

Informationssikkerhedspolitik gyldig fra ??.

Informationssikkerhedspolitik for <Virksomhedsnavn>

1 Målsætning/formål

Sikkerhedspolitikken skal til enhver tid understøtte <virksomhedsnavn>s værdigrundlag og vision samt de strategiske mål, der er i IT-strategien.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til <virksomhedsnavn>, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinier.

<Virksomhedsnavn> ønsker derfor at opretholde og løbende udbygge et IT sikkerhedsniveau på højde med de krav, som skitseres i 'Den fællesstatslige standard for informationssikkerhed' (DS 484 basale krav). Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at <virksomhedsnavn> fremstår troværdig både nationalt og internationalt.

For at fastholde <virksomhedsnavn>s troværdighed skal det sikres, at information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som <virksomhedsnavn>s mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødig besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at <virksomhedsnavn>s image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Målene er derfor, at:

- opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og databas - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

Ovenstående mål skal konkretiseres i Service Level Agreements (SLAs) og kontrakter overfor samarbejdspartnere.

Regler og retningslinjer fra informationssikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

2. Omfang

Sikkerhedskonceptet omfatter følgende:

Informationssikkerhedspolitik gyldig fra ??.

- En informationssikkerhedspolitik, der godkendes af direktionen på baggrund af indstilling fra Udvalget for informationssikkerhed.
- En informationssikkerhedshåndbog, der uddyber informationssikkerhedspolitikken, fastlægges af Udvalget for informationssikkerhed.
- Sikkerhedsinstrukser og -procedurer, som formuleres af respektive ejere og liniechefer ud fra krav og retningslinier i informationssikkerhedshåndbogen
- En 12-trins styringsmodel opbygget efter Plan, Do, Check, Act principperne i BS 7799 Del 2 : 2002 og anbefalet af det fællesstatslige sikkerhedsprojekt.

3. Gyldighedsområde

Politikken er gældende for alle <virksomhedsnavn>s informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i <virksomheden> eller af samarbejdspartnere. Dette inkluderer f.eks. alle data om personale, data om finansielle forhold, alle data som bidrager til administrationen af virksomheden, produktionsdata og anlægsdata samt informationer som er overladt til <virksomhedsnavn> af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information, som kun er til intern brug.

Informationssikkerhedspolitikken har gyldighed for alle ansatte i <virksomhedsnavn> og al anvendelse af <virksomhedsnavn>s informationsaktiver.

4. Organisation og ansvar

Det delegerede sikkerhedsrelaterede ansvar og den tilhørende myndighed er generisk beskrevet/rollefordelt i Bilag 1 til denne politik.

5. Beredskabsplanlægning

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici i mod sikringsomkostninger og udmøntes i SLAs.

<Virksomhedsnavn>s beredskabsplan aftales med KIT og indarbejdes i dennes overordnede beredskabsplan. Heri skal hhv. <virksomhedsnavn>s og partnernes ansvar for sikkerhedskopiering og nødplaner entydigt præciseres.

Beredskabsplanerne skal omfatte:

- Skadebegrensende tiltag
- Etablering af temporære nødløsninger
- Genetablering af permanent løsning

Beredskabsplanerne skal ajourføres og testes løbende – og minimum en gang om året.

6. Sanktionering

Medarbejdere, der bryder de gældende informationssikkerhedsbestemmelser i <virksomhedsnavn>, kan straffes disciplinært. De nærmere regler om dette fastsættes i overensstemmelse med den gældende personalepolitik.

Bilag 1 Organisation og ansvar

1. Udvalget for informationssikkerhed

Udvalget består af:

Informationssikkerhedspolitik gyldig fra ??.

- Administrationschefen (formand for udvalget)
- <Virksomheden>'s IT-sikkerhedskoordinator (sekretær for udvalget), samt repræsentanter fra relevante aktører/interessenter i <virksomhedsnavn>
- Kontorchefen for ***
- En repræsentant for *** på ledelsesniveau
- En – eller flere – repræsentanter for brugerfunktionerne

Udvalget er normgivende og fastsætter på grundlag af den vedtagne informationssikkerhedspolitik de principper/retningslinier, der skal sikre målopfyldelsen.

Udvalget behandler alle sikkerhedsspørgsmål af principiel karakter.

Udvalget foretager en årlig vurdering af informationssikkerhedspolitikken og de tilknyttede sikkerhedsretningslinier – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidigt, om der er behov for fornyet risikovurdering/konsekvensanalyse.

Udvalget kan ad hoc lade sig supplere med faglig assistance fra IT-Sikkerhedsfunktionen

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.2 (også DS 484:2005 reference)

*** den interne IT-sikkerhedsfunktion.

2. IT Sikkerhedsfunktionen

Formuleres efter situationen

På grund af <virksomhedsnavn>s store grad af outsourcing af drift og support til Koncern-IT og derigennem ofte til større, professionelle samarbejdspartnere er det ikke hensigtsmæssigt at operere med en større særskilt/funktionsadskilt IT Sikkerhedsafdeling/-funktion. I stedet løses opgaverne primært ved:

- at tage hensyn hertil i aftalegrundlag med samarbejdspartnere, f.eks. ved at pålægge samarbejdspartnere at foretage forskellige former for kontrol og opfølgning og rapportere herom til Udvalget for informationssikkerhed
- at iværksætte egne revisionsopgaver og/eller sikkerhedsundersøgelser i det omfang Udvalget for informationssikkerhed finder det fornødent.

Funktionen har ansvar for:

- At udarbejde og vedligeholde sikkerhedshåndbogen indeholdende sikkerhedsprincipper for informations anvendelsen – evt. med ekstern assistance
- At udarbejde relevante sikkerhedskrav, der operationaliserer informationssikkerhedspolitikken – evt. med ekstern assistance
- At foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende
- At behandle dispensationsansøgninger for begrundede afgivelser i forhold til retningslinierne og rapportere disse til Udvalget for informationssikkerhed
- At holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
- At koordinere relevante initiativer med de øvrige aktører i koncernsamarbejdet

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.2 (også DS 484:2005 reference)

Informationssikkerhedspolitik gyldig fra ??.

3. Linieledelsen

Den enkelte chef i linien – herunder direktionen - har ansvar for:

- At informationssikkerhedspolitikken og de regler, der er relevante for hans/hendes ansvarsområde, er kendte og efterleves
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer og at disse efterleves
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for <virksomheden>s/kontorets område
- At der ved installation af nye systemer gennemføres en forudgående sikkerheds-/risikovurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Resultatet rapporteres til IT Sikkerhedsfunktionen
- At retningslinierne for ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholdes

Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig betydning for <virksomhedsnavn>. Som supplement hertil skal dokumentationen tilhørende disse områder også holdes ajourført og evt. udbygges.

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.1 (også DS 484:2005 reference)

4. Systemejere

System ejere har ansvar for:

- at der udarbejdes en kravspecifikation som tager eksplisit hensyn til sikkerhedsmæssige forhold forud for enhver systemudvikling/-ændring/-anskaffelse/-opdatering – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at Change Management retningslinierne følges ved enhver ændring af systemet
- at der ved idriftsætning af systemet foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til systemet i h.t. retningslinierne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for systemadministrationen.

5. Dataejere

Dataejer har ansvar for:

- at der udarbejdes en risikovurdering i h.t. kravene hertil – for systemtilknyttede data i samarbejde med systemejeren
- at der inden indrapportering af data i systemer foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil

Informationssikkerhedspolitik gyldig fra ??.

- at autorisere adgangen til data i h.t. retningslinierne herfor samt at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for dataadministrationen.

6 Ejere af fysiske aktivier

Alle fysiske aktiver får udpeget/ tildelt en ejer.

Såfremt aktivet er omfattet af en aftale om hosting, tages der hensyn hertil i aftalegrundlaget med samarbejdspartneren, f.eks. ved at pålægge samarbejdspartneren at foretage forskellige former for kontrol og opfølgning og rapportere herom.

Ejeren af det fysiske aktiv har ansvar for:

- at der udarbejdes en kravspecifikation ved placering, indretning, forandring m.v. som tager eksplisit hensyn til sikkerhedsmæssige forhold – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at der ved ibrugtagning af lokaler/udstyr foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til lokalerne/ udstyret i h.t. retningslinierne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for fysisk sikkerhed og adgangsadministrationen.

7. Medarbejdere

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsplanet. Hvor dette ikke er praktisk eller økonomisk hensigtsmæssigt, skal kompenserende kontroller indføres.

Den enkelte medarbejder har ansvar for:

- At overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef og til IT-Sikkerhedsfunktionen

8. Samarbejdspartnere

Samarbejdspartnere – herunder KIT - bærer p.g.a. det valgte koncept en meget væsentlig del af ansvaret for at det valgte sikkerhedsniveau etableres og opretholdes.

Samarbejdspartnerne har ansvar for:

Informationssikkerhedspolitik gyldig fra ??.

- At <virksomhedsnavn>s informationssikkerhedspolitik og de regler, der er relevante for deres ansvarsområde, er kendte og efterleves – mest hensigtsmæssigt ved at egne sikkerhedspolitikker og regler til enhver tid afspejler krav fra < virksomhedsnavn >
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer, herunder tiltrædelseserklæringen
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for samarbejdspartnerens område
- At der ved installation af nye og modifikation af eksisterende interne systemer og komponenter med påvirkningsmulighed til <virksomhedsnavn>s informationsaktiver gennemføres en forudgående risiko-/sikkerhedsvurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Hændelsen og resultatet rapporteres via egen sikkerhedsorganisation til <virksomhedsnavn>s IT Sikkerhedsfunktion

IT-Sikkerhedsregler/håndbog -

Indholdsfortegnelse for <virksomhedsnavn>s IT-sikkerhedshåndbog

Dette er en oversigt over punkter i IT-sikkerhedshåndbogen, udarbejdet af Dansk Standard. For nærmere uddybelse af samtlige underpunkter, se 'Forøg virksomhedens informationssikkerhed', et hæfte udarbejdet gennem et samarbejde mellem Dansk Standard Center for ICT, ITEK og Dansk Industri.

Hæftet kan erhverves i Dansk Industri's butik på www.di.dk

DS 484:2005 struktur.

Indholdsfortegnelse

Indledning

IT sikkerhedsorganisation i <virksomhedsnavn>

Informationssikkerhedspolitik gyldig fra ??.

4. RISIKOVURDERING OG -HÅNDTERING

- 4.1. VURDERING AF SIKKERHEDSRISICI
- 4.2. RISIKOHÅNDTERING

5. OVERORDNEDE RETNINGSLINIER

- 5.1. INFORMATIONSSIKKERHEDSSTRATEGI
 - 5.1.1. Formulering af en informationssikkerhedspolitik
 - 5.1.2. Løbende vedligeholdelse

6. ORGANISERING AF INFORMATIONSSIKKERHED

- 6.1. INTERNE ORGANISATORISKE FORHOLD
 - 6.1.1. Ledelsens rolle
 - 6.1.2. Koordinering af informationssikkerhed
 - 6.1.3. Ansvarsplacering
 - 6.1.4. Godkendelsesprocedure ved anskaffelser
 - 6.1.5. Tavshedserklæringer
 - 6.1.6. Kontakt med myndigheder
 - 6.1.7. Fagligt samarbejde med grupper og organisationer
 - 6.1.8. Periodisk opfølgning
- 6.2. EKSTERNE SAMARBEJDSPARTNERE
 - 6.2.1. Identifikation af risici i forbindelse med eksternt samarbejde
 - 6.2.2. Sikkerhedsforhold i relation til kunder
 - 6.2.3. Samarbejdsaftaler

7. STYRING AF INFORMATIONSRELATEREDE AKTIVER

- 7.1. IDENTIFIKATION AF OG ANSVAR FOR INFORMATIONSRELATEREDE AKTIVER
 - 7.1.1. Fortegnelse over informationsaktiver
 - 7.1.2. Ejerskab
 - 7.1.3. Accepteret brug af aktiver
- 7.2. KLASSEFIKATION AF INFORMATIONER OG DATA
 - 7.2.1. Klassifikation
 - 7.2.2. Mærkning og håndtering af informationer og data

8. MEDARBEJDERSIKKERHED

- 8.1. SIKKERHEDSPROCEDURE FØR ANSÆTTELSE
 - 8.1.1. Opgaver og ansvar
 - 8.1.2. Efterprøvning
 - 8.1.3. Aftale om ansættelse
- 8.2. ANSÆTTELSESFORHOLDET
 - 8.2.1. Ledelsens ansvar
 - 8.2.2. Uddannelse, træning og oplysning om informationssikkerhed
 - 8.2.3. Sanktioner
- 8.3. ANSÆTTELSENS OPHØR
 - 8.3.1. Ansvar ved ansættelsens ophør
 - 8.3.2. Returnering af aktiver
 - 8.3.3. Inddragelse af rettigheder

9. FYSISK SIKKERHED

- 9.1. SIKRE OMRÅDER
 - 9.1.1. Fysisk afgrænsning
 - 9.1.2. Fysisk adgangskontrol
 - 9.1.3. Sikring af kontorer, lokaler og udstyr

Informationssikkerhedspolitik gyldig fra ??.

- 9.1.4. Beskyttelse mod eksterne trusler
- 9.1.5. Arbejdsmæssige forhold i sikre områder
- 9.1.6. Områder til af- og pålæsning med offentlig adgang.
- 9.2. BESKYTTELSE AF UDSTYR
 - 9.2.1. Placering af udstyr
 - 9.2.2. Forsyningssikkerhed
 - 9.2.3. Sikring af kabler
 - 9.2.4. Udstyrs og anlægs vedligeholdelse
 - 9.2.5. Sikring af udstyr uden for virksomhedens overvågning
 - 9.2.6. Sikker bortskaffelse eller genbrug af udstyr
 - 9.2.7. Fjernelse af virksomhedens informationsaktiver

10. STYRING AF NETVÆRK OG DRIFT

- 10.1. OPERATIONELLE PROCEDURER OG ANSVARSMRÅDER
 - 10.1.1. Driftsafviklingsprocedurer
 - 10.1.2. Ændringsstyring
 - 10.1.3. Funktionsadskillelse
 - 10.1.4. Adskillelse mellem udvikling, test og drift
- 10.2. EKSTERN SERVICELEVERANDØR
 - 10.2.1. Serviceleverancen
 - 10.2.2. Overvågning og revision af serviceleverandøren
 - 10.2.3. Styring af ændringer hos ekstern serviceleverandør
- 10.3. STYRING AF DRIFTSMILJØET
 - 10.3.1. Kapacitetsstyring
 - 10.3.2. Godkendelse af nye eller ændrede systemer
- 10.4. SKADEVOLDENDE PROGRAMMER OG MOBIL KODE
 - 10.4.1. Beskyttelse mod skadevoldende programmer
 - 10.4.2. Beskyttelse mod mobil kode
- 10.5. SIKKERHEDSKOPIERING
 - 10.5.1. Sikkerhedskopiering
- 10.6. NETVÆRKSSIKKERHED
 - 10.6.1. Netværket
 - 10.6.2. Netværkstjenester
- 10.7. DATABÆRENDE MEDIER
 - 10.7.1. Bærbare datamedier
 - 10.7.2. Destruktion af datamedier
 - 10.7.3. Beskyttelse af datamediers indhold
 - 10.7.4. Beskyttelse af systemdokumentation
- 10.8. INFORMATIONSUDVEKSLING
 - 10.8.1. Informationsudvekslingsretningslinier og procedurer
 - 10.8.2. Aftaler om informationsudveksling
 - 10.8.3. Fysiske datamediers sikkerhed under transport
 - 10.8.4. Elektronisk post og dokumentudveksling
 - 10.8.5. Virksomhedens informationssystemer
- 10.9. ELEKTRONISKE FORRETNINGSYDELSER
 - 10.9.1. Elektronisk handel
 - 10.9.2. On-line transaktioner
 - 10.9.3. Offentligt tilgængelige informationer
- 10.10. LOGNING OG OVERVÅGNING
 - 10.10.1. Opfølgningslogging
 - 10.10.2. Overvågning af systemanvendelse
 - 10.10.3. Beskyttelse af log-oplysninger

Informationssikkerhedspolitik gyldig fra ??.

10.10.4. Administrator- og operatørlog

10.10.5. Fejllog

10.10.6. Tidssynkronisering

11. ADGANGSSTYRING

11.1. DE FORRETNINGSMÆSSIGE KRAV TIL ADGANGSSTYRING

11.1.1. Retningslinier for adgangsstyring

11.2. ADMINISTRATION AF BRUGERADGANG

11.2.1. Registrering af brugere

11.2.2. Udvidede adgangsrettigheder

11.2.3. Adgangskoder

11.2.4. Periodisk gennemgang af brugernes adgangsrettigheder

11.3. BRUGERNES ANSVAR

11.3.1. Brug af adgangskoder

11.3.2. Uovervåget udstyr

11.3.3. Beskyttelse af datamedier på den personlige arbejdsplads

11.4. STYRING AF NETVÆRKSADGANG

11.4.1. Retningslinier for brug af netværkstjenester

11.4.2. Autentifikation af brugere med ekstern netværksforbindelse

11.4.3. Identifikation af netværksudstyr

11.4.4. Beskyttelse af diagnose- og konfigurationsporte

11.4.5. Opdeling af netværk

11.4.6. Styring af netværksadgang

11.4.7. Rutekontrol i netværk

11.5. STYRING AF SYSTEMADGANG

11.5.1. Sikker log-on

11.5.2. Identifikation og autentifikation af brugere

11.5.3. Styring af adgangskoder

11.5.4. Brug af systemværktøjer

11.5.5. Automatiske afbrydelser

11.5.6. Begrænset netværksforbindelsestid

11.6. STYRING AF ADGANG TIL BRUGERSYSTEMER OG INFORMATIONER

11.6.1. Begrænset adgang til informationer

11.6.2. Isolering af særligt kritiske brugersystemer

11.7. MOBILT UDSTYR OG FJERNARBEJDSPLADSER

11.7.1. Mobilt udstyr og datakommunikation

11.7.2. Fjernarbejdspladser

12. ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF

INFORMATIONSBEHANDLINGSSYSTEMER

12.1. SIKKERHEDSKRAV TIL INFORMATIONSBEHANDLINGSSYSTEMER

12.1.1. Krav til sikkerhedsanalyser og specifikationer

12.2. KORREKT INFORMATIONSBEHANDLING

12.2.1. Validering af inddata

12.2.2. Kontrol af den interne databehandling.

12.2.3. Meddelelzers integritet

12.2.4. Validering af uddata

12.3. KRYPTOGRAFI

12.3.1. Retningslinier for brugen af kryptografi

12.3.2. Nøglehåndtering

12.4. STYRING AF DRIFTSMILJØET

12.4.1. Sikkerhed ved systemtekniske filer

Informationssikkerhedspolitik gyldig fra ??.

12.4.2. Sikring af testdata

12.4.3. Styring af adgang til kildekode.

12.5. SIKKERHED I UDVIKLINGS- OG HJÆLPEPROCESSER

12.5.1. Ændringsstyring

12.5.2. Teknisk gennemgang af forretningssystemer efter ændringer i styresystemerne

12.5.3. Begrænsninger i ændringer til eksternt leverede systemer

12.5.4. Lækage af informationer

12.5.5. Systemudvikling udført af en ekstern leverandør

12.6. SÅRBARHEDSSTYRING

12.6.1. Sårbarhedssikring

13. STYRING AF SIKKERHEDSBRUD

13.1. RAPPORTERING AF SIKKERHÆNDELSER OG SVAGHEDER.

13.1.1. Rapportering af sikkerhedshændelser

13.1.2. Rapportering af svagheder

13.2. HÅNDTERING AF SIKKERHEDSBRUD OG FORBEDRINGER

13.2.1. Ansvar og forretningsgange

13.2.2. At lære af sikkerhedsbrud

13.2.3. Indsamling af beviser

14. BEREDSKABSSTYRING

14.1. BEREDSKABSSTYRING OG INFORMATIONSSIKKERHED

14.1.1. Informationssikkerhed i beredskabsstyringen

14.1.2. Beredskab og risikovurdering

14.1.3. Udarbejdelse og implementering af beredskabsplaner

14.1.4. Rammerne for beredskabsplanlægningen

14.1.5. Afprøvning, vedligeholdelse og revurdering af beredskabsplaner

15. OVERENSSTEMMELSE MED LOVBESTEMTE OG KONTRAKTLIGE KRAV

15.1. OVERENSSTEMMELSE MED LOVBESTEMTE KRAV

15.1.1. Identifikation af relevante eksterne krav

15.1.2. Ophavsrettigheder

15.1.3. Sikring af virksomhedens kritiske data

15.1.4. Beskyttelse af personoplysninger

15.1.5. Beskyttelse mod misbrug af informationsbehandlingsfaciliteter

15.1.6. Lovgivning vedrørende kryptografi

15.2. OVERENSSTEMMELSE MED SIKKERHEDSPOLITIK OG -RETNINGSLINIER

15.2.1. Overensstemmelse med virksomhedens sikkerhedsretningslinier

15.2.2. Opfølgning på tekniske sikringsforanstaltninger

15.3. BESKYTTELSESFORANSTALTNINGER VED REVISION AF

INFORMATIONSBEHANDLINGSSYSTEMER

15.3.1. Sikkerhed i forbindelse med systemrevision

15.3.2. Beskyttelse af revisionsværktøjer