
| 5.14 | Information transfer | **Control**<br>Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. |
| 5.15 | Access control | **Control**<br>Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. |
| 5.16 | Identity management | **Control**<br>The full life cycle of identities shall be managed. |
| 5.17 | Authentication information | **Control**<br>Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. |
| 5.18 | Access rights | **Control**<br>Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. |
| 5.19 | Information security in supplier relationships | **Control**<br>Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. |
| 5.20 | Addressing information security within supplier agreements | **Control**<br>Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. |
| 5.21 | Managing information security in the information and communication technology (ICT) supply chain | **Control**<br>Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. |
| 5.22 | Monitoring, review and change management of supplier services | **Control**<br>The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. |
| 5.23 | Information security for use of cloud services | **Control**<br>Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. |
| 5.24 | Information security incident management planning and preparation | **Control**<br>The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. |
| 5.25 | Assessment and decision on information security events | **Control**<br>The organization shall assess information security events and decide if they are to be categorized as information security incidents. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| 5.26 | Response to information security incidents | **Control**<br>Information security incidents shall be responded to in accordance with the documented procedures. |
| 5.27 | Learning from information security incidents | **Control**<br>Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. |
| 5.28 | Collection of evidence | **Control**<br>The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. |
| 5.29 | Information security during disruption | **Control**<br>The organization shall plan how to maintain information security at an appropriate level during disruption. |
| 5.30 | ICT readiness for business continuity | **Control**<br>ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |
| 5.31 | Legal, statutory, regulatory and contractual requirements | **Control**<br>Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date. |
| 5.32 | Intellectual property rights | **Control**<br>The organization shall implement appropriate procedures to protect intellectual property rights. |
| 5.33 | Protection of records | **Control**<br>Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. |
| 5.34 | Privacy and protection of personal identifiable information (PII) | **Control**<br>The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. |
| 5.35 | Independent review of information security | **Control**<br>The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. |
| 5.36 | Compliance with policies, rules and standards for information security | **Control**<br>Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed. |
| 5.37 | Documented operating procedures | **Control**<br>Operating procedures for information processing facilities shall be documented and made available to personnel who need them. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| **6** | **People controls** | |
| 6.1 | Screening | **Control**<br>Background verification checks on all candidates to become personnel shall 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. |
| 6.2 | Terms and conditions of employment | **Control**<br>The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. |
| 6.3 | Information security awareness, education and training | **Control**<br>Personnel of the organization and relevant interested parties shall 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. |
| 6.4 | Disciplinary process | **Control**<br>A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. |
| 6.5 | Responsibilities after termination or change of employment | **Control**<br>Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. |
| 6.6 | Confidentiality or non-disclosure agreements | **Control**<br>Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. |
| 6.7 | Remote working | **Control**<br>Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises. |
| 6.8 | Information security event reporting | **Control**<br>The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. |
| **7** | **Physical controls** | |
| 7.1 | Physical security perimeters | **Control**<br>Security perimeters shall be defined and used to protect areas that contain information and other associated assets. |
| 7.2 | Physical entry | **Control**<br>Secure areas shall be protected by appropriate entry controls and access points. |
| 7.3 | Securing offices, rooms and facilities | **Control**<br>Physical security for offices, rooms and facilities shall be designed and implemented. |
| 7.4 | Physical security monitoring | **Control**<br>Premises shall be continuously monitored for unauthorized physical access. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| 7.5 | Protecting against physical and environmental threats | **Control**<br>Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |
| 7.6 | Working in secure areas | **Control**<br>Security measures for working in secure areas shall be designed and implemented. |
| 7.7 | Clear desk and clear screen | **Control**<br>Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. |
| 7.8 | Equipment siting and protection | **Control**<br>Equipment shall be sited securely and protected. |
| 7.9 | Security of assets off-premises | **Control**<br>Off-site assets shall be protected. |
| 7.10 | Storage media | **Control**<br>Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. |
| 7.11 | Supporting utilities | **Control**<br>Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. |
| 7.12 | Cabling security | **Control**<br>Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. |
| 7.13 | Equipment maintenance | **Control**<br>Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. |
| 7.14 | Secure disposal or re-use of equipment | **Control**<br>Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |
| **8** | **Technological controls** | |
| 8.1 | User end point devices | **Control**<br>Information stored on, processed by or accessible via user end point devices shall be protected. |
| 8.2 | Privileged access rights | **Control**<br>The allocation and use of privileged access rights shall be restricted and managed. |
| 8.3 | Information access restriction | **Control**<br>Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |
| 8.4 | Access to source code | **Control**<br>Read and write access to source code, development tools and software libraries shall be appropriately managed. |
| 8.5 | Secure authentication | **Control**<br>Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| 8.6 | Capacity management | **Control**<br>The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |
| 8.7 | Protection against malware | **Control**<br>Protection against malware shall be implemented and supported by appropriate user awareness. |
| 8.8 | Management of technical vulnerabilities | **Control**<br>Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |
| 8.9 | Configuration management | **Control**<br>Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. |
| 8.10 | Information deletion | **Control**<br>Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. |
| 8.11 | Data masking | **Control**<br>Data masking shall 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. |
| 8.12 | Data leakage prevention | **Control**<br>Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. |
| 8.13 | Information backup | **Control**<br>Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. |
| 8.14 | Redundancy of information processing facilities | **Control**<br>Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |
| 8.15 | Logging | **Control**<br>Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. |
| 8.16 | Monitoring activities | **Control**<br>Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. |
| 8.17 | Clock synchronization | **Control**<br>The clocks of information processing systems used by the organization shall be synchronized to approved time sources. |
| 8.18 | Use of privileged utility programs | **Control**<br>The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. |
| 8.19 | Installation of software on operational systems | **Control**<br>Procedures and measures shall be implemented to securely manage software installation on operational systems. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

**Table A.1** *(continued)*

| | | |
|---|---|---|
| 8.20 | Networks security | **Control**<br>Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. |
| 8.21 | Security of network services | **Control**<br>Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. |
| 8.22 | Segregation of networks | **Control**<br>Groups of information services, users and information systems shall be segregated in the organization's networks. |
| 8.23 | Web filtering | **Control**<br>Access to external websites shall be managed to reduce exposure to malicious content. |
| 8.24 | Use of cryptography | **Control**<br>Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |
| 8.25 | Secure development life cycle | **Control**<br>Rules for the secure development of software and systems shall be established and applied. |
| 8.26 | Application security requirements | **Control**<br>Information security requirements shall be identified, specified and approved when developing or acquiring applications. |
| 8.27 | Secure system architecture and engineering principles | **Control**<br>Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities. |
| 8.28 | Secure coding | **Control**<br>Secure coding principles shall be applied to software development. |
| 8.29 | Security testing in development and acceptance | **Control**<br>Security testing processes shall be defined and implemented in the development life cycle. |
| 8.30 | Outsourced development | **Control**<br>The organization shall direct, monitor and review the activities related to outsourced system development. |
| 8.31 | Separation of development, test and production environments | **Control**<br>Development, testing and production environments shall be separated and secured. |
| 8.32 | Change management | **Control**<br>Changes to information processing facilities and information systems shall be subject to change management procedures. |
| 8.33 | Test information | **Control**<br>Test information shall be appropriately selected, protected and managed. |
| 8.34 | Protection of information systems during audit testing | **Control**<br>Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.

# Bibliography (FI)

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*



Tämä julkaisu on ladattu SFS Online-palvelusta (sop. nro ) 28.08.2024.
Lataaja: AC7750@jamk.fi. Vain Jyväskylän ammattikorkeakoulu käyttöön.