RAPORTTEJA 5/2005

Tero Tammisalo

# Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt

## Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi



Taitto: Ursula Cornér
ISBN 951-33-1628-9 (paperimoniste)
ISSN 1236-0740
ISBN 951-33-1629-7 (verkkokirja)
ISSN 1795-8210

Stakesin monistamo
Helsinki

STAKES

Sosiaali- ja terveysalan
tutkimus- ja kehittämiskeskus

Helsinki 2005

# Sisällys

# Esipuhe

Tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellutusten ja tietoteknisen infrastruktuurin perusedellytys. Suomen lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti.

Sosiaali- ja terveydenhuollon tietojärjestelmät käsittelevät arkaluontoista ja salassa pidettävää asiakas- ja potilastietoa. Erityisesti terveydenhuollossa on meneillään siirtyminen sähköiseen asiakasdokumentaatioon, sähköisiin arkistoihin, sähköisiin konsultaatioihin ja kansalaisten palveluun tietoverkkojen välityksellä. Tämä prosessi asettaa suuria ja myös uusia haasteita tietojen käsittelyn tietoturvallisuudelle ja tietosuojan toteutukselle.

Valtakunnallisella tasolla ei ole tähän mennessä laadittu sosiaali- ja terveydenhuollon organisaatioille yhtenäisiä toimintaperiaatteita tietoturvallisuuden hallinnassa. Tämä ohje pyrkii täyttämään tämän aukon terveydenhuollon osalta. Koska tässä ohjeessa annettavat suositukset perustuvat tietojenkäsittelyn hallinnan yleisiin standardeihin, voidaan sitä käyttää pitkälti ohjeena myös sosiaalihuollossa. Sosiaalihuollon erityiskysymykset vaativat kuitenkin perusteellista analyysiä ja tarvittaessa erityisohjeistusta.

Tämän dokumentin ohjeet on tarkoitettu ennen kaikkea sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietoturvallisten toimintaperiaatteiden laatimiseen ja tietoturvatoiminnan kehittämiseen. Ohje on osa valtakunnallista terveydenhuollon tulevaisuuden turvaamista koskevaa projektia. Ohje auttaa toimintayksiköitä määrittelemään käytettävät ja hyväksyttävät tietojenkäsittelytavat, joilla terveydenhuollon tietojen käsittelyn turvallisuus ja tietosuoja voidaan taata.

Ohjetta kirjoitettaessa on käytetty eri tasoista tietoturvallisuuteen liittyvää dokumentaatiota ja kirjallisuutta, joka selviää tarkemmin dokumentin lopussa olevasta luettelosta standardeja ja kirjallisuutta. Dokumentti pohjautuu pääsääntöisesti kansainväliseen standardiin *ISO/IEC 17799: 2000 "Code of Practice for Information Security Management"*.

Tietoturvapolitiikka on kannanotto organisaation toiminnan turvallisuuteen yleensä. Tietosuojapolitiikka on ohje ja samalla myös julkilausuma henkilötietojen käsittelytavoista. Tämä ohje suosittaa, että jokaiseen terveydenhuollon toimintayksikköön ja potilastietoja käsittelevään organisaatioon luodaan dokumentoidut tietoturva- ja tietosuojapolitiikat ja otetaan käyttöön siinä määritellyt toimintaperiaatteet ja kontrollit. Tämän ohjeen mukaisesti toteutetut ja dokumentoidut toimintaperiaatteet on sertifioitavissa ja tarkastettavissa muiden terveydenhuollon organisaatioiden toimesta.

Tämä ohje ei määritä yksityiskohtaisia teknisiä ratkaisuja jotka tulisi ottaa käyttöön. Se ei myöskään ole riskien hallinnan opas.

Tästä ohjeesta on saatu lausunnot Keski-Pohjanmaan sairaanhoitopiirin kuntayhtymästä, Helsingin kaupungin terveyskeskuksesta, Medici Data Oy:stä, Pohjois-Karjalan sairaanhoitopiirin kuntayhtymästä, Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymästä, Helsingin ja Uudenmaan sairaanhoitopiirin kuntayhtymästä, Etelä-Karjalan sairaanhoitopiirin kuntayhtymästä, Medi-IT Oy:stä, Päijät-Hämeen sairaanhoitopiirin kuntayhtymästä, Oulun kaupungin sosiaali- ja terveystoimelta, Suomen Potilasliitto ry:ltä, Turun kaupungin terveystoimelta, Kansaneläkelaitokselta, Sisäasiainministeriöstä, Suomen Kuntaliitosta, Pirkanmaan sairaanhoitopiirin kuntayhtymästä ja tietosuojavaltuutetun toimistosta.

Tätä ohjetta täydennetään Stakesin ja tietosuojavaltuutetun toimiston yhteistyönä ottamalla huomioon sosiaali- ja terveysministeriössä valmisteilla oleva lain "laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä" mahdolliset vaikutukset samoin kuin ne henkilötietolaista johdettavat tietosuojavaatimukset, joita tämä tieturvaohje ei kata.

# 1 Johdanto

## 1.1 Tietoturvallisuus ja tietosuoja

Tietoturvallisuudella tarkoitetaan asiantilaa, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä. Suomen lainsäädäntö lähtee siitä, tietoturvallisuus on hoidettava asianmukaisesti (Valtionvarainministeriö). Tietoturvallisuus on kiinteä osa jokaisen sosiaali- ja terveydenhuollon toimijan ja organisaation toimintaa ja se koskee koko henkilöstöä.

Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä. Tieturvallisuuden järjestämistä koskevia säädöksiä sisältyy useihin lakeihin.

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelemiseltä. Tietosuojatoimien tavoitteena on tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. Tietosuoja on yksilön suojaa.

Henkilötietojen käsittelyyn ja luottamuksellisen viestinnän suojaan liittyviä säännöksiä on lukuisissa eri laissa. Liitteessä 1 on luettelo keskeisistä sähköisen viestinnän tietoturvallisuuden järjestämistä ja tietosuojaa koskevista säädöksistä.

Oikeudesta käsitellä arkaluontoisia ja salassa pidettäviä tietoja on säädetty henkilötietolaissa ja viranomaisten osalta julkisuuslaissa. Henkilötietolain lisäksi sosiaali- ja terveydenhuollon tietojen käsittelyä ohjataan erityislailla ja asetuksilla kuten potilaslailla ja potilasasiakirja-asetuksella (T. Mikola, H. Sorvari ja P. Ruotsalainen, Turvallinen kommunikaatioalusta, Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004, Marja Pajukoski, Sähköinen asiointi sosiaali- ja terveydenhuollossa, lainsäädännön rajat ja mahdollisuudet, Stakes Raportteja 283-2004).

Henkilötietolaki korostaa tietojärjestelmien ja henkilötiedon käsittelyn etukäteissuunnittelua. Toiminnat tulee kartoittaa etukäteen, henkilötietojen käsittely suunnitella ja toteuttaa lainmukaisesti. Henkilötietolain periaatteista voidaan johtaa mm. seuraavat tietojenkäsittelyn vaatimukset (T. Itälä ja P. Ruotsalainen, Tietoturvallinen kommunikaatioalusta, Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004):

- etukäteissuunnittelun vaatimus
- huolellisuus ja suojaamisvelvoite
- virheettömyys-, eheys- ja luotettavuusvaatimus
- käyttötarkoitussidonnaisuus
- tarpeellisuusvaatimus
- yhteysvaatimus
- informointivelvoite
- tarkastusoikeus
- korjaamisoikeus

Sosiaali- ja terveydenhuollon organisaation on kehitettävä ja hallinnoitava samanaikaisesti sekä tietoturvallisuutta että tietosuojaa.

Sosiaali- ja terveydenhuollon organisaatioiden toiminta ja päätöksenteko perustuvat nykyään tietoon, jota on yhä enemmän ja joka on entistä yksityiskohtaisempaa. Lisäksi tämä tieto on suurimmaksi osaksi sähköisessä muodossa ja jopa luodaan suoraan sähköisiin järjestelmiin: tietoja ei välttämättä ole edes olemassa paperimuodossa, vaan kaikki käsittely ja säilytys pitkäaikaisine arkistointeineen hoidetaan sähköisesti. Sähköinen tieto on paperilla olevaa tietoa alttiimpaa erilaisille tietoturvaloukkauksille. Tietoon voi päästä käsiksi ajasta ja paikasta riippumatta pitkienkin matkojen takaa, ja kaikki tieto on saavutettavissa ja kopioitavissa murto-osassa siitä ajasta, mikä kuluisi paperidokumenttien läpikäymiseen.

Toisaalta erilaiset vika- ja häiriötilanteet, kuten tietojärjestelmien vioittuminen, voivat estää kaikkien tietojen käytön ja pahimmassa tapauksessa lamauttaa koko organisaation toiminnan.

Tietoturvallisuus ja tietojen suojaaminen onkin muodostumassa yhteiskunnassamme yhä tärkeämmäksi osaksi myös viranomaisten toimintaa. Vaikka viranomaisten toiminta on julkista, ne käsittelevät toimissaan ja päätöksenteossaan usein salaista tai arkaluonteista tietoa, joka on suojattava asianmukaisesti. Toisaalta on välttämätöntä, että tietyt viranomaisen tarvitsemat tiedot ovat aina käytettävissä ja että tiedot ovat oikeellisia. Tietojen käsittelystä ja säilytyksestä, käsittely- ja säilytystapojen turvallisuudesta ja käytettävien tietojen suojaamisesta onkin jo säädetty useassa laissa ja asetuksessa.

Voimassa oleva lainsäädäntö asettaa määräyksiä tietojen turvaamiselle. Tämä ohje tarkastelee ainoastaan voimassa olevaa lainsäädäntöä. On huomioitava, että lainsäädännön muuttuessa myös organisaation käytössä oleva tietoturvadokumentaatio ja toimintatavat on päivitettävä ajantasaiseksi riippumatta siitä, onko kulloinkin voimassa oleva ja käytettävä dokumentaatio tehty tämän ohjeen pohjalta.

Tietojen sähkömuotoisuus asettaa mittavat vaatimukset turvallisuudelle. Toisaalta vasta sähkömuotoisuus ja tietojärjestelmien hyödyntäminen tekevät mahdolliseksi monipuolisen ja varman käytön seurannan, valvonnan ja käyttäjien valtuuksien määrittelyn. Valtuudettomalta käyttäjältä estetään pääsy kaikkiin niihin tietoihin, joihin hänelle ei ole nimenomaisesti määritelty pääsyoikeuksia. Seuranta ja poikkeustilanteiden valvonta voidaan toteuttaa reaaliaikaisesti, jolloin ajantasaiset hälytykset esimerkiksi turvaloukkauksista ja virhetilanteista aikaansaavat erittäin nopean korjauksen ja paluun normaalitilanteeseen.

Tietoturvallisuutta ja sen vaarantavia tekijöitä on tutkittu runsaasti. Yleisesti voidaan todeta, että ihmisen toiminta, joko tahallinen tai tahaton, on suurin yksittäinen turvallisuuden vaarantava tekijä. Toisaalta lukuisat eri organisaatioihin tehdyt kyselytutkimukset ovat myös osoittaneet, että suurin osa organisaatioista ei ole varautunut vakaviin riskeihin ja sellaisen kohdatessa vaikutus organisaation toimintaan on lamauttava ja vakavia seurauksia aiheuttava, olipa riski sitten ihmisen toiminnasta tai esimerkiksi teknisestä viasta aiheutuva. Kuitenkin, muokkaamalla henkilöstön asenteita, kouluttamalla työntekijöitä ja parantamalla heidän osaamistaan sekä sitouttamalla kaikki organisaation työntekijät tietoturvalliseen toimintaan saadaan aikaan merkittävä parannus tietoturvallisuuden tasoon. Sitä voidaan täydentää turvaamalla tärkeät prosessit, käyttämällä turvallisia toimintatapoja sekä toteuttamalla tarvittavat tekniset toimet.

Tietoturvan vaarantuminen teknisten ja teknologisten uhkien kautta on usein estettävissä myös teknisiä menetelmiä hyödyntämällä. Esimerkiksi tietojärjestelmärikkoihin voidaan varautua teknisin toimenpitein. Käyttämällä varajärjestelmiä, varayhteyksiä ja vastaavanlaisia toimenpiteitä organisaatio voi tehokkaasti turvata keskeytymättömän toiminnan, vaikka kriittinenkin tietojärjestelmä vikaantuisi. Vastaavasti viruksia ja muita haittaohjelmia vastaan voidaan suojautua teknisin menetelmin: käyttämällä palomuureja, viruksentorjuntaohjelmia, varmistamalla sähköpostin ja liitetiedostojen turvallisuus ja estämällä vaarallisiksi havaittujen tai epäilyttävien verkkosivujen käyttö. Teknisillä toimilla ei kuitenkaan koskaan voida korvata eikä rakentaa vastaavaa tietoturvallisuutta, kuin mikä muodostuu ihmisten riittävästä osaamisesta, oikeanlaisista asenteista ja oikeasta suhtautumisesta turvallisuuteen.

## 1.2 Tietoturvallisuuden osatekijät

Puhuttaessa tietoturvan osista voidaan ensin puhua tietojen saatavuudesta (*availability*) ja käytettävyydestä (*usability*). Ensin mainitulla tarkoitetaan sitä, että tiedot ovat saatavissa silloin, kun niitä tarvitaan ja siellä, missä niitä tarvitaan. Jotta tiedot olisivat saatavilla, on tietojärjestelmien (laitteet, ohjelmistot ja tietoliikenne) toimintakuntoisuus ja saavutettavuus on turvattava. Toimintahäiriöihin voidaan varautua rakentamalla erilaisia tietoturvamekanismeja, jotka estävät tietoturvaloukkauksia. Erilaisista vika- tai ylikuormitustilanteista on kyettävä toipumaan erilaisin varajärjestelyin *(fault management, performance management*), kahdennetuin varajärjestelmin, apuohjelmin (kuten virustorjunta ja palomuurit) ja esimerkiksi varmistamalla tiedot nauhakopioille, joista ne ovat palautettavissa käyttöön. Termiä käytettävyys käytetään usein synonyyminä saatavuudelle: tiedot ovat saatavissa eli käytettävissä. Käytettävyydellä tarkoitetaan kuitenkin myös käyttökelpoisuutta: sitä, että tietojen on oltava tallennettuina sellaisessa

muodossa, että tiedot ovat yksiselitteisesti sekä luettavissa että ymmärrettävissä. Tällöin ei esimerkiksi muodostu turvariskiä sille, että tietojen tallennusformaatti olisi vanhentunut ja tiedot käyttökelvottomia eikä myöskään sille, että tietojen vaikea muoto voisi aiheuttaa virhetulkinnan.

Edellä mainitut termit eivät ota kantaa tietojen laatuun ja käyttötarkoitukseen: ovatko sinänsä eheät ja teknisesti käyttökelpoiset tiedot sopivia kussakin asiayhteydessä käytettäviksi, ovatko ne hyödyllisiä tai ylipäätään tarpeellisia. Sosiaali- ja terveydenhuollossa käytettävien tietojen tarkoituksenmukaisuus ja käyttötarkoitus on kuitenkin huomioitu lainsäädännössä.

Yleisiä turvallisuuteen vaikuttavia tekijöitä ovat lisäksi esimerkiksi organisaation kiinteistöjen ja kulunvalvonnan turvallisuus, joka onkin usein kuvattu kohtuullisen tarkasti ja riittävän kattavasti. Kulunvalvonnalla hallitaan sekä pääsy että pääsyn estyminen organisaation tiloihin, joissa on mahdollisuus tietojen käyttöön.

Toiseksi tietojen, joita käytetään, on oltava oikeellisia ja eheitä (*integrity*). Tiedot eivät saa olla vahingossa muuttuneet esimerkiksi ohjelmiston, tietokannan tai järjestelmän vioittumisen tai korruptoitumisen (turmeltumisen) vuoksi. Tiedot eivät saa myöskään olla alttiina väärentämiselle. Tietojen eheyden rikkoutuminen on yleensä erittäin vaikeasti havaittavaa ja aiheuttaa mahdollisesti suuret haittavaikutukset. Tästä syystä tietojen eheyden rikkoutuminen katsotaankin usein yhdeksi vakavimmista tietoturvaloukkauksista. Monesti tietojen olemassaoloon kytketään myös tekijä ja tekoaika, jolloin tietojen aitous ja alkuperäisyys voidaan tunnistaa. On olemassa menetelmiä, joilla asiakirjan tekijä voidaan kiistämättömästi todentaa (*authentication, non-repudiation*) ja joilla tietoihin voidaan liittää tekoajan tai muuttumishetken aikaleima. Teknisesti puhuttaessa tällaista menetelmää kuvataan usein termillä sähköinen allekirjoitus. Tietojärjestelmien sisäiseen tietojen käsittelyyn ja järjestelmien väliseen tietojen siirtoon on olemassa menetelmiä, joilla tietojärjestelmät ylläpitävät tietojen eheyttä ja tarkastavat käytettävien tietojen oikeellisuuden automaattisesti. Tekninen termi tällaiselle menetelmälle on järjestelmäallekirjoitus tai organisaatioallekirjoitus. Puhuttaessa sähköisestä allekirjoituksesta on yleensä syytä erottaa, tarkoitetaanko sähköistä allekirjoitusta sen teknisessä vai juridisessa merkityksessä.

Kolmanneksi, tietojen luottamuksellisuus (*confidentiality*) täytyy taata: tietoja käyttävillä henkilöillä on oltava valtuudet (*authorisation*) käyttää tietoja. On myös määriteltävä, millaisin valtuuksin kukin käyttäjä tietoja käsittelee. Tämä edellyttää tietojen luokittelua (*classification*), henkilöiden tunnistamista (*identification*), todennusta (*authentication*) ja valtuuksien määrittelyä (*privilege management*) sekä käsittelytapojen ja -sääntöjen määrittelyä. Esimerkkinä tietojen luokittelusta voidaan käyttää Valtiovarainministeriön tekemää valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjetta, jossa viranomaisen tieto on luokiteltu julkiseen ja salassa pidettävään tietoon, joista salassa pidettävä on puolestaan jaettu kolmeen alaluokkaan: erittäin salainen, salainen ja luottamuksellinen tieto. Henkilöiden tunnistaminen ja todennus tietojärjestelmien käytön yhteydessä voidaan toteuttaa lukuisilla eri menetelmillä, joista osa noudattaa heikkoja tai erittäin heikkoja tunnistamismenetelmiä (esimerkiksi ryhmäkohtaiset tunnukset ja salasanat) ja osa vahvaa tunnistamista (toimikorttipohjainen todentaminen). Todennettujen henkilöiden käyttövaltuudet perustuvat esimerkiksi henkilön asemaan, työtehtävään tai rooliin. Valtuudet ja oikeudet on tyypillisesti määritelty tietojärjestelmään. Erilaisia tietojen käsittelytapoja ovat esimerkiksi oikeus luoda, muuttaa tai tuhota asiakirja.

Tietojen käytön yhteydessä puhutaan usein myös jäljitettävyydestä (*logging, audit trail*), tarkastettavuudesta (*auditability*) ja tilivelvollisuudesta (*accountability*). Näillä tarkoitetaan kaikkien tietojärjestelmässä tapahtuvien toimien kirjaamista, järjestelmien ja tietojen käytön seurantaa sekä valvontaa. Kaikista käyttäjien toimista ja järjestelmän automaattisesti suorittamista toimista pitää jäädä sellainen tieto järjestelmään, että tilanteen myöhempi toteaminen (mitä on tehty, milloin on tehty, kuka on tehnyt) on mahdollista. On rakennettava sopivat kontrollit tietojärjestelmien toiminnan turvallisuuden seurantaan sekä ohjelmistojen, laitteistojen että tietoliikenteen osalta (suorituskyky, vikatilanteet). Yhtä lailla, samanlaiset kontrollit on rakennettava käyttäjien toiminnan seurantaan. Kontrollit tukevat organisaation tietoturvasta vastaavien henkilöiden toimintaa ja ylläpitävät organisaatioiden prosesseissa käytettävien tietojen turvallisuutta.

## 1.3 Tietoturvalliset toimintaperiaatteet

Tietoturvallisten toimintaperiaatteiden määrittely on välttämätöntä, jotta organisaation johto saa toteutettua turvalliset tietojenkäsittelytavat koko organisaatioon ja sen kaikkiin prosesseihin. Tietoturvallisuuden vaarantumisen yksi perimmäisistä syistä on inhimillinen toiminta – päivittäisten toimien hoito, ymmärrys, osaaminen, asenteet, johtaminen. Organisaation tietojenkäsittelyn turvallisuuden taso on ainoastaan yhtä vahva kuin sen tietojenkäsittelyprosessien heikoimman osan turvataso. Koska tämän heikoimman lenkin muodostaa yleensä ihmisen – yksilön – toiminta, tietoturvallisten toimintaperiaatteiden määrittelyn tehtävänä ei ole ainoastaan turvattavien ja suojattavien tietojen käsittelyä koskevien periaatteiden, toimintamallien ja ohjeiden luonti. Näiden on myös oltava koko organisaation henkilöstön tiedossa, ymmärtämiä ja käytössä, jotta turvallinen tietojenkäsittelyn taso saavutettaisiin ja sitä voitaisiin ylläpitää. Terveydenhuollon ammattilaisten eettisten ohjeiden on myös vastattava tietojen suojaamisen vaatimuksia.

Tietoturvan kehittäminen ei olekaan projekti vaan prosessi, joka vaatii organisaatiolta ja erityisesti sen johdolta vankkaa sitoutumista. Toimintaperiaatteiden määrittely on ensimmäinen vaihe prosessin kehittämisessä. Tämän jälkeinen tietoturvallisuuden ylläpito vaatii jatkuvaa, järjestelmällistä ja dokumentoitua turvallisuustason kehittämistä, ylläpitoa, seurantaa, valvontaa ja henkilöstön koulutusta sekä osaamisen tason seurantaa. Toiminnan on oltava organisoitua, ja sille on määrättävä nimetyt vastuuhenkilöt ja varattava riittävät resurssit. Tietoturvallisuustoiminnan tulokset ovat myös mitattavissa, ja säännöllisen palautteen antaminen tulosten perusteella ohjaa toimintaa edelleen.

## 1.4 Riskit ja uhkat

Kaikelle tietojen turvaamistoiminnalle on yhteisenä tekijänä ja perusteena tunnistettu riski. Toteutuessaan riski estää tai haittaa tietojen käyttöä siinä tarkoituksessa ja laajuudessa kuin mihin tietoja on tarkoitettu käytettävän. Riskin voi aiheuttaa myös uhka tietojen olemassaololle. Se voi koskea esimerkiksi tietojen katoamista tai tuhoutumista, muuttumista tai väärentämistä, vääränlaista tai valtuudetonta käyttöä, käytettävien tietojen väärää tulkintaa ja inhimillisiä virheitä sekä erilaisten tahallisten tietojärjestelmähyökkäysten tai -murtautumisten vaikutuksia (muun muassa tunkeutumiset, tietomurrot ja palvelunestohyökkäykset). Tästä syystä tietojen turvaamisen yhtenä keskeisenä tarkoituksena onkin erilaisten riskien tunnistaminen ja riskeihin varautuminen. Kaikkiin niihin ei kuitenkaan kannata eikä edes voi varautua: on tunnistettava riskit, jotka ovat todennäköisiä ja joista toteutuessaan aiheutuu tai voi aiheutua mahdollista haittaa (esimerkiksi sähkökatkokset, tietomurrot ja inhimilliset virheet). Jos haittavaikutusta ei ole, riskiltä ei kannata suojautua, vaikka mahdollisuus olisi kuinka todennäköinen. Toisaalta, vaikka tiettyjen riskien haittavaikutus olisi suuri mutta todennäköisyys erittäin pieni (kuten luonnonkatastrofit ja sodat), ei niihin tietoturvaa määriteltäessä yleensä varauduta.

Riskien vaikutus voi olla sama vaikka riskin aiheuttajat olisivat keskenään täysin erilaiset. Siksi riskeiltäkin joudutaan suojautumaan eri menetelmillä. Tätä havainnollistaa seuraava esimerkki.

Oletetaan, että sovelluksen käytön yhteydessä tietojärjestelmästä saatavat potilastiedot ovat vääriä tai puutteellisia. Tämä voi aiheutua esimerkiksi seuraavista syistä:

- väärien tietojen kirjaaminen inhimillisen virheen takia
- väärien tietojen saanti organisaation ulkopuolelta
- inhimillisestä virheestä johtuvat tietojärjestelmässä olevat vanhentuneet tiedot
- ohjelmiston toiminnasta johtuvat tietojärjestelmässä olevat vanhentuneet tiedot
- tietojärjestelmän käyttökatkoksen seurauksena tapahtuva vanhentuneiden tietojen palauttaminen varmistusmedialta
- järjestelmän tai ohjelmiston vikaantumisesta aiheutuneet tietojen tahattomat muutokset (tietojen pilaantuminen, korruptoituminen)

- tietoliikenneongelmista aiheutunut väärien tai puutteellisten tietojen kirjautuminen tietojärjestelmään
- käytettävän ohjelmiston tai tietojärjestelmän virheellisestä toiminnasta aiheutunut väärien tai puutteellisten tietojen kirjautuminen (esimerkiksi ohjelmistossa oleva ohjelmointivirhe tai toiminnallinen epäloogisuus)
- tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen valtuutetun henkilön toimesta (esimerkiksi lääkäri tai hoitaja)
- tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen henkilön itsensä toimesta
- valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietojärjestelmään
- valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietoliikenteen aikana
- tietoliikenneyhteyksien vikaantumisesta tai katkoksesta aiheutunut pääsyn estyminen kaikkiin tai osaan tietojärjestelmästä tarvittavista potilastiedoista
- pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin johtuen tietojärjestelmän vikaantumisesta
- pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin väärin määriteltyjen käyttövaltuuksien takia.

Potilasturvallisuus voi vaarantua kaikissa alla mainituissa tapauksissa. Potilas voi esimerkiksi saada väärää tai puutteellista hoitoa ja hänen yksityisyyden suojansa voi vaarantua. Huolimatta siitä, että vaikutus potilaaseen on sama, jokainen mainittu uhka vaatii omanlaisensa toimenpiteen, jotta vahinkoa ei pääse syntymään. Luonnollisesti myös vahingon toteutumisen mahdollisuus on kussakin erilainen, eikä kaikkiin riskeihin siten tarvitse varautua yhtä voimakkain varotoimenpitein

Yleisesti voidaan sanoa, että on sitä parempi mitä yksityiskohtaisemmin uhkat ja riskit on tunnistettu. Tällöin niiden seuraukset voidaan yksilöidä tarkasti ja varautumistoimet voidaan mitoittaa ja kohdistaa oikein. Suojaamistoimet kohdistuvat näin parhaiten suoraan riskiin eivätkä ole "yleispäteviä". Luonnollisesti tietyt toimenpiteet suojaavat monia eri tietoja monilta eri riskeiltä. Esimerkiksi fyysisen kulunvalvonnan kontrolleilla voidaan suojata kaikkia toimitiloissa olevia tietoja. Vastaavasti palomuuri suojaa kaikkia tietoja erityyppisiltä verkkohyökkäyksiltä.

Uhkien tunnistamisessa pitää myös tutustua tietoturvaloukkauksiin, joita muualla on jo tapahtunut. Tietomurtojen yrittäjät käyttävät usein samoja tai samantyyppisiä menetelmiä. Motiivi erilaisiin tietomurtoihin ja siten myös tietomurtoyrityksen todennäköisyys on suoraan verrannollinen tiedon arvoon, joko todelliseen tai kuviteltuun, ja tiedon oletettuun käytettävyyteen murtautujalle. Tiedon arvo voi olla huomattavan erilainen organisaatiolle kuin mitä se on murtautujalle.

Kaikenlaiset haittaohjelmat, muun muassa virukset, troijanhevoset ja madot sekä erilaiset ohjelmistojen takaportit ovat uhka tietoturvalle. Tyypillisesti niiden avulla voidaan joko paljastaa luottamuksellisia tietoja tai vioittaa tietojärjestelmiä, jolloin näiden sisältämät tiedot eivät ole saatavilla. Ne ovat usein uhkia vain tiettyjen käyttöjärjestelmien ja ohjelmistojen käyttäjille, mutta mahdollisuus täytyy silti ottaa huomioon tietoturvariskejä arvioitaessa. Tietojen saatavuuteen voidaan myös yrittää vaikuttaa verkosta tapahtuvilla palvelunestohyökkäyksillä (DoS, *denial of service*), jotka tyypillisesti kohdistetaan tiettyä palveluntarjoajaa kohden tarkoituksena estää verkkokäyttäjien pääsy palveluihin.

Yllämainitut muodostavat vain pienen osan organisaation tietoturvallisuuskokonaisuudessa. Nämä ovat silti ne uhkat, jotka yleensä ymmärretään parhaiten ja joista julkisestikin puhutaan. Moni mieltääkin tietoturvan ainoastaan virustorjuntana ja palomuureina. Jopa kaupallisilla markkinoilla on yrityksiä, jotka myyvät "tietoturvan ulkoistamista", vaikka todellisuudessa yritys tarjoaa ulkoistamispalveluita esimerkiksi ainoastaan virustorjunnan tai verkkosuojauksen hoitoon.

Riskien täydellinen välttäminen on käytännössä mahdotonta – organisaation toimintaan liittyy aina riskejä. Myös yksittäisten riskien ehkäiseminen ja kokonaan poistaminen saattaa aiheuttaa liikaa kustannuksia verrattuna riskeistä aiheutuviin haittoihin. Tästä syystä riskien hallinnan tavoitteena onkin usein pienentää riskiä – pyritään estämään vahinkojen syntyminen sekä vähentämään tai lieventämään niiden seurauksia tunnistamalla riskit yksityiskohtaisesti ja valitsemalla sopivat kontrollit ja suojautumiskeinot. Tiettyjä riskejä voidaan esimerkiksi sopimuksellisesti tai vakuuttamalla siirtää jopa muille, jolloin mahdollisesti aiheutuvat vahingot eivät kohdistu täysimittaisena ainoastaan omaan organisaatioon, vaan

mahdolliset korvausvastuut riskin toteutuessa voidaan jakaa useamman organisaation kesken. Toteutumisen seuranta ja monitorointi voi aiheuttaa esimerkiksi toteutuneen riskin korjaamis- ja toipumisprosessin. Riski voidaan jättää myös huomiotta – vaikutus on tiedossa, mutta toistaiseksi riskiltä päätetään olla suojautumatta.

## 1.5 Tietoturvatyön tavoitteet

Tietoturvatyön tavoitteena on parantaa organisaation kykyä turvata käytössään olevat tiedot erilaisilta niihin kohdistuvilta uhkilta. Tietoturvatoiminta pohjautuu sille asetettuihin vaatimuksiin, joissa määritellään sopivat ja sallitut tavat käsitellä ja säilyttää tietoja: tietojenkäsittely on suunniteltava ja toteutettava siten, että tietojen saatavuus, oikeellisuus, luottamuksellisuus ja käytön seurattavuus eivät vaarannu.

Tietoturvallisuuden kehittämisen yhteydessä on tunnistettavissa seuraavat osa-alueet, joiden toteutuminen on tärkeää, että kehityksessä voitaisiin onnistua.

1. Tunnistetaan ja määritellään suojattavat tiedot ja syyt, miksi tiedot pitää suojata.
2. Tunnistetaan, miltä tiedot pitää suojata (muuttuminen, katoaminen, paljastuminen ym.).
3. Tunnistetaan riskit, jotka johtavat tietoturvaloukkauksiin.
4. Estetään riskien toteutuminen.
    - politiikat, käytettävät standardit ja toimintaprosessit
    - tietoturvaorganisaatio ja hallinnointi
    - turvalliset tietojärjestelmäarkkitehtuurit, menetelmät ja teknologiat

Tietoturvallisuus vaatii ennen kaikkea oikeaa johtamista ja oikeita, kunnollisia menetelmiä. Seuraavassa pikaohjeessa on kuvattuna nimenomaan johdolta vaadittavia toimenpiteitä, jotta turvallisuuspäämäärät voitaisiin parhaiten saavuttaa.

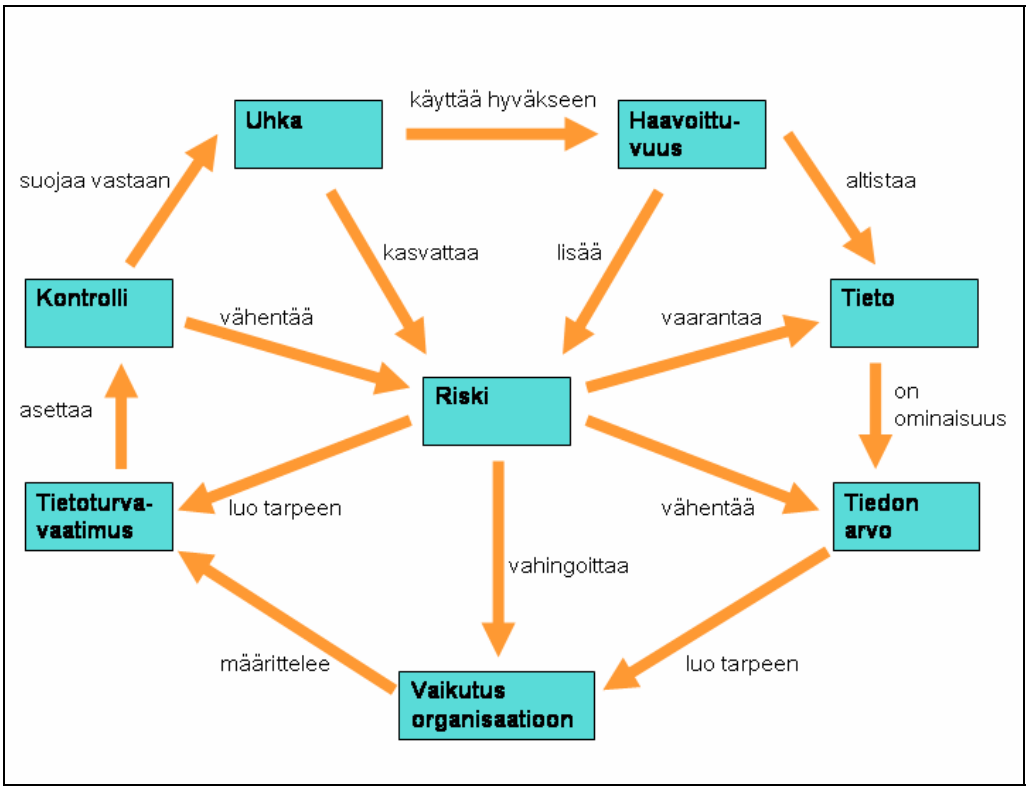
1. Sitoudu, tue ja motivoi.
2. Näytä esimerkkiä.
3. Määritä tavoitteet ja ymmärrä ne.
4. Määritä vastuuhenkilöt ja tietoturvaorganisaatio.
5. Varaa riittävästi resursseja.
6. Huolehdi, että kommunikaatio toimii organisaatiossa ja ettei tietokatkoksia ole.
7. Huolehdi, että koko organisaatio saa riittävästi tietoa ja koulutusta.
8. Valvo, mittaa ja seuraa.
9. Palkitse ja ojenna.

## 1.6 Tietoturvallisuuden toteuttaminen

Tietoturvaa toteutetaan käytännössä erilaisten säätimien ja hallintakeinojen (kontrollien) avulla. Oikein toteutettuna kontrollit voivat olla joko ennalta ehkäiseviä (*proactive*) tai ongelmatilanteissa käynnistyviä tai käynnistettäviä (*reactive*). Yhteisenä näille on se, että ongelmatilanne pyritään korjaamaan ja tietoturvallisuutta vaarantaviin riskeihin varautumaan ennalta suunnitellun mukaisesti. Sopivasti näkyvillä ja näkymättömissä olevat valvontakeinot toimivat myös pelotteena, jolloin on tarkoitus sekä ehkäistä tahallisia väärinkäytösyrityksiä että ohjata oikeutettuja käyttäjiä huolelliseen ja tarkkaan toimintaan.

Tietoturvallisuus toteutetaan suunnitelmallisella työllä: ensin määritellään suojattavat kohteet, siis tiedot ja tietojärjestelmät, niiden arvo ja suojauksen tarve. Tämän jälkeen arvioidaan uhkat ja riskit, jotka uhkaavat suojattavien tietojen turvallisuutta. Kun sekä suojattavat tiedot on määritelty että niitä uhkaavat riskit kartoitettu, voidaan valita sopivat kontrollit – ne toimenpiteet ja säätimet, joilla riskeihin varaudu-

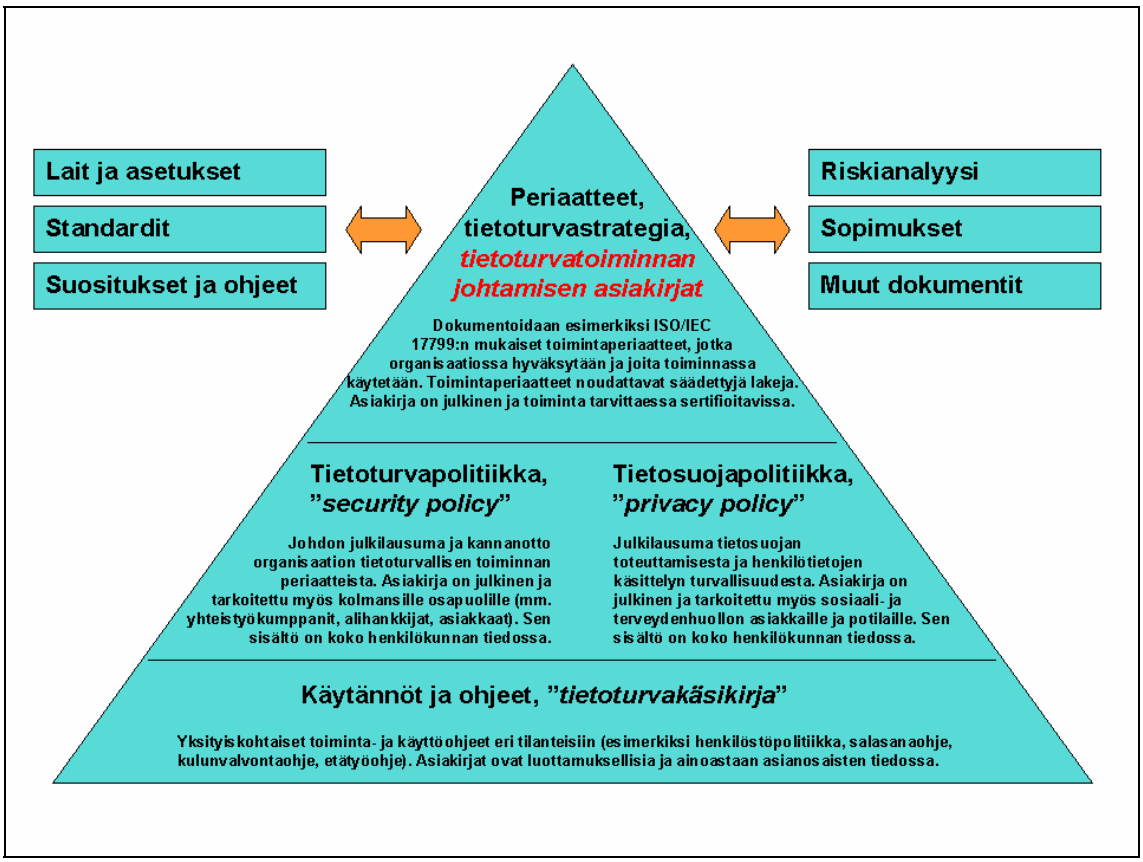
taan, miten niiden toteutumisesta toivutaan ja ongelmat korjataan sekä miten toimintaa mitataan. Kuva 1 hahmottaa riskien, haavoittuvuuksien, uhkien ja hallintakeinojen keskinäisiä suhteita.




Kuva 1 – Riskit, uhkat, haavoittuvuudet ja kontrollit (lähde: Ross Fraser, ESQ & EHTEL Joint Workshop, Lahti, Finland, 18-19 June 2004)

## 1.7 Tietoturvan ja tietosuojan dokumentaatio

Lainsäädännön vaatimusten, sosiaali- ja terveysministeriön ohjeiden, organisaation tietoturvavaatimusten riskianalyysin, uhkien ja haavoittuvuuksien analyysin, valittujen tietoturva- kontrollien ja tietoturvaperiaatteiden perusteella luodaan ohjeet ja periaatteet organisaation tietoturvalliselle toiminnalle. Kaikkien näiden edellä mainittujen pohjalta kuvataan organisaation Tietoturvalliset toimintaperiaatteet, jonka mukaisesti luodaan organisaation tietoturvapolitiikka *(security policy*), ja tietosuojaperiaatteet, jonka mukaisesti luodaan tietosuojapolitiikka (*privacy policy*). Lisäksi laaditaan yksityiskohtaiset toiminta- ja käyttöohjeet. Kuvassa 2 on esitetty kaaviona tarvittava tietoturvallisuuden dokumentaatiokokonaisuus.



Kuva 2 – Tietoturvadokumentaation hierarkia

## 1.8 Tietoturvallisuuden standardeista

Sosiaali- ja terveydenhuollossa noudatettavia lakeja, joissa säädetään tietoturvallisuustyössä huomioitavia määräyksiä, on lueteltu luvussa *laillisuus ja sääntöjen mukaisuus*. Lakitekstit löytyvät kokonaisuudessaan verkkosivuilta *http://www.finlex.fi*.

Tietoturvallisuuteen liittyvien standardien noudattaminen tarpeellisilta ja soveltuvilta osiltaan on organisaatiolle hyödyllistä; niiden mukaan toimittaessa otetaan huomioon myös turvallisuuteen liittyvät vaatimukset. Turvallisuustietous ylipäätään ja sen jokapäiväinen huomioiminen muodostuvat itsestäänselvyydeksi ja sitä kautta yhdeksi organisaation arvoista ja kilpailueduista. Organisaatio pystyy varautumaan tietoturvaan liittyviin riskeihin ja suojautumaan niiltä. Sekä yksityishenkilöt, palveluiden käyttäjät ja organisaation työntekijät että muut organisaatiot ja viranomaiset saadaan vakuutettua toiminnan turvallisuudesta, mikä omalta osaltaan kasvattaa luottamusta organisaatioon. Standardien mukainen turvallisuustoiminta on yhteismitallinen sekä oman että muiden toimialojen turvallisuustoiminnan kanssa. Tietojen suojaaminen on järjestelmällistä ja kaikessa turvaamistoimissa noudatetaan samoja, dokumentoituja menetelmiä. Tämä luo pohjan luottamuksen ja toimintaedellytysten syntymiseen myös yli kansallisten rajojen.

Erilaisia ja eritasoisia sekä kansainvälisiä että kansallisia standardeja on luotu runsaasti. Ohessa on listattuna muutamia oleellisimpia ja tärkeimpiä *ISO/IEC:n* standardeja. Muiden standardointielinten laatimia ja kansallisia standardeja ei ole listattu. Näistä tärkein on *British Standardisation Institute'n standardi BS7799*, jota on käytetty pohjana useille *ISO/IEC*:n standardeille. Sitä onkin joissakin yhteyksissä kutsuttu "tietoturvallisuusstandardoinnin isäksi" tai "isoisäksi", mikä termi sisältänee kuitenkin hieman liioittelua: se ei suinkaan ole ensimmäinen eikä liioin kaikissa yhteyksissä paras mahdollinen tai sopivin käytettävissä oleva standardi. BS7799 sisältää teknisten ja toiminnallisten kontrollien lisäksi

täsmällisiä määrittelyitä myös tietoturvallisuuden hallinnointiin ja johtamiseen. Sitä käytetään, kun organisaation tietoturvallisuustoiminta halutaan sertifioida.

Kansainvälinen yhteenliittymä *Information Security Forum* (*ISF*) muodostuu lähes 300 yrityksestä ja organisaatiosta, jotka ovat yhteistyössä toteuttaneet ja rahoittaneet hankkeen turvallisten tietojenkäsittelytapojen ja parhaiden käytäntöjen (*best practices*) määrittämiseksi. Joukossa on tämän ohjeen kirjoitushetkellä yksitoista suomalaista yritystä. Turvallisuushankkeen tärkeimpänä tuotoksena on laadittu standardi "*the Standard of Good Practice for Information Security*", joka sisältää käytännöllisen lähestymistavan tietoturvallisuuden toteuttamiseen ja hyviin käytäntöihin. ISF:n verkkosivut löytyvät osoitteesta *http://www.securityforum.org* ja standardi osoitteesta *http://www.isfsecuritystandard.com*.

Keskeiset tietotuvallisuusstandardit ovat:

- *ISO/IEC 17799:2000 "Code of Practice for Information Security Management"* sisältää hyväksi havaitut ja valitut toimintaperiaatteet *("best practice guidelines and controls")* organisaation tietoturvallisen toiminnan ja hallinnoinnin toteutukselle. Standardissa on otettu huomioon esimerkiksi standardit BS7799 ja ISO13335.
- *ISO/IEC 13335 Technical Report: Guidelines of the Management of IT Security*, GMITS, sisältää viisi osaa, joiden perusteella on laadittu *ISO/IEC 13335 "Management of Information and Communications Technology Security"*, MICTS, jossa erityisesti riskien hallinta on määritelty. Dokumentin sisältöön onkin syytä tutustua riskienhallintaprosessia määritettäessä ja toteutettaessa. GMITS:n osat ovat
    - Part 1: Concepts and Models
    - Part 2: Management and Planning
    - Part 3: Techniques for IT Security Management
    - Part 4: Selection of Safeguards
    - Part 5: External Connections
- *ISO/IEC 15408:1999 "Evaluation Criteria for IT Security"* (Common Criteria) on standardi tietoturvallisten järjestelmien ja tuotteiden määrittelyyn ja arviointiin. Sen avulla voidaan luoda turvaprofiilit käytettäville järjestelmille. On aiheellista myös arvioida, voidaanko standardia käyttää määritettäessä vaatimuksia alihankkijoille ja ohjelmisto- ja laitetoimittajille.
- *ISO/IEC TR 15446 "Guide for the production of Protection Profiles and Security Targets"* on hyvä apu edellä mainitun dokumentin mukaisten turvaprofiilien laadintaan. Siinä on myös havainnollinen, joskin työläs malli riskien hallintaan. Myös kryptografian osuutta tietoturvapolitiikassa on kommentoitu.
- Lukuisa määrä standardeja ja suosituksia, jotka liittyvät kiistämättömyyteen, eheyteen, käyttäjien hallintaan, todentamiseen, käyttöoikeuksiin, vikatilanteisiin ja niistä toipumiseen, ongelmanhallintaan, jäljitettävyyteen ja auditointiin, PKI:iin, aikaleimoihin, TTP:n toimintaan, varmenteisiin, avainten hallintaan, salaukseen, sähköisiin allekirjoituksiin, kryptografiaan, sen funktioihin ja algoritmeihin. Monet näistä löytyvät tämän teoksen lopussa olevasta luettelosta *standardeja ja kirjallisuutta.*

## 1.9 Standardien soveltaminen terveydenhuollossa

*ISO/IEC 17799 "Code of Practice for Information Security Management"* on laajasti käytetty terveydenhuollon informaatiojärjestelmien tietosuojan ja -turvan hallinnoinnissa kansallisena ja alueellisena ohjeena. Standardia käytetään terveydenhuollossa muun muassa Australiassa, Kanadassa, Hollannissa, Etelä-Afrikassa ja Englannissa.

Standardissa *ISO/IEC 17799* määritellään tietoturvan säätö- ja toimenpidekohteet ja niihin kohdistuvat säätötoimet (kontrollit). *ISO/IEC 17799-1:2004* sisältää kaikkiaan 11 säätö/toimenpidekohdetta ja 136 kontrollia. Säätökohteita ovat:

- tietoturvapolitiikka,
- tietoturvallisuuden hallinnointi ja organisaatio,
- omaisuuden ja tieto-omaisuuden hallinta,
- henkilöstöturvallisuus,
- fyysisen ympäristön turvallisuus,
- tietojärjestelmien käytön ja tiedonvälityksen turvallisuuden hallinta,
- pääsynhallinta,
- tietojärjestelmien kehitys ja ylläpito,
- toiminnan jatkuvuus,
- laillisuus ja sääntöjen noudattaminen sekä
- poikkeustilanteiden ja ongelmatapahtumien hallinta.

Tässä raportissa tietoturvan ja tietosuojan säätökohteen ja kontrollit on ryhmitelty *ISO/IEC 17799* -standardin mukaisesti.

Valmistumisvaiheessa oleva standardi *ISO 27799 "Health Informatics - Security Management in Health Using ISO/IEC 17799"* ohjeistaa terveydenhuollon toimintayksiköitä ja muita terveydenhuollon luottamuksellista tietoa käsitteleviä toimijoita *ISO/IEC 17799*:n käyttöönotossa terveydenhuollossa. Siinä esitetään spesifiset vaatimukset terveydenhuollon tietojen käsittelyn luottamuksellisuudelle, tietojen muuttumattomuudelle ja saatavuudelle. Standardi määrittää tietoturvan ja tietosuojan hallinnan vaatimukset mutta ei määrittele sitä, kuinka ne saavutetaan tai miten vaatimukset on teknisesti toteutettava.

Standardissa säätökohteet noudattavat yllä mainittua jakoa yhteentoista osa-alueeseen, joissa on 39 pääluokkaa. Standardi ei kuitenkaan vielä tämän dokumentin kirjoitushetkellä ole täysin valmis ja tultaneen hyväksymään vuonna 2006. Standardiluonnokseen sisältyy joukko *pakolliseksi* ehdotettuja tietoturvallisuusvaatimuksia, jotka on esitetty tämän ohjeen liitteessä 5. Näiden "pakollisten" vaatimusten toteuttamiseen on perusteltua ryhtyä välittömästi, vaikka itse standardi ei ole vielä hyväksytty.

## 1.10 Tietoturvan ja tietosuojan tekninen toteutus

Teknisiä ratkaisuja ja palveluja, joilla voidaan toteuttaa organisaatiolle asetetut tietosuoja- ja tietoturvavaatimukset, on tarjolla runsaasti. Sähköisen tietojenkäsittelyn alueella uusia tekniikoita ja tietoteknisiä tietoturvajärjestelmiä kehitetään eri yritysten toimesta intensiivisesti. Sen jälkeen kun organisaatio on tunnistanut uhkat ja analysoinut riskit sekä päättänyt niistä kontrolleista, jotka se ottaa käyttöönsä, tulee organisaation valita markkinoilla tarjolla olevista tekniikoista ja palveluista sille teknisesti ja taloudellisesti sopivat ratkaisut.

Valittujen teknisten ratkaisujen tulee toteuttaa samalla kertaa sekä valittu tietoturvan taso että vaadittava tietoturva. Esimerkiksi

- luottamuksellisuus voidaan saavuttaa tietojen salauksella ja tietojärjestelmien käyttäjien pääsynhallinnalla, käyttöoikeuksien ja suostumusten hallinnalla,
- eheys saavutetaan mm. tarkistussummilla, tarkistuskoodeilla ja digitaalisella allekirjoituksella ja
- käyttäjän todentaminen ja kiistämättömyys voidaan varmistaa mm. käyttämällä PKI:ta soveltavaa järjestelmää (liite 2) ja digitaalista allekirjoitusta.

Tyypillisin käytössä oleva tietojärjestelmien käyttäjien hallinnan, tunnistamisen ja todentamisen menetelmä on käyttäjätunnus-salasanamenetelmä, jossa käyttäjä tunnistetaan käyttäjätunnuksella ja todennetaan oikeaksi ja valtuutetuksi käyttäjäksi salasanalla. Tämä edustaa heikkoa tietoturvaa tyypilli-

simmillään. Käyttäjällä on yksivaiheinen pääsy tietojärjestelmään – riittää, että hänellä on tiedossaan käyttäjätunnus ja salasana. Vastaavanlainen esimerkki yksivaiheisesta todentamisesta olisi, että pankkiautomaatilla asiointiin riittäisi pelkkä toimikortin käyttö ilman PIN-koodia.

Vahvassa tunnistamisessa tietojärjestelmät tunnistavat ja todentavat käyttäjän kaksivaiheisesti. Kaksivaiheisuudessa yhdistetään kaksi kolmesta ominaisuudesta, jotka voidaan liittää käyttäjään: jotakin, mitä käyttäjä on (käyttäjän henkilökohtainen ts. biometrinen ominaisuus, kuten kasvokuva, sormenjälki tai DNA), jotakin, mitä käyttäjällä on hallussaan (toimikortti, salasanalista) ja jotakin, mitä käyttäjä tietää (salasana, PIN-koodi). Ensin käyttäjä tunnistetaan jollakin menetelmällä, jonka jälkeen todennus tapahtuu jollakin toisella menetelmällä. Hyvä menetelmä on esimerkiksi sellainen, jossa toimikorttia hyödynnetään käyttäjän tunnistamisessa (jotakin, mikä käyttäjällä on hallussaan) ja vastaavasti PIN-koodia (jotakin, mitä käyttäjä tietää) tai sormenjälkeä (jotakin, mitä käyttäjä on) käyttäjän todentamisessa. Esimerkkinä voidaan käyttää jo edellä mainittua pankkiautomaattiasiointia: saadakseen oikeuden pankkiasiointiin henkilö tarvitsee sekä kortin että PIN-koodin: pankkikortin tunnistamiseen ja kortin käyttöön oikeuttavan PIN-koodin todentamiseen. Vastaava esimerkki vahvasta käyttäjän tunnistamisesta on pankkien verkkoasiointipalveluihin käyttämät menetelmät. Voidakseen asioida verkkopankissa henkilö tarvitsee sekä käyttäjätunnus-salasanayhdistelmän että muuttuvien salasanojen listan. Tässäkin tapauksessa todentaminen on kaksivaiheinen: ensin käyttäjä tietää salaiset tunnuksensa ja salasanansa, jonka jälkeen hänellä on oltava hallussaan muuttuvien salasanojen lista. Jos asiakkaalla ei ole salasanalistaa hallussaan, hänen asiointinsa verkkopankissa estetään.

Jos todentamiseen käytetään esimerkiksi sormenjälkeä, täytyy henkilötietojen ja erityisesti käyttäjän biometristen ominaisuuksien käsittelystä säädettyjä lakeja noudattaa. Vastaavasti, kun kasvokuvan käyttö esimerkiksi passissa on hyväksyttyä, sähköisessä asioinnissa voitaisiin ajatella sormenjäljen käyttöä, koska tietojärjestelmän tekemä luotettava todentaminen kasvokuvasta on erittäin vaikeaa. Joka tapauksessa tämä edellyttäisi, että sormenjälki (ts. kuva tai näyte sormenjäljestä) talletetaan ja säilytetään ainoastaan esimerkiksi henkilön hallussa olevalla toimikortilla vastaavasti, kun kasvokuvakin on ainoastaan passissa. Biometrisistä tunnisteista ei voida ajatella tehtävän rekisteriä, jonka perusteella suoritetaan käyttäjän tunnistaminen. Biometrian käyttö on suotavaa ainoastaan tunnistamis-todentamisprosessin toisessa vaiheessa, kun jo tunnistettu käyttäjä todennetaan biometrista tunnistetta käyttämällä oikeaksi. Joka tapauksessa kaikkien biometristen tunnistusmenetelmien käytöstä on syytä keskustella erikseen tietosuojavaltuutetun kanssa ja hyväksyttää käytettävä menetelmä.

Joissakin keskusteluissa on esiintynyt kysymyksiä, edustavatko esimerkiksi verkkopankkitunnukset aidosti vahvaa tunnistamista – tietäähän myös pankki asiakkaansa käyttäjätunnuksen ja salasanalistat. Pankki ja asiakas ovatkin keskenään sopimussuhteessa ja verkkoasioinnissa osapuolet keskenään, ja tällöin toki vahvan tunnistamisen vaatimukset täyttyvät. Kolmannen osapuolen, esimerkiksi viranomaisen, pitää kuitenkin tarkkaan harkita, voiko se luottaa kyseiseen sopimussuhteeseen ja voidaanko pankkitunnuksia käyttää myös viranomaisasioinnissa, näin tehtäessähän pankilla on tieto asiointitapahtumasta. Tämän lisäksi henkilön tunnukset ovat tosiasiassa myös pankin hallussa, ja halutessaan pankki voisi teoriassa tekeytyä asiakkaakseen. Tämän tietoturvariskin toteutumisen todennäköisyys lienee tosiasiallisesti lähellä nollaa, mutta tärkeää on ainakin ymmärtää riskin olemassaolo. Ymmärtämällä riski voidaan tehdä valintoja, minkä palveluntuottajien (pankit ja vakuutusyhtiöt, kauppojen keskusliikkeet, lentoyhtiöt, hotelliketjut ym.) erilaisiin todentamismenetelmiin luotetaan.

## 1.11 Lopuksi

Tietoturvasta puhuttaessa kuulee usein esitettävän erilaisia iskulauseita, joiden tarkoitus on pitää tietoturva-asiat "tuoreena mielessä". Siten ihmiset saadaan myös ymmärtämään, motivoitumaan ja noudattamaan ohjeita. Tässä yhteydessä onkin hyvä mainita muutama slogan, jota voidaan käyttää myös tietoturvatoiminnan ja viholliselta – tietoturvariskiltä – suojautumisen yhteydessä. Iskulauseet eivät kaivanne sen enempää selityksiä, ja asiayhteydestä huomaa, että ne on suunniteltu tietoturvasta vastuullisten (johto ja nimetyt henkilöt) motivoimiseksi.

*"Ihmiset tekevät virheitä."*
*"Paras kannustin on johtajan esimerkki."*
*"Hyvin suunniteltu on puoliksi tehty."*
*"Säännöt ovat hyödyttömiä ilman valvontaa ja kuria."*
*"Jos et tiedä, mitä vastaan puolustaudut, et voi onnistua."*
*"Jos et tiedä, mitä olet puolustamassa, et voi onnistua."*

Joskus organisaation tietoturvatoiminnan kehittämisen yhteydessä on myös hyvä ottaa käyttöön jokin iskulause, joka jää helposti ihmisten mieleen ja joka on omiaan parantamaan toimintaan ja sen turvallisuuteen liittyviä asenteita. Kautta historian ehkä eniten tietoturvallisuuteen vaikuttanut slogan onkin peräisin George Orwellin vuonna 1949 kirjoittamasta teoksesta 1984: "isoveli valvoo". Tämä oli ja on yhä ajankohtainen siitäkin huolimatta, että tietokoneita ei Orwellin aikana käytännössä edes vielä ollut olemassa.

# 2 Tämän dokumentin käyttö ja rajaukset

Tämä dokumentti on tehty ohjeeksi, jolla organisaation tietoturvallisuuden taso voidaan asettaa standardin *ISO/IEC17799: 2000 "Code of Practice for Information Security Management"* mukaiseksi. Ohje ei ole kattava vaan luo näkymän rakenteeseen, jolla periaatteet ja toiminta määritellään ja kuvataan, ja jonka mukaan koko organisaatiossa on toimittava. Ohje on kirjoitettu silmälläpitäen henkilö- ja potilastietojen käsittelyä terveydenhuollossa, ja tähän vaikuttavilta osilta dokumentti onkin huomattavasti yksityiskohtaisempi.

Ohje toimii käytännön oppaana terveydenhuollon organisaatiolle, kun kehitetään toiminnan tietoturvallisuutta standardin mukaiseksi ja lakien vaatimukset täyttäväksi. Saavutettu tietoturvan taso on sertifioitavissa ja syntynyttä dokumentaatiota voidaan käyttää luottamuksen luomisessa organisaatioiden välillä. Sertifiointi ei luonnollisesti edellytä tämän ohjeen mukaista toimintaa, mutta ohje toimii hyvänä apuvälineenä etenkin silloin, kun vastaavanlaisia tietoturvaperiaatteita ja toimintatapoja ei vielä ole määritetty.

## 2.1 Dokumentin sisältö ja rakenne

Dokumentti käsittelee edellä mainitun standardin mukaisesti tietoturvallisuutta hallinnollisiin osa-alueisiin jaoteltuna. Osa-alueet on kuvattu yhdessätoista luvussa, joista kussakin keskitytään tiettyyn hallinnalliseen kokonaisuuteen. Lueteltuna on, millaisia keinoja ja menettelytapoja – kontrolleja – on olemassa kyseiseen osa-alueeseen liittyvien riskien hallintaan, niihin varautumiseen ja niiltä suojautumiseen. Kuhunkin kontrolliin liittyen kuvataan, millaiset periaatteet ja millaiset toimenpiteet ovat hyväksyttäviä ja suositeltavia.

Osa-alueet ovat

- tietoturvapolitiikka,
- tietoturvallisuuden hallinnointi ja organisaatio,
- omaisuuden hallinta,
- henkilöstöturvallisuus,
- fyysisen ympäristön turvallisuus,
- tietojärjestelmien käytön ja tiedonvälityksen turvallisuus,
- pääsynhallinta,
- tietojärjestelmien kehitys ja ylläpito,
- toiminnan jatkuvuus,
- laillisuus ja sääntöjen mukaisuus sekä
- poikkeustilanteet.

Lisäksi mukaan on liitetty tarkastuslista oleellisista asioista silloin, kun se on mahdollista tai tarpeellista. Listalla on mainittu kontrolliin liittyvä toimenpide, varattu paikka valmiusmerkinnälle, vastuuhenkilölle ja aikataululle sekä tarvittaessa lisätiedoille. Liitteissä on myös malli sekä tietoturva- että tietosuojapolitiikalle. Mallit ovat käytettävissä sellaisenaan, kunhan lisää oman organisaation tiedot niille varattuihin kohtiin ja tekee muut tarvittavat muutokset esimerkiksi organisaation, vastuiden ja roolien osalta.

Dokumentin alussa on yleinen esittely tietoturvasta sekä luettelo niistä termeistä ja termien merkityksestä, jotka ovat yleisimmässä käytössä, ja jotka helpoimmin mielletään tietoturvallisuuteen liittyviksi.

Suomessa näkee usein tietoturvallisuuden osa-alueita jaoteltuna hieman eri tavalla kuin yllä on mainittu. Vaikka jaottelut sinänsä olisivat toimivia ja niiden perusteella voitaisiin laatia esimerkiksi riskien kartoitus, ne eivät kuitenkaan sellaisenaan vastaa standardia ja saattavat usein sisältää joitakin oleellisiakin puutteita. Tietoturvallisuustyön hallinnointi ja toimeenpano suositellaan tehtäväksi yllä mainittujen osa-alueiden mukaisesti, eikä mainittuihin muunlaisiin, tässä esitellystä jaottelusta poikkeaviin malleihin oteta tässä dokumentissa tämän enempää kantaa.

On huomattava, että osa eri hallinnollisiin kokonaisuuksiin liittyvistä kontrolleista ovat päällekkäisiä. Päällekkäisyydet on kuitenkin pyritty minimoimaan, mutta niiltä ei pysty kokonaan välttymään. Esimerkiksi hallinnollisissa toimenpiteissä ja henkilöstöturvallisuuden toimenpiteissä on löydettävissä joitakin yhtäläisyyksiä.

## 2.2 Rajaukset

Tässä dokumentissa ei käsitellä tietoturvariskien arviointia. Riskejä ei ole lueteltu eikä niiden todennäköisyyksiä tai vaikutuksia ole arvioitu. Ohjeen mukaisesti määriteltyjä kontrolleja ja periaatteita noudattamalla voidaan suojautua tyypillisimmiltä tietoturvariskeiltä. Riskien arviointi ja analysointi jää kuitenkin tämän ohjeen käyttäjälle. Apuna voi käyttää esimerkiksi Valtiovarainministeriön julkaisua *Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa*.

Tässä dokumentissa ei luokitella organisaation käytössä olevia tietoja eikä anneta näihin luokitteluohjeita. Pääsääntöisesti ohje on sovellettavissa henkilötietojen käsittelyn tietoturvallisten toimintaperiaatteiden luomiseen. Dokumentin rakenne on kuitenkin edellä mainitun standardin mukainen, joten ohjetta voidaan soveltaa myös organisaation muiden tietojen käsittelyssä, olivatpa ne julkisia tai salaisia. Tällaisia tietoja voivat olla esimerkiksi henkilöstöön liittyvät tiedot, tiedot erilaisista sopimuksista ja näiden yksityiskohtainen sisältö sekä yhteistyökumppaneiden luottamuksellisiksi luokittelemat tiedot. Tietojen luokittelu (tärkeyden ja luottamuksellisuuden tasot) kunkin tiedon osalta on laadittava joko ennen riskianalyysin tekoa tai viimeistään sen yhteydessä. ISO:n dokumentaatiosta ja olemassa olevista standardeista on löydettävissä paljon käyttökelpoisia määrittelyitä, kuten dokumentista *ISO/IEC 15408 "Evaluation Criteria for IT Security"*. Myös koko standardi *ISO/IEC 13335 "Guidelines for the Management of IT Security"* on tutustumisen arvoinen:

- ISO/IEC 13335-1:1996 Part 1: Concepts and Models for IT Security
- ISO/IEC 13335-2:1997 Part 2: Managing and Planning IT Security
- ISO/IEC 13335-3:1998 Part 3: Techniques for the Management of IT Security
- ISO/IEC 13335-4:2000 Part 4: Selection of Safeguards
- ISO/IEC 13335-5:2001 Part 5: Management Guidance on Network Security.

Voimassa olevien lakien perusteella ohjeessa oletetaan potilaaseen liittyvien henkilötietojen osalta, että tietojen tärkeys on kriittinen ja luottamuksellisuus salainen. Kaikki yksityiskohdat ja perustelut on lueteltu Valtiovarainministeriön julkaisussa *Tietoaineistojen käsittelyn tietoturvallisuusohje*. Eri potilastietojen osalta esimerkiksi tiedon tärkeys voidaan tapauskohtaisesti määritellä esimerkiksi perustuen riskin toteutuessa mahdollisten haittojen suuruuteen.

# 3 Tietoturvan ja tietosuojan kohteet ja kontrollit

## 3.1 Yleistä

Tämä ohjeen lähtökohta on, että sosiaali- ja terveydenhuollon toimintayksiköt ja henkilötietoja tietoja käsittelevät toimijat laativat tietoturva- ja tietosuojapolitiikat.

Tietoturvapolitiikka on johdon kannanotto ja julkilausuma organisaation tietoturvallisuuden toteuttamiseen. Se kertoo esimerkiksi organisaation tietojenkäsittelyn turvaamisen tavoitteet, periaatteet ja miten turvaamistoiminta organisaatiossa käytännössä hoidetaan. Siinä luonnollisesti otetaan huomioon myös liiketoiminnan ja voimassa olevien lakien vaatimukset. Politiikka on koko organisaation tiedossa ja johto osoittaa selkeää sitoutumista, tukea ja motivointia kuvattuun tietoturvatoiminnan kehittämiseen ja ylläpitoon sekä sovittujen periaatteiden ja käytäntöjen noudattamiseen koko organisaatiossa.

Tietoturvapolitiikka osoittaa organisaation kanssa asioiville osapuolille, että organisaatio panostaa tietoturvallisuuden kehittämiseen ja ylläpitoon ja antaa osaltaan luotettavan kuvan organisaation toiminnasta.

Terveydenhuollossa henkilötietojen, kuten potilastietojen, käsittely on tarkoituksenmukaista kuvata joko tietoturvapolitiikassa tai nimenomaisesti henkilötietojen käsittelyä varten laadittavassa erillisessä kuvauksessa, tietosuojapolitiikassa. Asiakirja voidaan jakaa potilaalle tai asiakkaalle tarpeen mukaan, esimerkiksi sitä pyydettäessä. Jokaiselle, jonka henkilötietoja organisaatiossa käsitellään ja säilytetään, voidaan tällöin osoittaa, että näitä tietoja käsitellään turvallisesti, luottamuksellisesti ja hyvien tietojenkäsittelytapojen mukaisesti. Tietosuojapolitiikka on eräänlainen turvallisuusvakuutus ja sitä voisi kutsua myös nimellä "tietoturvapolitiikka henkilötietojen käsittelyssä" tai "tietosuojaseloste". Voisi myös todeta, että tietosuojapolitiikka laajentaa olemassa olevia eettisiä ohjeita huolellisuudesta ja tarkkaavaisuudesta myös nimenomaisesti tietosuojan huomioimiseen. Tietosuojapolitiikassa voidaan kuvata esimerkiksi menettelyt *"clean desk policy"* ja *"clear screen policy"*.

Sekä tietoturva- että tietosuojapolitiikka ovat koko organisaation tiedossa. Henkilöstöä on koulutettu riittävästi, asiakirjat ovat käytössä ja niiden sisältö ja periaatteet ymmärretään. On mahdollista, että organisaatiossa yhdistetään nämä kaksi asiakirjaa yhdeksi. Tässä luvussa tietoturva- ja tietosuojapolitiikkaa käsitellään kuitenkin kahtena erillisenä dokumenttina, koska tässä yhteydessä on tarkoituksenmukaista erottaa organisaation yleinen tietoturvallisuus ja henkilötietojen käsittely. On silti syytä mainita, että seuraavissa luvuissa puhuttaessa esimerkiksi tietoturvapolitiikkaan tehtävistä muutoksista tarkoitetaan molempia dokumentteja relevanteilta osiltaan.

Jotta organisaatiossa toimittaisiin tietoturva- ja tietosuojapolitiikkojen mukaisesti, on noudatettavat käytännöt, ohjeet ja periaatteet hyvä koota yhteen, *"tietoturvakäsikirjaksi"*. Se dokumentoi ja ohjeistaa käytännön toiminnan yksityiskohtaisesti. Ollessaan kaikkien organisaation henkilöiden saatavilla ja tiedossa se on siten erittäin hyödyllinen dokumentti sertifioitaessa organisaation tietoturvallisuus.

### A1.1 Tietoturvapolitiikan luominen

#### kontrolli

Tietoturvapolitiikan täytyy olla organisaation liiketoiminta ja voimassa olevat lait huomioiden kirjoitettu ja johdon hyväksymä. Asiakirjan täytyy sisältää oleelliset asiakokonaisuudet ja kuvata ne riittävästi mutta ei liian yksityiskohtaisesti.

### käytännön ohjeita

Ainakin seuraavien vaiheiden, tehtävien tai ohjeistuksen on oltava tiedossa ja ne täytyy yksityiskohtaisesti määritellä ennen tietoturvapolitiikan laatimista tai sen laatimisen aikana. Tietoturvapolitiikan tulee kuvata nämä siltä osin ja siinä laajuudessa kuin on tarpeen. On kuvattava

a) kannanotto johdon sitoutumisesta,
b) vastuu tietoturvasta,
c) vastuu ja menettely tietoturvapolitiikan ylläpidossa,
d) turvattavien tietojen määrittely,
e) turvattavien tietojen luokittelu,
f) liiketoiminnan ja sen jatkuvuuden vaatimukset tietoturvatoiminnalle,
g) riskit,
h) lakien vaatimukset,
i) noudatettavat standardit,
j) mahdollisten voimassa olevien sopimusten vaikutus,
k) tietoturvatoiminnan päämäärä ja tavoitteet,
l) hyväksytyt periaatteet turvalliselle tietojenkäsittelylle ja tietoturvalliselle toiminnalle tarpeellisilta osiltaan,
m) organisaation tietoisuus, koulutus ja miten osaamista ylläpidetään,
n) tietoturvallisuusorganisaatio ja sen toiminta, mukaan lukien seuranta ja raportointi,
o) toiminta tietoturvaloukkauksissa ja ohjeiden vastaisen toiminnan seuraukset ja
p) siltä osin kuin on tarpeellista, ne asiakirjat, jotka vaikuttavat politiikan sisältöön tai joihin politiikka vaikuttaa.

## A1.2 Tietoturvapolitiikan julkaisu ja jakelu

### kontrolli

Tietoturvapolitiikka täytyy julkaista ja jakaa ja siitä täytyy tiedottaa siten, että tarvittavilta osin koko organisaatio ja kolmannet osapuolet ovat tietoisia ja heillä on ymmärrys asiakirjasta ja sen sisällöstä.

### käytännön ohjeita

a) Asiakirja julkaistaan siten, että se on saatavilla helposti ja ymmärrettävässä muodossa.
b) Asiakirjasta tiedotetaan ja se jaetaan organisaatiolle siten, että tarvittava tietoisuus sen merkityksestä ja ymmärrys sisällöstä syntyy.
c) Kolmansien osapuolten käyttöön jaettavasta asiakirjasta on tarvittaessa karsittava ne tiedot ja asiat, joiden paljastuminen voisi olla uhka tietoturvallisuudelle ja joita on tarpeetonta mainita tietoturvapolitiikassa. Organisaation sisäiseen käyttöön tarkoitetuissa tarkemmissa toimintaohjeissa ja kuvauksissa voidaan esimerkiksi käytettävät menetelmät ja toimintaohjeet kuvata yksityiskohtaisemmin.

## A1.3 Tietoturvapolitiikan ylläpito

### kontrolli

Asiakirjalla on oltava omistaja ja vastuullinen taho, joka vastaa asiakirjan ylläpidosta, säännöllisistä katselmuksista, asiakirjan arvioinnista ja muutoksista tarpeen mukaan. Muutosten dokumentoinnin ja tiedotuksen on oltava vastaavalla tasolla ja vastaavanlaajuisia kuin koko asiakirjan jakelu.

### käytännön ohjeita

a) Asiakirjalle määritellään omistaja ja päivityksistä vastaava taho.
b) Säännöllisistä katselmuksista sovitaan. Katselmuksen tuloksena on tieto mahdollisista kustannus- ja muista vaikutuksista ja politiikan muutostarpeista esimerkiksi lainsäädännön, organisaation, sen toiminnan tai teknisen ympäristön ja uusien tai muuttuneiden riskien perusteella.
c) Päivitetty asiakirja jaetaan ja siitä tiedotetaan asianmukaisesti.

## A1.4 Tietosuojapolitiikan luominen

### kontrolli

Tietosuojapolitiikan on oltava organisaation toiminta ja voimassa olevat lait huomioiden kirjoitettu ja johdon hyväksymä.

### käytännön ohjeita

Ainakin alla mainitut asiat sisällytetään tietosuojapolitiikkaan, kaikkia yksityiskohtia ei ole välttämätöntä mainita. Tietosuojavaltuutetun toimisto on julkaissut ohjeen *Laadi tietosuojaseloste*, johon on myös hyvä tutustua.

a) yleiset periaatteet
   - maininta voimassa olevista ja noudatettavista laeista
   - henkilötietolain edellyttämä (henkilörekisterin) käyttötarkoituksen kuvaus
   - henkilötietolain edellyttämä etukäteissuunnittelu
   - henkilötietolain edellyttämät muut periaatteet
   - perusteluista: viranomaisen toiminnan julkisuudesta ja salassapidon periaatteista
   - lainmukaisuudesta: millaista salassapitoa ja suojaamista edellytetään
   - vastuut
   - henkilön yksityisyyden suojaan liittyen henkilötietojen ja henkilön muiden luottamuksellisten tietojen suojaamisesta: kyse kaikista henkilön tiedoista
   - standardin mukaisesta tietojen turvaamisesta ja hyvästä tietojenkäsittelytavasta
   - organisaation voimassa olevasta tietoturvapolitiikasta
b) tietojen luokittelun ja ryhmittelyn periaatteet
   - henkilötiedot, potilastiedot, muut tiedot: jos tietoturvan takia on erillinen tarve ryhmitellä, näin voidaan tehdä
   - mistä lähteistä tietoja tulee (esimerkiksi hoitotapahtuman yhteydessä annettavat ja hoitotapahtumassa syntyvät tiedot, jo olemassa olevat tiedot, muilta terveydenhuollon toimintayksiköiltä ja muilta viranomaisilta saatavat tiedot)
c) tietojen säilytyksen ja käsittelyn periaatteet
   - henkilötietolain edellyttämä tietojen käyttötarkoituksen kuvaus koko tietojen elinkaaren aikana
   - säilytysvaatimukset (katso STM:n oppaita 2001:3, Potilasasiakirjojen laatiminen ja muun hoitoon liittyvän materiaalin säilyttäminen)
   - poiston ja muuttamisen periaatteet (vanhentuneet, virheelliset, oikaisu)
d) tietojen luovutuksen periaatteet (katso STM:n oppaita 2001:3, Potilasasiakirjojen laatiminen ja muun hoitoon liittyvän materiaalin säilyttäminen, OSVE 6/2004, Tietoturvallinen kommunikaatioalusta, luovutusten ja luovutuslokin hallinnan suositukset OSVE 6/2004, Turvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004)
   - suostumus
   - lain mahdollistamat tapaukset
e) henkilöstö
   - lista oikeutetuista henkilöistä ja rooleista (lääkärit, hoitajat ym.)

- valtuuksista ja oikeutetuista henkilöistä (hoitosuhteen olemassaolo, käyttötarkoitussidonnaisuus olemassa, käsittely vain tarpeen mukaisessa laajuudessa)
- ammattihenkilön velvollisuuksista, oikeuksista ja ammattietiikasta (salassapito- ja vaitiolovelvollisuus)
- tietoturvatietoisuus ja -koulutus
- väärinkäytösten seuraukset

f) tietojärjestelmien periaatteellinen kuvaus
- käyttäjien ja käyttöoikeuksien hallinta
- mahdollisesti maininta fyysisen ympäristön ja tietoliikenteen turvallisuudesta
- seuranta, valvonta, hälytykset

g) henkilön oikeus omiin tietoihinsa
- rekisteriseloste
- mihin tietoihin oikeudet ja millä poikkeuksilla
- tietojen korjausmahdollisuus
- mahdollisesti maininta, mihin tietoihin henkilöllä ei ole oikeutta (esim. lokitiedot ovat herättäneet keskustelua)
- käytännön kuvaus ja toimintaohje henkilölle
- jos henkilön tarkastusoikeus toteutettu verkkosovellukseksi, sen tarkempi kuvaus turvaominaisuuksineen

h) valitusmenettely
- rekisteröidyn havaitsemat tietosuojaloukkaukset
- henkilöstön ja ulkopuolisten havaitsemat tietosuojaloukkaukset
- valvova viranomainen.

## A1.5 Tietosuojapolitiikan julkaisu ja jakelu

### kontrolli

Tietosuojapolitiikka täytyy julkaista ja jakaa ja siitä täytyy tiedottaa siten, että tarvittavilta osin koko organisaatio on tietoinen ja sillä on ymmärrys asiakirjasta ja sen sisällöstä.

### käytännön ohjeita

a) Asiakirja julkaistaan ja jaetaan siten, että se on saatavilla helposti ja ymmärrettävässä muodossa. Potilaalle tai asiakkaalle asiakirja voidaan jakaa esimerkiksi aina sitä pyydettäessä. Se voi olla jaossa myös odotustiloissa ja saatavilla Internetissä.

b) Asiakirjasta tiedotetaan riittävällä laajuudella ja esimerkiksi informoidaan potilasta tai asiakasta hoito- tai palvelutilanteessa.

## A1.6 Tietosuojapolitiikan ylläpito

### kontrolli

Asiakirjalla täytyy olla omistaja ja vastuullinen taho, joka vastaa asiakirjan ylläpidosta, säännöllisistä katselmuksista, asiakirjan arvioinnista ja muutoksista tarpeen mukaan.

### käytännön ohjeita

a) Asiakirjalle määritellään omistaja ja päivityksistä vastaava taho.

b) Säännöllisistä katselmuksista sovitaan. Katselmuksen tuloksena on tieto mahdollisista muutostarpeista.

c) Päivitetty asiakirja jaetaan ja siitä tiedotetaan asianmukaisesti.

## 3.2 Uhkista ja riskeistä

Seuraavassa on mainittu tyypillisiä uhkia, joiden aiheuttamiin riskeihin voidaan vaikuttaa toteuttamalla ja käyttöönottamalla riittävän kattavat politiikat:

a) Johto ei ole tietoinen organisaation toimintaan vaikuttavista uhkista ja riskeistä.
b) Organisaation toiminnalle tärkeitä tietoja ei ole tunnistettu.
c) Johto ei ole sitoutunut tietoturvallisuustyöhön.
d) Henkilöstö ei ole tietoinen tietoturvapolitiikasta.
e) Henkilöstö ei ymmärrä tietoturvapolitiikan sisältöä.
f) Tietoturvapolitiikalle ei ole määritelty omistajaa ja vastuuhenkilöä.
g) Tietoturvapolitiikkaa ei katselmoida säännöllisesti.
h) Katselmoinnin tuloksista ei raportoida asianmukaisesti.
i) Tietoturvapolitiikka ei vastaa voimassa olevia lakeja tai lakeihin tehtyjä muutoksia.
j) Tietoturvapolitiikka ei vastaa teknologian muutoksia ja kehitystä.
k) Tietoturvapolitiikka ei vastaa organisaatioon tehtyjä muutoksia.
l) Tietoturvapolitiikka ei vastaa muutoksia organisaation toiminnassa.
m) Tietoturvapolitiikka ei vastaa muutoksia tietoturvallisuuteen kohdistuvissa riskeissä.
n) Yhteistyökumppaneille (mukaan lukien asiakkaat ja alihankkijat) ei ole jaettu tietoturvapolitiikkaa.
o) Puutteellisesta tai väärin ymmärretystä dokumentaatiosta johtuen yhteistyökumppanit ovat epätietoisia, epäluuloisia ja osoittavat epäluottamusta, joka kohdistuu organisaation toiminnan ja sen tietoturvallisuuden laatuun.
p) Puutteellisesti laadittu tietoturvapolitiikka aiheuttaa organisaatiolle huonoa mainetta.
q) Puutteellisesti laadittu tietoturvapolitiikka aiheuttaa organisaatiolle juridisia ongelmia.
r) Liian yksityiskohtainen tai liian tarkkoja yksityiskohtia sisältävä tietoturvapolitiikka luo ulkopuoliselle pääsymahdollisuuden organisaation luottamuksellisiin tietoihin.

Politiikat julkaistaan tarvittavalla laajuudessa, jaetaan henkilöille ja organisaatioille tarpeen mukaan ja huolehditaan, että henkilöstö on omaksunut ne sisältöineen. Johdolla ei välttämättä ole tietoturvapolitiikan kirjoittamiseen tarvittavia perustietoja ja ymmärrystä. Silti politiikkojen laatiminen, hyväksyminen ja käyttöönotto edellyttävät toimenpiteitä nimenomaan johdolta.

# 4 Tietoturvallisuuden hallinnointi ja organisaatio

## 4.1 Yleistä

Tietoturvallisuustoimintaan sitoutunut, esimerkkiä näyttävä johto ja toimivat johtamisen menetelmät ovat edellytys tietoturvallisen toiminnan olemassaololle ja kehitykselle. Organisaatiossa on myös oltava tarkasti määritelty hyväksytyt toimintaperiaatteet ja käytännöt, julkistettu tietoturvapolitiikka, nimetty turvahallinto ja määritelty sen henkilöiden roolit ja vastuut. Koko henkilöstön on oltava tietoinen tietoturvapolitiikasta, tietoturvallisuustavoitteista ja hyväksytyistä toimintatavoista. Kaikki tämä täytyy dokumentoida kirjallisesti, selkeästi ja kattavasti.

Turvallisuudesta vastaavan organisaation tehtävänä on tunnistaa ja hallita riskit ja suojata koko organisaatio, sen toiminta ja omaisuus riskeiltä ja niiden aiheuttamilta vahingoilta. Turvaorganisaation täytyy olla teknisesti ajan tasalla, koska nykyteknologian muuttuessa ja kehittyessä jatkuvasti haasteet uhkien ja riskien torjumiseksi lisääntyvät ja niiltä suojautuminen monimutkaistuu. Yhteistoiminta eri standardointi- ja teknisillä foorumeilla on usein suositeltavaa.

Tiedottaminen ja palautteen antaminen sekä tietoturvaorganisaatiolle että koko henkilöstölle on tärkeää, vaikka tietoturvaloukkauksia ei olisikaan havaittu. Myös positiivinen palaute edesauttaa turvallisuustietoisuutta ja parantaa turvallisuutta. Poikkeamien ja rikkeiden käsittely on kuvattu omassa luvussaan.

Nykyään organisaatiot saattavat ulkoistaa toiminnastaan tiettyjä osia, jotka esimerkiksi eivät kuulu organisaation ydintoimintaan tai joiden ulkoistamisella haetaan toiminnallisia, taloudellisia tai kilpailullisia etuja. Jos esimerkiksi tietojenkäsittelylaitteistoja tai -palveluita operoi joku kolmas osapuoli, on tästä toiminnasta syntyvät riskit kartoitettava ja huomioitava myös sopimuksellisella tasolla.

Organisaation tiloissa saattaa myös liikkua ulkopuolisia, organisaatioon kuulumattomia ihmisiä, jotka saattavat aiheuttaa turvallisuusriskejä. Näitä henkilöitä voivat olla esimerkiksi huoltohenkilöt (siivoojat, kiinteistö-, laite- ja ohjelmistohuolto, ulkoiset konsultit), asiakkaat, potilaat ja omaiset. Tietyissä tapauksissa heiltä voidaan vaatia henkilökohtaisen salassapito- ja vaitiolosopimuksen allekirjoitus. Tämä tyypillisesti estää ainakin tahattomia rikkeitä, kun turvatietoisuus paranee ja henkilökohtaisten sanktioiden uhka ohjaa tarkkaavaisuuteen.

Turvahallinnon on hyvä tehdä joitakin oletuksia ympäristöön, organisaatioon ja järjestelmien toimintaan liittyen. Nämä oletukset voivat olla "truismeja", jotka ovat käytännössä todellisia kaikessa toiminnassa ja useimmissa organisaatioissa. Jokapäiväisestä toiminnasta aiheutuu usein erilaisia riskejä, joten oletuksien listaaminen ja niistä aiheutuvien riskien tunnistaminen auttaa tietoturvallisuutta. Oletus voi olla joko tiedossa oleva erittäin todennäköinen tapahtuma tai ympäristöön liittyvä tosiasia. Tyypillisiä oletuksia voivat olla esimerkiksi

- käyttäjät tekevät huolimattomuusvirheitä
- käyttäjät eivät omaksu kaikkia toimintatapoja ja ohjeita vaan käyttävät oikoteitä
- pääkäyttäjät voivat olla pahantahtoisia
- verkkohyökkäyksiä yritetään
- työasemia käytetään siten, että mahdollisuus erilaisten virusten leviämiseen on mahdollista
- järjestelmissä on toimintahäiriöitä
- järjestelmät sijaitsevat paikassa X, varmistusmediat paikassa Y
- kaikki ulkoinen tietoliikenne on suojattu palomuurilla
- työasemissa ei ole korppuasemia
- toimitiloissa on käytössä kulunvalvonta
- kiinteistössä ei voi liikkua ilman kulkukorttia.

## A2.1 Johdon sitoutuminen ja toiminta

### kontrolli

Johdon täytyy sitoutua ja tukea organisaatiota tietoturvatoiminnassa näkyvästi ja varata toimintaan riittävästi resursseja. Tietoturvan hallinnoinnin täytyy olla tarkasti määritelty ja organisaation nimetty ja selkeästi vastuutettu. Palautetta on annettava säännöllisesti.

### käytännön ohjeita

a) Johto näyttää esimerkkiä ja motivoi tietoturvatoimintaa.
b) Tietoturvallisuustavoitteet määritellään kattavasti ja selkeästi.
c) Tietoturvapolitiikka määritellään ja sitä ylläpidetään. Katselmuksille ja arvioinneille on määritelty prosessi.
d) Ohjataan riskienhallintatoimintaa.
e) Nimetään tietoturvallisuusorganisaatio ja määritellään roolit ja vastuut. Varataan kaikki tarvittavat resurssit. Tarvittaessa tietoturvallisuusorganisaatio nimetään organisaation yleisestä turvallisuudesta vastaavan organisaation yhteyteen, ja joka tapauksessa luodaan yhteistyökanava näiden toimintojen välille. Kuitenkin varotaan tarkkaan, että näiden organisaatioiden käytössä ei ole sellaisia yhteisiä resursseja, joiden toiminta voi vaarantua tai ylikuormittua vakavassa vikatilanteessa, ettei näiden organisaatioiden välillä ole eturistiriitoja ja ettei vastuita ole keskitetty liikaa.
f) Johdon ja turvaorganisaation välinen yhteistyö on saumatonta ja säännöllistä.
g) Turvatoiminnan kehittäminen, seuranta ja käytännön työ noudattavat sovittuja prosesseja.
h) Turvallisuustietoisuutta kehitetään ja turvallisuusasioista tiedottaminen liitetään osaksi toimivia käytäntöjä.
i) Arvioidaan koulutuksen tarve ja päätetään koulutuksesta. Henkilöstön koulutus on suunnitelmallista ja säännöllistä.
j) Toimintaa seurataan, valvotaan ja mitataan. Toiminnasta annetaan säännöllistä palautetta.
k) Turvaloukkauksiin puututaan.
l) Jos organisaation on tarpeen sertifioida tietoturvallisuustoimintansa, johto organisoi sertifioinnin osaksi tietoturvapolitiikan katselmus- ja arviointiprosessia. Sertifiointi teetetään ulkopuolisella auditoijalla.

## A2.2 Turvaorganisaation toiminta

### kontrolli

Päivittäisessä tietoturvatyössä on toimittava sovittujen käytäntöjen mukaisesti ja noudatettava tietoturvapolitiikkaa. Kaikkien tehtävien on oltava selkeästi vastuutettuja. Muutoksen hallintaan ja uusien tietojärjestelmien hyväksyntään on noudatettava sovittuja prosesseja. Yhteistyön johdon kanssa on oltava säännöllistä. Turvaorganisaation on toteutettava tehtävänsä: sen on hallittava riskit ja suojauduttava niiltä.

### käytännön ohjeita

a) Tietoturvatyössä noudatetaan tietoturvapolitiikkaa.
b) Suojattavat tiedot ja tieto-omaisuus määritellään. Tutustutaan myös dokumenttiin *ISO/IEC 15408 "Evaluation Criteria for Information Technology Security"*, joka on tietoturvallisten järjestelmien arviointikriteeristö. Se auttaa laatimaan tietojärjestelmille niiden tietoturvallisuuden vahvuuden ja luokittelun kuvaavan tietoturvaprofiilin. On huomattava, että vaikka koulutusta tai sen yksityiskohtia ei saada mukaan järjestelmän turvaprofiiliin, on näiden huomioiminen tuiki tarpeellista.
c) Riskien hallinnan osalta tutustutaan dokumenttiin ISO/IEC 13335 "Guidelines for the Management of IT Security".

d) Riskienarviointi- ja hallintatyölle määritellään prosessit ja valitaan noudatettavat menetelmät ja toimintatavat. Uhkat ja riskit voidaan luokitella esimerkiksi tämän dokumentin mukaisesti. Riskienhallintaan liittyen kannattaa tutustua myös Valtiovarainministeriön ohjeeseen riskien arvioinnista. Se sisältää käytännön tietoa, toimintaohjeita ja valmiiksi jäsenneltyjä asialistoja ja taulukoita.
e) Määritellään yksilölliset vastuut tiedoille ja tietojärjestelmille. Tästä on mainittu lisää tämän ohjeen luvussa *omaisuuden hallinta*.
f) Tietoihin kohdistuvat riskit kuvataan ja analysoidaan. Esimerkki riskitaulukosta on tietojen luokittelutaulukoiden yhteydessä luvussa *omaisuuden hallinta*.
g) Määritellään menettelytapa uusien tietojärjestelmien käyttöönotolle. Lisätään uudet tietojärjestelmät olemassa oleviin toimintaohjeisiin.
h) Seurataan ja valvotaan turvaloukkauksia. Raportoidaan johdolle sovitulla tavalla tarpeen mukaan.
i) Ylläpidetään omaa teknistä osaamistasoa. Muualla havaittuja ja raportoituja tietoturvauhkia ja haavoittuvuuksia seurataan ja tiedossa olevat korjaukset otetaan tarpeen mukaan käyttöön. Seurannan piirissä pidetään ainakin käytössä olevien tietojärjestelmä-, laitteisto- ja ohjelmistotoimittajien raportoimia ongelmia sekä erilaisia julkisia tietoturvapalveluita (esimerkiksi Viestintäviraston CERT-FI-palvelun verkkosivuilla julkaistavat: *www.ficora.fi/suomi/tietoturva/varoitukset.htm*, *www.ficora.fi/suomi/tietoturva/ohjeet.htm* ja *www.ficora.fi/suomi/ tietoturva/ttnytarkisto.htm*).
j) Sovitaan organisaation koulutuksesta, määrästä ja laadusta. Järjestetään koulutus sekä tuki- ja neuvontapiste.
k) Järjestetään menetelmä, jota käyttämällä kuka tahansa voi raportoida turvaloukkauksista ja -uhkista.
l) Organisaation ulkopuolisille toimijoille, kolmansille osapuolille, määritellään auditointi- ja seurantaprosessi. Oikeuksien ja valtuuksien määrittelyssä pyritään käyttämään samoja menettelyitä ja toimintatapoja kuin mitä on käytössä omassa organisaatiossa.
m) Kolmansien osapuolten kulkuoikeudet ja pääsy tarvitsemiinsa tietoihin määritellään tapauskohtaisesti. Kolmansia osapuolia voivat olla esimerkiksi potilaat, asiakkaat, ohjelmisto- ja laitteistoylläpito, opiskelijat, ulkoistuspalveluiden tuottajat ja huoltohenkilöstö.

## A2.3 Lakien, standardien ja sopimusten huomioiminen

### kontrolli

Turvaorganisaation täytyy seurata lainsäädännön ja standardien kehitystä ja sillä on oltava tieto lakeihin ja standardeihin tehtävistä muutoksista. Sen on ylläpidettävä omaa osaamistaan ja oltava perillä uusien teknologioiden vaikutuksista uhkiin, riskeihin ja niiden torjuntaan. Tiedossa oleviin riskeihin pitää varautua myös sopimuksellisesti sekä kolmansien osapuolten (kuten alihankkijat ja palvelu-, laite- ja ohjelmistotoimittajat) kanssa solmittavissa sopimuksissa että henkilökohtaisilla salassapito- ja vaitiolosopimuksilla aina tarvittaessa.

### käytännön ohjeita

a) Arvioidaan muutoksia riskeissä, laeissa ja standardeissa. Päivitetään tietoturvapolitiikkaa, toimintatapoja ja -ohjeita tarpeen mukaan.
b) Seurataan viranomaisten ja muiden tahojen antamia suosituksia. Seurattavia tahoja ovat esimerkiksi tietosuojavaltuutettu, Stakes ja Viestintävirasto. Toimitaan tarvittaessa näiden kanssa yhteistyössä.
c) Ollaan mukana tarvittavissa standardointi- ja yhteistyöelimissä. Tuodaan esille omat tarpeet ja vaatimukset.

d) Huolehditaan, että ulkoisten toimijoiden kanssa solmittavat sopimukset noudattavat tietoturvapolitiikkaa. Tarvittaessa tehdään henkilökohtaisia salassapito- ja vaitiolosopimuksia tapauskohtaisesti.

## 4.2 Uhkista ja riskeistä

Seuraavassa on mainittu tyypillisiä uhkia, joiden aiheuttamiin riskeihin voidaan vaikuttaa johdon ja tietoturvaorganisaation toiminnalla: organisoimalla ja vastuuttamalla, tiedottamalla ja kouluttamalla, tarpeellisten standardien ja teknologioiden hyödyntämisellä, palautteen antamisella sekä solmituilla sopimuksilla. Alla mainitut uhkat ovat luonteeltaan yleisiä, joten yksi uhka voi aiheuttaa lukuisia erilaisia ja eritasoisia riskejä.

a) Tietoturvallisuustavoitteita ei ole määritelty selkeästi.
b) Riskienhallintatoimintaa ei ohjata ja seurata.
c) Tietoturvallisuusorganisaatiota ei ole nimetty.
d) Tietoturvallisuusorganisaatiota ei ole vastuutettu selkeästi.
e) Tietojen turvaamistoimintaan ei ole varattu riittävästä resursseja.
f) Yhteistyö johdon ja turvaorganisaation välillä ei suju.
g) Turvallisuusasioista ei tiedoteta.
h) Henkilöstöllä ei ole riittävää turvallisuustietoutta.
i) Henkilöstöä ei kouluteta tai koulutus on puutteellista.
j) Henkilöstö ei välitä tietoturvallisuusmääräyksistä ja -ohjeista.
k) Turvatoimintaa ja toiminnan turvallisuutta ei mitata.
l) Turvallisuusasioista ja -toiminnasta ei anneta palautetta.
m) Turvaloukkausten seuranta puuttuu tai on puutteellista.
n) Havaittuihin turvaloukkauksiin ei puututa.
o) Poikkeusolojen tietojenkäsittelyyn ei ole toimintasuunnitelmaa.
p) Vikatilanteesta palautumiseen ei ole toipumissuunnitelmaa.
q) Tietoturvatyö ei ole järjestelmällistä ja tietoturvapolitiikan mukaista.
r) Turvattavia tietoja ja tietojärjestelmiä ei ole määritelty.
s) Riskienhallintatyö on puutteellista.
t) Uusia tai muuttuneita riskejä ei tunnisteta.
u) Uudet tietojärjestelmät eivät pääse riskienhallinnan piiriin.
v) Uudet tietojärjestelmät aiheuttavat riskejä, joita ei ole tunnistettu.
w) Uusien tietojärjestelmien käyttöönotolle ei ole sovittua menettelytapaa.
x) Tietojärjestelmille ei ole määritelty vastuuhenkilöitä.
y) Turvaloukkauksia ei seurata eikä niistä raportoida.
z) Organisaatiota ei kouluteta.
å) Turvallisuusasioista organisaatiossa syntyviin kysymyksiin ei ole tuki- tai palvelupistettä.
ä) Turvaloukkausten raportointiin ei ole menetelmää tai se ei ole tiedossa.
ö) Kolmansien osapuolten turvakäytäntöjä ei arvioida.
aa) Kolmansien osapuolten aiheuttamia riskejä ei tunnisteta.
bb) Kolmansien osapuolten toimintaa ei seurata.
cc) Kolmansille osapuolille myönnetään liian suuret valtuudet.
dd) Lakeja ei seurata tai muutoksia ei huomioida.
ee) Standardeja ei seurata tai muutoksia ei huomioida.
ff) Viranomaisten antamia suosituksia ei seurata tai niitä ei huomioida.
gg) Standardeja tai viranomaisten suosituksia ei pystytä teknisesti toteuttamaan.
hh) Ulkopuolisten tahojen kanssa solmitut sopimukset eivät ota huomioon tietoturvallisuusvaatimuksia.
ii) Ulkopuolisten henkilöiden kanssa ei ole voimassa olevia salassapito- ja vaitiolosopimuksia.

# 5 Omaisuuden hallinta

## 5.1 Yleistä

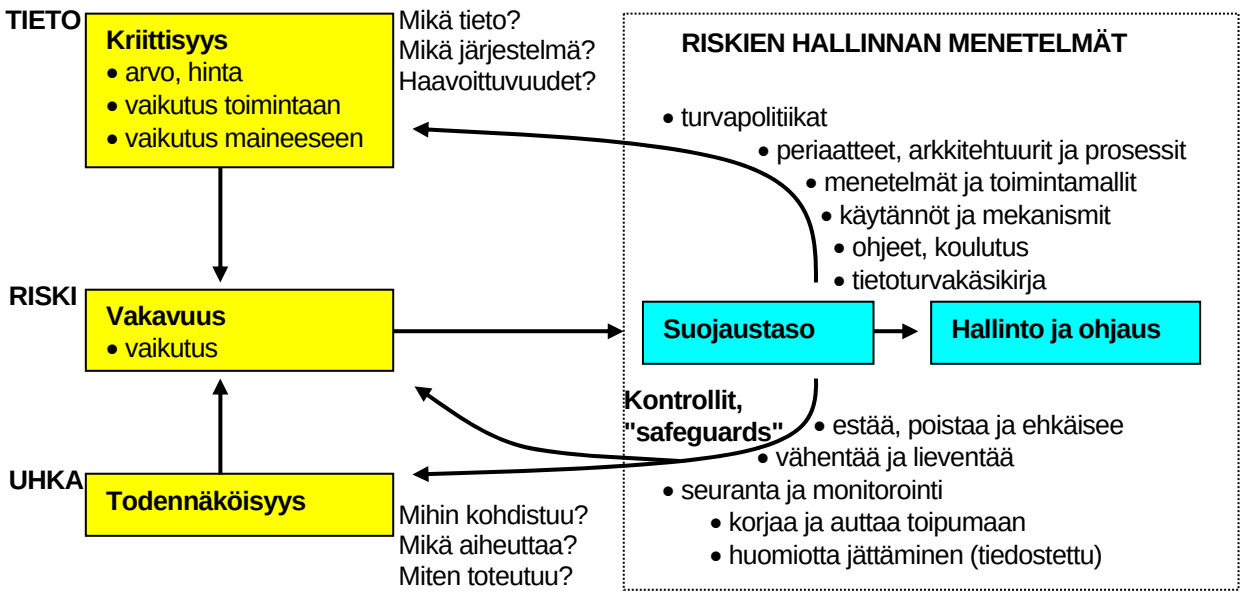
ISO 17799 standardissa käytetty omaisuuden käsite (*asset*) ei ole yhtenevä suomalaisen lainsäädännön käsitteiden kanssa. Sen mukaan voi omistaa laitteistoja, mutta asiakirjojen ja tietojen käsittelyssä puhutaan lähinnä määräämisvallasta sekä rekisterinpitäjän toimivallasta, vastuista ja tehtävistä (M. Kleemola, tietosuojavaltuutetun toimisto). Tässä raportissa pyritään pitäytymään termissä (tieto)omaisuus.

Organisaation toiminnan kannalta kaikki omaisuus ja sen merkitys on oltava tarkassa tiedossa, oli tämä omaisuus kiinteässä muodossa tai tieto-omaisuutta. Organisaation toiminnan ja tietoturvallisuuden kannalta oleellinen tieto-omaisuus – tiedot ja tietojärjestelmät – on pääomaa, joka on dokumentoitava ja suojattava. Usein tieto-omaisuudesta puhuttaessa käytetään myös termiä tietovaranto, mutta termit eivät ole täsmälliset synonyymit keskenään. Luettavuuden helpottamiseksi tieto-omaisuutta kutsutaan vastedes yksinkertaisemmin pelkästään tiedoksi tai tiedoiksi.

Omaisuuteen kohdistuu erilaisia uhkia ja riskejä. Näitä tunnistettaessa on määriteltävä, miltä kaikelta tietoja ollaan suojaamassa – muodostavatko riskin esimerkiksi käytettävät tekniset tai teknologiset järjestelmät, liittyykö riski käytössä olevaan ympäristöön kuten toimitiloihin, vai onko se mahdollisesti ihmisten toiminnasta johtuva, tahallinen tai tahaton. Riski täytyy tunnistaa mahdollisimman yksityiskohtaisesti. Täytyy myös olla selvillä, ollaanko suojaamassa tietojen eheyttä (tiedot ovat alkuperäisiä ja muuttumattomia), saatavuutta ja käytettävyyttä (tiedot ovat niitä tarvitsevien henkilöiden saatavissa ja käyttökelpoisia) vai luottamuksellisuutta (tiedot eivät joudu vääriin käsiin).

Kaikella tiedolla on oltava omistaja, joka vastaa kuhunkin tietoon kohdistuvilta riskeiltä suojautumisesta ja asianmukaisten kontrollien olemassaolosta. Vaikka tiedon omistaja vastaa kontrolleista ja valvoo niiden toimintaa, vaadittava työ tehdään usein jonkun muun, määritellyn tahon toimesta.

Jotta voidaan varmistua, että tiedot on suojattu riittävällä tasolla, kaikki tiedot täytyy luokitella. Tietojen tärkeys on määriteltävä, samoin kuin tietojen turvaluokitus eli julkisuuden ja salaisuuden taso. Kun tietojen tärkeys ja erilaisten riskien kriittisyys – todennäköisyys ja vaikutukset – on tunnistettu, tiedoille saadaan määriteltyä suojaustaso ja prioriteetti. Tältä pohjalta voidaan valita ja toteuttaa sopivat ja tarpeelliset suojausmenetelmät. Kun riskeiltä suojaudutaan, tiedon omistaja tekee yhteistyötä turvaorganisaation kanssa ja antaa tälle riittävät tiedot, jotta valmius tietojen asianmukaiseen suojaukseen syntyy. Tietojen luokittelu valaakin perustan ymmärtämiselle, miten erilaisia tietoja täytyy käsitellä ja suojata. Ohessa on periaatekuva tiedoista ja niihin kohdistuvien riskien hallinnasta.




Kuva 3 – tietoihin kohdistuvat riskit ja niiden hallinta

## 5.2 Uhkista ja riskeistä

Organisaatiolle tärkeisiin tietoihin kohdistuviin uhkiin varauduttaessa on oleellista, että tiedot tunnistetaan, luetteloidaan, merkitään ja luokitellaan tiedot sekä määritellään niille vastuullinen omistaja. Kuhunkin tietoon kohdistuvat riskit analysoidaan ja määritetään tietojen suojaustaso. Jos tässä epäonnistutaan, tietoturvallisuudelle aiheutuu erilaisia uhkia. Oheinen lista ei ole kattava eikä missään nimessä riittävän yksityiskohtainen. Kuhunkin kohtaan liittyen voidaan tunnistaa ja nimetä useita erillisiä riskejä.

a) Tärkeitä tietoja ei ole tunnistettu.
b) Tietoja ei ole luetteloitu tai ne on luetteloitu puutteellisesti.
c) Tietoja säilytetään siten, että ei voida taata niiden pitkäaikaista saatavuutta ja käytettävyyttä.
d) Tietojen sijainti ei ole selvillä.
e) Tiedoille ei ole määritelty omistajaa.
f) Omistaja ei ole tietoinen vastuistaan.
g) Tietoja ei ole luokiteltu.
h) Tietoihin kohdistuvia uhkia ei ole tunnistettu.
i) Tietoihin kohdistuvia riskejä ja niiden seurauksia ei ole analysoitu.
j) Ei ole selkeää määrittelyä, miten erilaisia tietoja pitää käsitellä ja miten ne pitää suojata.
k) Tietoja on suojattu liian tiukasti.
l) Tietoja on suojattu liian kevyesti.
m) Tietoja ei ole merkitty siten, että suojaustaso käy selvästi ilmi.
n) Henkilöstölle ei ole jaettu ohjetta eikä ole syntynyt selvyyttä siitä, miten eri suojaustason tietoja käsitellään.
o) Organisaation, kolmansien osapuolten henkilöt tai asiakkaat eivät ole tietoisia hallussaan olevan organisaation omaisuuden suojaamisvaatimuksista.
p) Organisaation, kolmansien osapuolten henkilöt tai asiakkaat eivät suojaa hallussaan olevaa organisaation omaisuutta riittävästi.
q) Henkilön työsuhteen loppuessa henkilön haltuun jää organisaation omaisuutta.
r) Ulkopuolisille toimijoille ei ole toimitettu tietojen käsittely- ja suojaussääntöjä.

## A3.1 Omaisuuden muoto

### kontrolli

Kaikki tieto on säilytettävä sellaisessa muodossa, mikä vastaa tiedon tärkeyttä ja tekee mahdolliseksi riittävien palvelujen luomisen tietojen saatavuudelle, käytettävyydelle ja oikeellisuudelle ja pääsyoikeuksien hallinnalle. Jos kriittistä tietoa säilytetään sähköisessä muodossa, on kiinnitettävä erityistä huomiota tietojärjestelmien riittävään suojaamiseen ja tietojenkäsittelyn menetelmien valintaan.

Seuraavissa luvuissa käsitellään tarkemmin laitteistoihin, käyttöympäristöihin, ohjelmistoihin, tietoliikenteeseen, käyttötapoihin ja toimintaan liittyviä vaatimuksia ja turvaamista.

### käytännön ohjeita

a) Varmistetaan, että tietojen säilytysmuoto vastaa tietojen kriittisyyttä ja tietojen saatavuuteen, käytettävyyteen ja oikeellisuuteen liittyviä vaatimuksia.
b) Säilytettäessä tietoja sähköisessä muodossa varmistutaan, että tiedot ovat sellaisessa formaatissa ja tietorakenteissa, että ne ovat luettavissa ja ymmärrettävissä pitkänkin ajan kuluttua.
c) Säilytettäessä tietoja sähköisessä muodossa varmistutaan, että käytetään sellaisia laitteistoja, ohjelmistoja ja tietovälineitä, jotka ovat käyttökelpoisia ja toimintakykyisiä pitkänkin ajan kuluttua.

## A3.2 Inventaario ja luettelointi

### kontrolli

Kaikkien tietojen täytyy olla selkeästi tunnistettu. Luettelo tärkeistä tiedoista ja niiden tarpeellisuuden kuvaus (tärkeysluokittelu) täytyy olla tehtynä ja sitä täytyy ylläpitää. Tietojen oikeellisuudesta vastaa kunkin tiedon omistaja. Kaikki erityyppiset tiedot ja niiden sijainti pitää tunnistaa ja dokumentoida. Luetteloitavat tiedot voivat olla esimerkiksi seuraavan tyyppisiä ja muotoisia:

- tiedostot ja tietokannat
- järjestelmä-, arkkitehtuuri-, prosessi- ja toimintakuvaukset sekä erilaiset suunnitelmat
- dokumentaation: ohjeet, manuaalit, koulutusmateriaalin
- varmistusmediat, arkistot ja paperit
- ohjelmistot, kehitystyökalut ja mittausvälineet
- fyysiset järjestelmät: tietokoneet ja laitteet, tietoliikennelaitteet, erilaiset mittaus- ja kuvauslaitteet, tulostimet, telefaxit, valokopiolaitteet, puhelimet ja puhelinvastaajat
- palvelut ja palvelukuvaukset
- ihmiset, heidän osaamisensa ja taitonsa.

Terveydenhuollossa tietoihin sisältyvät esimerkiksi potilastiedot kaikissa muodoissaan: tekstinä, röntgen- ja muina kuvina, erilaisina mittaustuloksina, lääkemääräyksinä jne. *ISO 27799* -standardin luonnos erittelee esimerkiksi seuraavanlaisia terveydenhuollossa käsiteltäviä tai syntyviä tietoja:

- henkilö- ja terveystiedot
- sellaiset henkilöön tai hoitoon liittyvät tiedot, joiden perusteella voidaan selvittää henkilöllisyys tai terveystiedot
- henkilö- tai terveystietojen perusteella luotavat muut henkilöä koskevat tiedot
- tilastolliset ja tutkimukselliset tiedot, joista on poistettu, ja joista ei käy ilmi mikään henkilökohtainen tieto
- kliininen ja lääketieteellinen tieto
- terveyspalveluiden tuottajia koskeva tieto
- julkinen terveystieto (seurantatieto, tilastotieto ym.)
- terveydenhuollon henkilöstöä ja sen toimintaa koskevat tiedot
- tietojärjestelmien hallinnassa ja operoinnissa käytettävät tiedot.

Yllä mainitut tiedot voidaan jakaa tarkkoihin osakokonaisuuksiin, joiden suojaaminen voidaan suunnitella yksityiskohtaisesti tietojen turvaluokituksen mukaisesti.

### käytännön ohjeita

a) Kaikki tärkeät tiedot luetteloidaan.
b) Kunkin tiedon osalta kuvataan sen arvo ja tärkeys. Tärkeysluokittelusta löytyy malleja esimerkiksi Valtiovarainministeriön laatimista *VAHTI-ohjeista* sekä *ISO/IEC:n* dokumenteista, esimerkiksi standardeista 13335 ja 15408. Yksinkertaisimmillaan tiedot voidaan jakaa kolmeen luokkaan: "erittäin tärkeä" (välttämätön), "tärkeä" (tarpeellinen) ja "ei-tärkeä" (tarpeeton). Periaatteena voi esimerkiksi olla, että näistä jälkimmäinen luokka ei vaadi mitään suojaamistoimenpiteitä eikä sen tietoja tarvitse luetteloida.
c) Inventaariota tehtäessä ja luetteloinnissa noudatetaan sovittuja toimintasääntöjä ja sovittua dokumentaatiorakennetta.
d) Luettelossa tulee olla kuvattuna kunkin tiedon osalta ainakin tieto ja sen tärkeys, tiedon sijainti, omistaja ja turvaluokitus. Organisaation tilojen ulkopuolella olevan omaisuuden sijainti on kuvattu erityisen tarkasti.
e) Yksittäisten henkilöiden, työntekijöiden, yhteistyökumppanien, kolmansien osapuolten tai asiakkaiden hallussa olevasta organisaation omaisuudesta tehdään tarvittaessa erillinen, henkilökohtainen luettelo.
f) Ne tietojärjestelmät, jotka ovat alttiita merkittäville muutoksille ja joissa aiotaan toteuttaa uudenlaisia teknologioita, tunnistetaan mahdollisimman aikaisessa vaiheessa ennen tarvittavia muutoksia, ja tieto välitetään tarvittavalla tavalla esimerkiksi muutoksenhallinnan prosesseille.

## A3.3 Tietojen omistus

### kontrolli

Standardin mukaisesti kaikilla tiedoilla täytyy olla nimetty omistaja. Omistajalla on vastuu tiedosta ja niihin kohdistuvilta riskeiltä suojautumisesta.

Terveydenhuollossa potilaaseen liittyvien tietojen omistus ei ole yksikäsitteisesti määritelty. Sillä terveydenhuollon toimintayksiköllä, jossa potilas on hoidossa, on velvollisuus arkistoida ja säilyttää tiedot STM:n asetuksen määräämän ajan muuttumattomina. Sillä on myös tietojen käsittelyn ja koko säilytyksen aikainen velvollisuus huolehtia tietoturvasta ja tietosuojasta. Potilalla puolestaan on oikeus (ellei laista muuta johdu) määrätä siitä, kuka hänen tietojaan käsittelee.

### käytännön ohjeita

a) Omistaja nimetään siten, että omistus ja vastuu tukevat parhaiten organisaation toimintaa. Omistaja voi määräytyä esimerkiksi organisaation toimintaprosessin, hierarkian tai tiedon luonteen mukaan. Terveydenhuollossa standardin tarkoittama omistaja on edellä mainittu. toimintayksikkö.
b) Omistaja vastaa, että tiedot, niiden tärkeys, turvaluokitus ja muut asiat on asianmukaisesti kuvattu.
c) Omistaja vastaa tarvittavien pääsyoikeuksien jakamisesta ja katselmuksista.
d) Omistaja vastaa, että tietoja ja tietojärjestelmiä ylläpidetään asianmukaisesti ja että tarvittaessa on sovittu palvelutasosta *(SLA, service level agreement)* kolmansien osapuolien ylläpitämien tai huoltamien järjestelmien osalta.
e) Omistaja vastaa, että tietojärjestelmistä ja sovelluksista on olemassa asianmukaiset käyttöohjeet.
f) Omistaja ylläpitää omaa osaamistaan, jota tarvitaan omistajuuteen liittyvien velvollisuuksien hoidossa.

g) Päivittäinen vastuu käytöstä nimetään tarpeelliseksi katsotulla tavalla. Vastuu päivittäisestä käytöstä ja ylläpidosta voi olla eri taholla kuin omistus. Tällöin omistajan ja päivittäistä hoitoa tekevän on syytä tavata säännöllisesti, ja käydä läpi järjestelmien hoitoon ja tietoturvaan liittyvät tapahtumat ja tarpeet.

## A3.4 Luokittelun periaatteet

### kontrolli

Tietojen luokittelussa on määriteltävä ainakin tiedon arvo ja tärkeys sekä turvaluokitus. Kuhunkin tietoon kohdistuvat riskit, niiden todennäköisyys ja seurausten vakavuus, on kuvattava. Kunkin tiedon kriittisyys ja prioriteetti on määriteltävä. Yhteistyössä turvaorganisaation kanssa tiedoille määritellään suojaustaso ja suojaustoimenpiteet. Suojauksesta on mainittu lisää tämän ohjeen luvussa *tietoturvallisuuden hallinnointi ja organisaatio.*

### käytännön ohjeita

a) Tietojen tärkeyden luokittelussa noudatetaan sovittuja periaatteita. Tärkeys määrittää osaltaan suojaamistason ja prioriteetin. Tärkeys voidaan jakaa esimerkiksi luokkiin "erittäin tärkeä", "tärkeä" ja "ei-tärkeä".

b) Inventaariossa otetaan huomioon tiedon arvo ja tärkeys sekä vaikutus organisaation toimintaan.

c) Turvaluokitus (salaisuusaste) määritellään. Valtiovarainministeriön laatimista VAHTI-ohjeista löytyy esimerkki tietojen turvaluokittelusta jaettuna julkiseen ja eriasteiseen salaiseen tietoon. Tätä ei kuitenkaan ole suunniteltu terveydenhuollon tietoja ja potilastietoja ajatellen, joten näiden osalta voi olla tarpeen määritellä oma turvaluokitus.

d) Inventaariossa otetaan huomioon tiedon turvaluokitus.

e) Pääsyvaltuudet tietoihin määritellään tarpeiden ja turvaluokituksen mukaisesti. Pääsyvaltuuksien määrittämisessä noudatetaan sovittuja periaatteita. Valtuudet voivat perustua esimerkiksi omistajuuteen, henkilön tehtävään (rooliin) organisaatiossa ja omistajan antamaan valtuutukseen.

f) Tärkeys- ja turvaluokitus arvioidaan aika ajoin sovitulla menetelmällä. Mahdolliset muutokset huomioidaan sekä päivittäisessä toiminnassa että dokumentaatiossa. Vastuu tästä on kunkin tiedon omistajalla.

g) Tietoihin kohdistuvat riskit kuvataan ja analysoidaan yhdessä turvaorganisaation kanssa. Tiedoille määritellään asianmukaiset suojaustoimenpiteet tämän ohjeen luvun tietoturvallisuuden hallinnointi ja organisaatio mukaisesti.

h) Suojaustason määrittelyssä sekä nimeämis- ja merkitsemiskäytännössä kiinnitetään huomiota siihen, että valitut käytännöt ovat selkeitä ja ymmärrettäviä: nimeäminen ja merkintä eivät saa aiheuttaa sekaannuksia tai väärinymmärrystä.

i) Luokittelussa vältetään sitä, että tiedot määritellään tärkeämmäksi tai turvaluokituksen taso suuremmaksi kuin mitä on tarpeen. Liian tiukat vaatimukset estävät organisaation toimintaa ja pyrkivät myös lisäämään erilaisten oikopolkujen käyttöä. Liialliset vaatimukset lisäävät kustannuksia, vaikka turvallisuus todellisuudessa saattaa heiketä, kun tietoja suojataan väärillä prioriteeteilla.

j) Oheisissa taulukoissa on esimerkki riskien määrittelystä. Luokittelu on esimerkinomainen: esimerkiksi sietämätön riski voi tarkoittaa erittäin suurta taloudellista menetystä ja/tai toiminnan keskeytymistä. Merkittävä ja kohtalainen riski eriasteisia taloudellisia, toiminnallisia ja muita (kuten organisaation maine ja julkisuus) vaikutuksia. Vähäinen riski voidaan katsoa sellaiseksi, joka aiheuttaa seurauksia, mutta johon ei erityisesti varauduta tai jonka prioriteetti asetetaan erityisen matalaksi. Riskien määrittelyn yhteydessä arvioidaan myös riskiltä suojautumisen aiheuttamat kustannukset ja turvakontrollien mahdolliset puutteet.

| *Kriittisyys, tärkeät tiedot* | | Seurausten vakavuus | | |
|---|---|---|---|---|
| | | **erittäin vakava** | **vakava** | **vähäinen** |
| **riskin** | **korkea** | merkittävä riski | kohtalainen riski | vähäinen riski |
| **todennäköisyys** | **keskimääräinen** | kohtalainen riski | vähäinen riski | merkityksetön |
| | **alhainen** | vähäinen riski | merkityksetön | merkityksetön |
| | ei merkitystä | "akateeminen" | | |

| *Kriittisyys, erittäin tärkeät tiedot* | | Seurausten vakavuus | | |
|---|---|---|---|---|
| | | **erittäin vakava** | **vakava** | **vähäinen** |
| **riskin** | **korkea** | sietämätön riski | merkittävä riski | kohtalainen riski |
| **todennäköisyys** | **keskimääräinen** | merkittävä riski | kohtalainen riski | vähäinen riski |
| | **alhainen** | kohtalainen riski | vähäinen riski | merkityksetön |
| | ei merkitystä | "akateeminen" | | |

k) Tietojen suojaustaso määritellään kunkin tiedon osalta perustuen seurausten vakavuuteen. Erilaiset suojaustasot sisältävät ennalta sovitut kontrollit ja menetelmät, millä kaikki kyseiseen suojaustasoon kuuluvat tiedot suojataan ja miten niitä käsitellään. Luokittelu täytyy suunnitella huolella, sillä tyypillisesti tiukkaan suojeltuihin tietoihin voi kuulua myös julkisia tietoja yhtä lailla kuin salaisia tai luottamuksellisia. Vaikka organisaation web-sivuilla julkaistut tiedot ovat julkisia, niiden muuttamisen täytyy olla erittäin tarkoin valvottua. Ohessa oleva esimerkki on ainoastaan suuntaa antava: suojausrakenteet täytyy suunnitella vedenpitäviksi, mutta samalla myös riittävän yksinkertaisiksi.

| Tiedon kriittisyys | Suojaustaso | Noudatettavat periaatteet ja menetelmät |
|---|---|---|
| **sietämätön riski** | suojaustaso 1 | Kullekin suojaustasolle on määritetty noudatettavat |
| **merkittävä riski** | suojaustaso 2 | periaatteet, menetelmät ja toimenpiteet, jotka on |
| **kohtalainen riski** | suojaustaso 3 | laadittu osaksi tietoturvakäsikirjaa ja joita käytetään |
| **vähäinen riski** | suojaustaso 4 | organisaation tietojen käsittelyssä ja suojaamisessa. |

## A3.5 Merkitseminen

### kontrolli

Tietojen täytyy olla merkittynä asianmukaisesti, jotta tunnistaminen käsittelyn yhteydessä on selkeää eikä käsittelyssä synny tietoturvariskejä puutteellisista merkinnöistä johtuen. Merkintä koskee sekä laitteiden merkitsemistä, tiedostojen ja tietokantojen merkitsemistä ja mahdollisesti nimeämistä. Myös paperitulosteissa täytyy olla tiedon suojauksen ja omistajan osoittava merkintä. Tyypillisesti tiedot on merkitty vähintään esimerkiksi tekstillä "erittäin salainen", "salainen", "luottamuksellinen", "sisäiseen käyttöön" tai muulla vastaavanlaisella. Merkintä omistajasta takaa, että ulkopuolinen organisaation henkilö voi palauttaa esimerkiksi asiakirjan oikealle omistajalle.

### käytännön ohjeita

a) Sekä fyysiset tiedot (laitteet, tulosteet, mediat ym.) että sähköiset tiedot (tiedostot, sähköpostit ym.) merkitään sovitulla tavalla.

b) Aina tietoja käytettäessä suojaustason tulee ilmetä selkeästi sekä näyttöpäätteellä että esimerkiksi tulostettaessa. Sähköisen tiedon ollessa kyseessä suojaustaso voidaan merkitä esimerkiksi metatietoihin.

c) Kunkin suojaustason vaatimat käsittelysäännöt ja ohjeistus (käyttö, talletus, tulostus, lähetys, tuhoaminen, suojaustason uudelleenmäärittely ym.) asetetaan näkyville ja tiedotetaan.

d) Henkilötietolain vaatimusten perusteella tietoihin tullee merkitä niiden käyttötarkoitus.

e) Perustetaan menettely, jolla jokainen voi raportoida havaitsemansa ongelmat tai rikkeet.

f) Ulkoisille osapuolille tiedotetaan valituista suojaustasoista, toimitetaan käsittelyohjeet ja velvoitetaan osapuolia myös sopimuksellisesti toimimaan annettujen sääntöjen ja ohjeiden mukaisesti.

# 6 Henkilöstöturvallisuus

## 6.1 Yleistä

Tietoturvallisuuteen vaikuttavat sekä tekniset että inhimilliset uhkat. Usein puhutaankin 80–20-säännöstä: turvallisuudesta 80 % muodostuu ihmisten toiminnasta, asenteista, ymmärryksestä ja osaamisesta. Vastaavasti 20 % turvallisuudesta koostuu teknisten ja teknologisten ratkaisuiden ja menetelmien vaikutuksista.

Ihmisten toiminta on suurin turvallisuutta uhkaava tekijä. Suurin osa tästä uhasta muodostuu organisaation sisäisestä toiminnasta ja omasta sekä kolmansien osapuolten – alihankkijoiden, yhteistyökumppaneiden ja asiakkaiden – henkilöstöstä. Henkilöstöturvallisuuden tarkoituksena onkin ehkäistä henkilöstöön liittyviä uhkia, kuten inhimillisiä virheitä, väärinkäytöksiä ja varkauksia. Uhkia ehkäistään ja turvariskejä pienennetään valitsemalla sopivat kontrollit, joiden avulla kiinnitetään huomiota henkilöiden koko työsuhteen aikaiseen ja sen jälkeiseen turvallisuuteen. Erilaiset kontrollit koskevat esimerkiksi henkilöstön palkkausprosessia, toimenkuvien ja vastuiden määrittämistä, sopimuksellista velvoittamista, turvaohjeistusta, -koulutusta ja turvatietoisuuden ylläpitoa sekä toimenpiteitä työsuhteen loppuessa ja salassapitovelvoittamista työsuhteen jälkeen.

## 6.2 Uhkista ja riskeistä

Henkilöstöturvallisuudella hallitaan henkilöstöön ja sen toimintaan liittyviä riskejä. Riskien hallinnassa tarkastellaan kaikkia henkilöstön hallintaan liittyviä toimintoja aina palkkauksesta ja soveltuvuudesta, työsuhteen aikaisesta koulutuksesta ja valvonnasta työsuhteen loppumiseen ja jopa sen jälkeiseen aikaan asti. Henkilöstöriskien toteutuminen käytännön toimissa ei ole hallittavissa, jos tähän ei ole käytettävissä sopivia menetelmiä.

Työtehtävien ja päivittäisen toiminnan kokonaisuutta käsitellään erikseen luvuissa *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus* sekä *tietojärjestelmien kehitys ja ylläpito*. Käyttö- ja pääsyoikeuksiin sekä valtuuksiin liittyvä kokonaisuus käsitellään luvussa *pääsynhallinta*.

Seuraavassa on mainittu yleisiä henkilöstöturvallisuuteen liittyviä uhkia, jotka ovat tarkennettavissa yksityiskohtaisemmiksi.

a) Organisaatioon palkataan henkilöitä, jotka eivät ole sopivia, päteviä tai kykeneviä työtehtävien hoitoon.
b) Henkilön perehdyttämisen yhteydessä ei käsitellä tietoturva-asioita eikä salassapitoa.
c) Kolmannen osapuolen työntekijät aiheuttavat haittoja, kuten varkauksia tai petoksia.
d) Kolmannen osapuolen työntekijät eivät kykene sovitun mukaisiin työtehtäviin tai tekevät työnsä huolimattomasti aiheuttaen organisaatiolle erilaisia haittoja.
e) Puutteellisten tarkastusten vuoksi organisaatiossa työskentelee henkilöitä, joille on määritelty liian suuret valtuudet väärin perustein.
f) Puutteellisten tarkastusten vuoksi organisaatiossa työskentelee henkilöitä, jotka aiheuttavat tietoturvaloukkauksia tahallisesti ja tarkoituksellisesti – esimerkiksi yrittävät päästä käsiksi heille kuulumattomiin tietoihin tai yrittävät muuttaa tai poistaa tietoja ilman asianmukaisia valtuuksia.
g) Arkaluonteisia tietoja vuotaa organisaatiosta ulos, koska salassapitoa ei ole määritelty tai siitä ei ole sovittu.
h) Erilaiset vahingot koituvat organisaation tappioksi eikä niitä saada korvattua, koska työsopimuksissa tai sopimuksissa kolmansien osapuolten kanssa ei sovita vahingonkorvauksista.
i) Organisaation tietoja väärinkäytetään organisaation tilojen ulkopuolella esimerkiksi puutteellisesta tai väärästä suojauksesta, osaamisesta tai ohjeistuksesta johtuen.
j) Organisaation tilojen ulkopuolella sijaitseva omaisuus joutuu varkauden kohteeksi.

k) Henkilön päivittäinen toiminta vaarantaa tietoturvallisuuden, koska tietoturvaan liittyviä vastuita ei ole määritelty koko henkilöstölle.
l) Henkilön päivittäinen toiminta vaarantaa tietoturvallisuuden, koska hän ei ole tietoinen vastuistaan ja tietoturvallisesti oikeanlaisista toimista.
m) Koko henkilöstöä ei ole koulutettu tietoturvalliseen toimintaan, osa henkilöistä on jäänyt koulutuksen ulkopuolelle.
n) Henkilöstölle ei osaa tunnistaa tietoturvariskejä.
o) Tietoturvakoulutus ei ole riittävän säännöllistä tai koulutustilaisuuksia ei järjestetä riittävän usein, että koko organisaatio olisi saanut tarpeellisen osaamisen tietoturvallisuuden hoitamiseen.
p) Ympäristössä, teknologioissa, menetelmissä, prosesseissa, periaatteissa tai päivittäisen käytön toimissa ja ohjeissa tapahtuneista muutoksista ei ole järjestetty asianmukaisia tiedotustilaisuuksia.
q) Henkilöille myönnetään pääsyvaltuuksia arkaluonteisiin tietoihin ennen kuin heille on järjestetty koulutus tietojen turvalliseen käsittelyyn.
r) Tietoturvaloukkauksia ei havaita.
s) Havaituista tietoturvaloukkauksista ei raportoida.
t) Loukkausten raportointiin ei ole menetelmää.
u) Tietoturvakysymyksiin ja raportointiin ei ole määritelty yhteyshenkilöä tai hänestä ei ole tiedotettu.
v) Havaitut ja raportoidut tietoturvaloukkaukset eivät aiheuta toimenpiteitä tai ryhdytään vääriin toimiin.
w) Loukkauksista ei opita vaan samat loukkaukset toistuvat myöhemmin.
x) Turvaloukkaukset aiheuttavat vääriin tahoihin kohdistuvat korjaus- tai kurinpitotoimet.
y) Kurinpitotoimet ja korvaukset ovat liioiteltuja haitan vakavuuteen nähden.
z) Kurinpitotoimet ja korvaukset ovat liian pieniä haitan vakavuuteen nähden.
å) Henkilön kaikista kulku- ja pääsyoikeuksista ja valtuuksista ei ole tarkkaa tietoa.
ä) Työsuhteen loppuessa henkilön kaikkia kulku- ja pääsyoikeuksia sekä valtuuksia ei poisteta.
ö) Henkilön hallussa on organisaation omaisuutta ilman, että organisaatiolla olisi siitä tieto.
aa) Työsuhteen loppuessa henkilön haltuun jää organisaation omaisuutta ilman, että siitä olisi erikseen sovittu.
bb) Työsuhteen loputtua henkilö paljastaa arkaluonteisia asioita, koska häntä ei velvoiteta työsuhteen jälkeisellä salassapidolla.
cc) Irtisanotun henkilön valtuuksia ei ole poistettu irtisanomishetkellä, jolloin henkilö voi väärinkäyttää tietoja.
dd) Työsuhteen loppumisesta ei tiedoteta riittävän laajasti.
ee) Työsuhteen loppuessa henkilö kopioi mukaansa organisaation arkaluonteisia tietoja.
ff) Avainhenkilön työsuhteen loppuessa hänelle jää ainutlaatuista tietoa, joka on tarpeen organisaation toiminnalle.

## A4.1 Tarkastukset työsuhteen solmimisen yhteydessä

### kontrolli

Uutta työntekijää palkattaessa on tehtävä riittävät henkilön taustojen tarkastukset ennen työsuhteen alkua ja työsopimuksen solmimista. Tämä koskee myös esimerkiksi kolmansilta osapuolilta ostettavan konsultointi-, huolto- tai muunlaisen työn tekijöitä. Tarkastuksia tehtäessä on noudatettava voimassa olevia lakeja ja määräyksiä tarkastuksista ja selvityksistä. Henkilöä palkattaessa voidaan toimenkuvan perusteella tehdä tarkastus esimerkiksi rikosrekisterimerkinnöistä, luotto- tai maksuhäiriötiedoista, mahdollisesta huumausaineiden käytöstä, koulutukseen ja osaamiseen liittyvistä todistuksista tai edellisistä työnantajista. Henkilöllisyys on selvitettävä erillisestä henkilöllisyystodistuksesta tai passista. Usein myös ajoneuvon ajolupa on tarkastettava. On huomattava, että usein tarkastuksiin tarvitaan lupa palkatta-

valta työntekijältä. Viranomaiselta tehtävästä turvallisuusselvitysmenettelystä (esimerkiksi rikosrekisterin selvitys) on olemassa oma lainsäädäntönsä ja määräyksensä, jotka on otettava huomioon selvityksiä tehtäessä.

Tyypillisesti tarkastuksen kohteena ovat henkilöllisyys ja toimenkuvasta riippuen palkattavan ansioluettelo sekä sen tiedot: työkokemuksen selvitys vähintään yhdeltä edelliseltä työnantajalta ja koulutukseen liittyvien todistusten oikeellisuuden selvitys tyypillisesti joistakin ulkomaisista tutkinnoista. Lisäksi on yleistä, että selvitetään kielitaito ja mahdolliset rikosrekisteritiedot.

### käytännön ohjeita

a) Organisaation noudattama palkattavien henkilöiden taustan tarkastus- ja selvityspolitiikka määritellään. Politiikassa määritetään, millaiset tarkastukset koskevat mitäkin toimenkuvaa ja kolmannen osapuolen työntekijää.
b) Politiikassa määritellään, miten ja ketkä tarkastuksia tekevät, keillä on oikeus tarkastuksissa ilmeneviin tietoihin ja missä ja miten näitä tietoja säilytetään ja käsitellään.
c) Määrättyä tarkastuspolitiikkaa noudatetaan kaikkien työntekijöiden palkkauksen yhteydessä.
d) Palkkausprosessin yhteydessä täytetään erillinen arkistoitava asiakirja suoritetuista tarkastuksista.
e) Strategisesti tärkeisiin tai tietoturvallisesti arkaluonteisiin asemiin palkattavia henkilöitä palkattaessa noudatetaan erityisen tiukkaa tarkastuspolitiikkaa.
f) Kun kolmansilta osapuolilta palkataan henkilöitä, esimerkiksi konsultteja, väliaikaisia työntekijöitä tai huoltohenkilökuntaa, niiltä edellytetään riittävää tarkastus- ja tiedonantovelvollisuutta vuokrattaviin tai palkattaviin henkilöihin. Kolmansien osapuolten toimintaa koskevat edellytykset mainitaan sopimuksissa.

## A4.2 Sopimukselliset velvoitteet

### kontrolli

Sekä organisaatioon palkattavien henkilöiden että alihankkijoiden, asiakkaiden ja muiden vastaavien organisaatioiden henkilöiden sopimuksissa on kuvattava tietoturvallisuuteen liittyvät ehdot ja vastuut, mihin henkilöiden on sitouduttava. Mikäli on aiheellista, henkilöiden kanssa on solmittava tämän lisäksi erilliset salassapitosopimukset. Näin toimitaan yleensä silloin, kun voimassa olevat sopimukset eivät kata salassapitoa ja vaitioloa ja henkilöillä on pääsy arkaluonteisiin tietoihin esimerkiksi osallistumiensa projektien kautta.

### käytännön ohjeita

a) Henkilöiden kanssa solmittavissa työ- ja muissa sopimuksissa mainitaan kaikki henkilön tietoturvalliseen toimintaan ja tietojen suojaamiseen kohdistuvat ehdot, vastuut ja velvollisuudet sekä noudatettavat lait mukaan lukien luottamuksellisten tietojen salassapito ja vaitiolovelvollisuus. Varmistetaan, että salassapitovelvollisuus jatkuu sopimuksellisesti myös työsuhteen loppumisen jälkeen, vaikka voimassa olevissa laeissa (esimerkiksi *laki potilaan asemasta ja oikeuksista sekä laki sosiaalihuollon asiakkaan asemasta ja oikeuksista*) näin edellytettäisiinkin.
b) Kaikkia henkilöitä on velvoitettava tietoturvalliseen toimintaan sopimuksellisesti tarpeen ja voimassa olevan tietoturvapolitiikan mukaisesti. Kaikkien kanssa on syytä noudattaa samoja ehtoja.
c) Jos henkilö ei ole työntekijä eikä muussa sopimussuhteessa organisaation kanssa, on hänen kanssaan solmittava salassapitosopimus, jos hänellä on mahdollisuus päästä käsiksi arkaluonteisiin tietoihin.
d) Jos nähdään tarpeelliseksi, sopimuksissa mainitaan erikseen organisaatioon ja liiketoimintaan liittyvien tietojen suojaamisesta sekä henkilötietojen suojaamisesta.

e) Sopimuksissa mainitaan henkilön vastuista ja velvollisuuksista tietojen suojaamisessa hänen työskennellessään organisaation tilojen ulkopuolella, kuten kolmansien osapuolten (yhteistyökumppanit, alihankkijat, asiakkaat) tiloissa, etätöissä tai työmatkoilla.
f) Velvollisuudet erilaisten työvälineiden, esimerkiksi kannettavien tietokoneiden, matkaviestinten, julkisten tietoliikenneyhteyksien ja paperitulosteiden käytössä mainitaan sopimuksissa ja ohjeistetaan tarvittaessa erikseen.
g) Sopimuksissa mainitaan seuraamukset, jotka koituvat sopimuksenvastaisista ja tietoturvallisuutta vaarantavista toimista.
h) Sopimuksissa on mainittava, kuinka pitkään ehdot ovat voimassa vielä sopimuksen voimassaolon jälkeen.
i) Tarkemmat käytännön toimintaohjeet, omaisuuden ja tietojen käsittelysäännöt, työvälineiden käyttö ja hallinta sekä eettisesti noudatettavat toimintaperiaatteet kuvataan tyypillisesti erikseen ja henkilöiltä edellytetään näiden kuvausten ja ohjeiden noudattamista.
j) Jos jo olemassa olevissa sopimuksissa, esimerkiksi työsopimuksissa, ei ole riittäviä mainintoja tietoturvallisuudesta, organisaation henkilöt allekirjoittavat erillisen dokumentin, jossa allekirjoittajalta edellytetään tietoturvallista toimintaa ja tietoturvasta huolehtimista voimassa olevien käytäntöjen ja ohjeiden mukaisesti.
k) Niille henkilöille, jotka joutuvat työtehtäviensä puolesta sitoutumaan kolmansien osapuolten laatimiin salassapito- tai vaitioloehtoihin ja allekirjoittamaan vastaavia sitoumuksia, laaditaan ohjeistus tällaisissa tilanteissa toimimista ja allekirjoitettavan sopimuksen arviointia varten. On syytä välttää tilanteita, joissa työntekijä joutuu esimerkiksi henkilökohtaiseen oikeudelliseen vastuuseen tai suorittamaan henkilökohtaisia sanktioita tai korvauksia kolmannelle osapuolelle. Mahdolliset vastuut ja niiden rikkomisesta liittyvät sanktiot, korvaukset tai rangaistukset on syytä liittää työntekijän työ- tai virkatehtävän hoitoon.

## A4.3 Tietoturvavastuiden määrittäminen

### kontrolli

Kaikki tietoturvallisuuteen liittyvät vastuut on määritettävä voimassa olevan tietoturvapolitiikan ja noudatettavien periaatteiden mukaisesti. Organisaation kaikille henkilöille on määritettävä osaamistaso ja vastuut, jotka jokaisen tulee vähintäänkin hallita ja joita jokaisen tulee noudattaa. Jokainen on omalta osaltaan velvollinen huolehtimaan tietoturvallisuudesta ja raportoimaan havaitsemistaan tietoturvaloukkauksista. Vastuiden määrittäminen on ennen kaikkea johdon tehtävä.

### käytännön ohjeita

a) Organisaation kaikille työntekijöille ja tarvittaessa muille henkilöille, kuten kolmansien osapuolten työntekijöille, määritetään tietoturvallisuuteen ja turvalliseen toimintaan liittyvä osaamistaso, tiedot ja taidot, mitkä jokaisen henkilön täytyy vähintäänkin hallita.
b) Kaikille edellä mainituille työntekijöille määritetään tietoturvallisuuteen ja turvalliseen toimintaan liittyvät vastuut, joita jokaisen henkilön on noudatettava. Tyypillisesti jokaisen vastuuksi määritellään vähintäänkin noudattaa tietoturvapolitiikkaa ja ilmoittaa havaituista tietoturvarikkeistä.
c) Kaikki erityisvastuut, kuten vastuu omaisuuden, tietojen tai tietojärjestelmien hallinnasta tai ylläpidosta tai osallistuminen tietoturvatoimintaan, määritellään ja kuvataan erikseen.

## A4.4 Tietoturvavastuista tiedottaminen

### kontrolli

On huolehdittava, että kaikki henkilöt, sekä organisaatioon kuuluvat että ulkopuoliset, tietävät tietoturvallisuuteen liittyvät vastuunsa. Vastuista tiedottaminen on ennen kaikkea johdon tehtävä. Johdon on

kannustettava kaikkia huolehtimaan tietoturvallisuudesta, noudattamaan voimassa olevia käytäntöjä ja toimimaan kaikkien tietoturvallisuusohjeiden mukaisesti.

### käytännön ohjeita

Motivoitunut ja tietoinen organisaatio on luotettavampi ja aiheuttaa vähemmän tietoturvariskejä kuin motivoimaton ja/tai ymmärtämätön organisaatio. Organisaation motivointikeinoina toimivat ennen kaikkea ymmärrys ja tiedottaminen, palkitseminen sekä väärinkäytöksistä rankaiseminen. Nämä edellyttävät, että organisaation tietoturvatoimintaa mitataan. Tästä on mainittu tarkemmin luvuissa *toiminnan jatkuvuus ja poikkeustilanteet.* Tietoturvallisuuden laiminlyöntejä ja väärinkäytöksiä ehkäistään muun muassa seuraavassa mainittujen toimenpiteiden avulla.

a) Kaikki henkilöt sekä organisaatiossa että sen ulkopuolella tutustutetaan voimassa oleviin tietoturvallisuusperiaatteisiin ja -ohjeisiin.
b) Kaikki henkilöt vastuutetaan huolehtimaan tietoturvasta tehtäviensä mukaisesti ja tutustutetaan henkilökohtaisiin tietoturvasta huolehtimisen ja tietojen suojaamisen vastuisiinsa.
c) Henkilöt ovat tietoisia ja ymmärtävät itselleen määritetyn tietoturvatietämyksen ja -osaamisen tason.
d) Kaikille henkilöille jaetaan tietoturvapolitiikka, tietosuojapolitiikka, tietoturvakäsikirja sekä muu tarvittava tietoturvaohjeistus. Henkilöt allekirjoittavat todistuksen asiakirjojen vastaanottamisesta.
e) Henkilöille ei myönnetä pääsyvaltuuksia arkaluonteisiin tietoihin tai niitä sisältäviin tietojärjestelmiin ennen kuin tietoturvaan liittyvät vastuut ja ohjeet ovat henkilön tiedossa ja omaksumia.
f) Henkilöt motivoidaan noudattamaan organisaation tietoturvakäytäntöjä ja -ohjeistusta.

## A4.5 Tietoturvatietoisuus, -osaaminen ja -koulutus

### kontrolli

Tietoturvakoulutus- ja tiedotustilaisuuksia on järjestettävä säännöllisesti. Kaikkien organisaation työntekijöiden ja tarvittaessa kolmansien osapuolten henkilöiden on osallistuttava koulutukseen niin, että jokainen saavuttaa omaan tehtäväkuvaansa tarvittavan tietoturvatietoisuuden tason. Kaikkien on myös osallistuttava säännöllisesti pidettäviin tiedotus- tai tietoiskutilaisuuksiin tietoturvaan liittyvistä päivityksistä ja muutoksista.

### käytännön ohjeita

a) Tietoturvakoulutustilaisuuksia järjestetään säännöllisesti. Koulutustilaisuuksissa esitellään vähintäänkin ne tiedot ja taidot, vaatimukset, vastuut, toiminta ja tietoturvallisuustaso, joita kaikilta organisaation henkilöiltä edellytetään. Tilaisuuksissa käsitellään tietoturvatoiminnan seuranta, mittaaminen, palkitseminen ja väärinkäytöksistä rankaiseminen. Koulutuksissa kerrotaan myös tunnettujen uhkien havaitsemisesta ja annetaan toimintaohjeet ja yhteyshenkilöt tilanteisiin, kun henkilö havaitsee tietoturvaloukkauksen tai tarvitsee tietoturvaan liittyviä lisätietoja.
b) Tietoturvasta kouluttamisen prosessi määritellään ja kuvataan. Prosessi on osa organisaation säännöllistä toimintaa, ja sen toteutumista seurataan ja mitataan. Prosessin olemassaolo on tyypillisesti edellytys tietoturvallisen toiminnan sertifioimiselle.
c) Jokainen velvoitetaan osallistumaan tietoturvakoulutukseen. Osallistuminen kirjataan.
d) Henkilöille ei myönnetä pääsyvaltuuksia arkaluonteisiin tietoihin tai niitä sisältäviin tietojärjestelmiin ennen kuin henkilö on osallistunut tarvittaviin koulutustilaisuuksiin.
e) Tietoturvallisuuteen liittyvien olosuhteiden, menetelmien, periaatteiden tai ohjeiden muutoksista järjestetään tiedotustilaisuuksia aina tarvittaessa. Tilaisuudet voidaan järjestää jonkin muun, säännöllisen, tiedotustilaisuuden yhteyteen. Muutoksista kerrotaan tiedotustilaisuuksien lisäksi myös tarvittavilla muilla keinoilla, esimerkiksi paperi- ja sähköpostitiedotteilla.

## A4.6 Toiminta tietoturvaloukkauksissa

### kontrolli

Tietoturvaloukkauksien käsittelyyn täytyy olla määritelty prosessi, jonka on koskettava sekä organisaation työntekijöitä että ulkopuolisia henkilöitä. Ennalta määriteltyjen ja ohjeistettujen toimenpiteiden on katettava kurinpito ja väärinkäytöksistä rankaiseminen, tiedotus riittävällä laajuudella sekä palautuminen normaaliin, turvallisen toiminnan tilaan.

### käytännön ohjeita

Tietoturvaloukkausten havaitsemisesta ja toimenpiteistä esimerkiksi riittävän laajuiseen tiedotukseen ja normaaliin, turvallisen toiminnan tilaan palautumisesta on myöhemmin oma lukunsa *poikkeustilanteet*. Seuraavat ohjeet koskevat nimenomaan kurinpitotoimia ja väärinkäytöksistä rankaisemista. Niiden tarkoitus on sekä ennaltaehkäistä turvaloukkauksia että ojentaa loukkauksia aiheuttaneita ja tietoja väärinkäyttäneitä henkilöitä. Turvaloukkaukset voivat olla tahallisia tai tahattomia, mikä on otettava huomioon myös kurinpitotoimia määritettäessä.

a) Tietoturvaloukkausten havaitsemiseen, raportoimiseen ja käsittelyyn on määritelty prosessit. Ne sisältävät sekä automaattiset mekanismit uhkien ja loukkausten havainnoimiseksi että yksittäisten henkilöiden raportoimismekanismit havaitsemistaan turvaloukkaustilanteista. Tämä koskee myös sosiaali- ja terveydenhuollon asiakkaan tai potilaan raportoimia tietoturvaloukkauksia.
b) Mahdollisuuksien mukaan kaikkien merkityksellisten uhkien toteutuminen liitetään automaattisen tarkkailun piiriin.
c) Havaituista uhkista opitaan: sekä omaan organisaatioon kohdistuneet että muualla esiintyneet uhkat arvioidaan ja liitetään tarkkailtaviksi.
d) Havaitut turvaloukkaukset käynnistävät aina loukkausten käsittelyprosessin. Prosessin kulku on määritelty etukäteen. Kaikissa loukkaustilanteissa noudatetaan järjestelmällisesti samaa prosessia.
e) Ennen mahdollisia kurinpitotoimia varmistetaan aina turvaloukkaushavainnon aitous ja totuuden mukaisuus.
f) Kurinpitotoimet ovat yhtäläisiä, samanarvoisia ja oikeudenmukaisesti tasapuolisia kaikille.
g) Kurinpitotoimia määritettäessä otetaan huomioon loukkauksen vakavuus ja seuraukset, oikeudelliset vaikutukset, tahallisuus, toistuminen, loukkauksen tehneen henkilön tietoturvavastuut ja oikeantasoinen koulutus sekä mahdollisuus estää tapahtunut turvaloukkaustilanne. Myös rankaisun laillisuus, mahdollinen vaikutus voimassa oleviin sopimuksiin ja muut tarvittavat tekijät huomioidaan. Pienissä rikkeissä voidaan myös olla ryhtymättä kurinpitotoimiin.
h) Kurinpitotoimien tiedottaminen on määritelty loukkausten käsittelyprosessiin. Loukkauksista ja kurinpitotoimista tiedotetaan sovitun käytännön mukaisesti.

## A4.7 Toimenpiteet työsuhteen loppuessa

### kontrolli

Kun työntekijän työsuhde lopetetaan tai kolmannen osapuolen työntekijän toiminta organisaatiossa loppuu, on henkilölle annetut valtuudet ja pääsyoikeudet lakkautettava ja hänen hallussaan oleva organisaatiolle kuuluva omaisuus palautettava.

a) Vastuut ja toimintatavat tilanteisiin, kun henkilön toiminta organisaatiossa loppuu, määritellään selkeästi. Prosessissa on määritelty, miten varmistetaan kaiken omaisuuden siirtyminen. Tähän tarkoitukseen voidaan käyttää esimerkiksi erillistä tarkastuslistaa tai luetteloa.

b) Henkilölle tiedotetaan kaikista häneen kohdistuvista velvollisuuksista ja vastuista työsuhteen loppumisen yhteydessä. Myös häneen kohdistuvista työsuhteen loppumisen jälkeisistä velvollisuuksista tiedotetaan. Esimerkiksi salassapito ja vaitiolo voivat olla tällaisia velvollisuuksia.

c) Henkilö palauttaa kaiken hallussaan olevan organisaation omaisuuden. Tällaista omaisuutta ovat kaikki työvälineet: tietokoneet, matkapuhelimet ja muut laitteet, ohjelmistot, käyttöohjeet, avaimet, kulku-, äly- ja luottokortit sekä sähköisessä muodossa oleva organisaatiolle kuuluva tieto-omaisuus. Myös organisaation vaatteet, kulkuvälineet ja vastaavat tarvikkeet palautetaan.

d) Jos työsuhteen loppumisen yhteydessä henkilön haltuun sovitaan jäävän organisaation omaisuutta (esimerkiksi matkapuhelin), kaikki tällainen omaisuus kirjataan.

e) Henkilön kaikki kulku- ja pääsyoikeudet sekä valtuudet lakkautetaan työsopimuksen loppuessa. Oikeuksien ja valtuuksien lakkauttaminen saattaa olla välttämätöntä jo irtisanomishetkellä.

f) Henkilön tiedot poistetaan kaikista asiakirjoista, joissa henkilö on mainittu organisaatioon kuuluvaksi.

g) Henkilön työsuhteen loppumisesta tiedotetaan kaikille tarvittaville tahoille, jos tämä nähdään tarpeelliseksi.

h) Jos on tarpeellista, työsuhteen loppuessa tehdään erillinen riskien kartoitus, jossa arvioidaan henkilön mahdollisuus päästä käsiksi tietoihin ja tietojärjestelmiin työsuhteen loppumisesta huolimatta sekä motiivi tällaisen tietoturvaloukkauksen yrittämisestä. Riskiä voivat lisätä irtisanominen työnantajan toimesta, henkilökohtaiset huonot suhteet johtoon ja esimieheen tai henkilön työnsä puolesta käsittelemien tietojen arvo.

i) Varmistetaan, että henkilöllä ei ole mahdollisuutta kopioida organisaation tietoja itselleen. Tällaisia tietoja ovat tyypillisesti esimerkiksi asiakasrekisterin tiedot.

j) Varmistetaan, että avainhenkilön työsuhteen loppuessa kaikki organisaatiolle tarpeellinen tieto on siirretty jollekin toiselle henkilölle.

# 7 Fyysisen ympäristön turvallisuus

## 7.1 Yleistä

Fyysisen ympäristön suojauksella käsitetään sekä organisaation tuotanto- ja toimitilojen että siellä sijaitsevien tietojenkäsittelylaitteiden fyysistä suojaamista. Tällä ehkäistään niiden riskien ja vahinkojen toteutumista, jotka aiheutuvat joko valtuudettomasta fyysisestä pääsystä organisaation tiloihin, tietoihin ja tietojärjestelmiin tai fyysisestä ympäristöstä (kuten virransyöttö tai jäähdytys). Fyysisen ympäristön suojaus koostuu kiinteistöjen ja tilojen suojauksesta rakenteellisesti, kulunvalvonnan osalta, teknisestä valvonnasta ja vartioinnista, erilaisten palo-, vesi-, sähkö-, murto- ja muiden vahinkojen sekä ihmisten virheellisestä toiminnasta johtuvien vahinkojen torjunnasta. Tärkeät tiedot ja tietojärjestelmät on säilytettävä tietojen kriittisyyden huomioon ottavissa ja säilytystarkoitukseen soveltuvissa turvallisissa tiloissa.

Tyypillisiä uhkia ovat puutteellisista määrityksistä tai puutteellisesta toiminnasta ja ohjeistuksesta johtuvat uhkat. Tilojen suojauksessa kiinnitetään erityistä huomiota sisään- ja uloskäyntien, lastausalueiden ja niiden tilojen suojaukseen, joihin kolmansille osapuolille on myönnetty kulkuoikeuksia. Kaikessa suojauksessa noudatetaan valittuja henkilöiden todennusmenettelyitä ja kulunvalvontaa. Tietojärjestelmien ohella suojataan myös esimerkiksi laitetilat ja tietoliikennekaapelit. Jotta arkaluonteiset tiedot eivät olisi saatavilla ilman asianmukaisia valtuuksia organisaation sisällä tai kolmansille osapuolille, on luotava käytännöt toimitilojen, toimistotilojen ja työhuoneiden suojaamiseksi ja erityiset ohjeet näyttöpäätteillä, työpöydillä ja jaetuissa tulostimissa ja telefax-laitteissa näkyvien tietojen suojaamiseksi. Toimitilojen suojaamisessa täytyy erityistä huomiota kiinnittää tiloihin, joissa käsitellään asiakas- ja potilastietoja ja joissa voi oleilla potilaita, asiakkaita, heidän omaisiaan tai ulkopuolisia henkilöitä. Tällaisia tiloja ovat esimerkiksi kaikki vastaanotto- ja odotustilat, hoito- ja toimenpidetilat ja -huoneet sekä osastot.

Organisaation tilojen ulkopuolella sijaitsevien tietojen ja tietojärjestelmien suojaamisesta täytyy huolehtia asianmukaisesti. Näitä ovat sekä kolmansien osapuolten hallussa olevat järjestelmät (kuten ulkoistetut ja huollossa olevat) että organisaation henkilöiden hallussa olevat laitteet (kuten kotitietokoneet, kannettavat tietokoneet, mukana kuljetettavat paperit ja muut dokumentit, USB-avaimet ja matkaviestimet). Omaisuuden viemiseen organisaation tilojen ulkopuolelle on oltava valtuutusmenettely. On varmistuttava, että käytöstä poistettaviin tietojärjestelmiin, esimerkiksi kovalevyille, ei jää tietoja ulkopuolisten saataville.

Kaikkia niitä organisaation tiloja tai organisaation ulkopuolisia tiloja, jotka ovat joko fyysisesti suojattuja tai fyysistä suojausta edellyttäviä ja joissa voi sijaita tai käsitellään esimerkiksi arkaluonteisia tietoja, kutsutaan myöhemmin turvatiloiksi. Turvatilat voivat olla luokiteltuja esimerkiksi sen mukaan, millaisia ja kuinka arkaluonteisia tietoja siellä säilytetään. Esimerkiksi tietokone- ja tietoliikennelaitteille varattuja huoneita ja konesaleja voidaan kutsua korkean turvallisuuden tiloiksi.

## 7.2 Uhkista ja riskeistä

Fyysisen ympäristön turvallisuus muodostaa organisaation turvalliselle toiminnalle ja tietoturvalle erittäin tärkeän kokonaisuuden. Siihen kohdistuu lukuisia uhkia, joista alla on mainittu muutamia esimerkkejä.

a) Kiinteistö tai toimitilat ovat alttiita onnettomuuksille (sijaitsevat esimerkiksi vilkkaasti liikennöityjen teiden tai lentoasemien läheisyydessä).
b) Turvarakenteet eivät ole riittävän vahvat tai niissä on aukkoja.
c) Tiloissa säilytetään sinne kuulumatonta materiaalia tai tavaraa.
d) Varmistusnauhoja varten ei ole erillisiä säilytystiloja.
e) Ulkopuolisia henkilöitä pääsee organisaation tiloihin vastaanottotiskin ja turvatarkastuksen ohi.
f) Tiloissa vierailevien henkilöiden taustoja ei selvitetä riittävän tarkasti.

g) Ovia ei pidetä lukittuna.
h) Kiinteistössä ei ole kulunvalvontaa tai vartiointia tai ne eivät ole riittäviä.
i) Samassa kiinteistössä olevien muiden organisaatioiden henkilöillä on pääsy heille kuulumattomiin tiloihin.
j) Tiloissa kulkevilla henkilöillä ei ole näkyviä tunnisteita, kuuluuko henkilö joko organisaatioon tai onko hän vierailija.
k) Neuvottelutilat eivät ole ääni- ja näköeristettyjä.
l) Arkaluonteisia tietoja jätetään neuvottelutiloihin vartioimatta.
m) Vierailijoilla ei ole saattajaa.
n) Korkean turvallisuuden tiloissa asioinnista ei kirjata asianmukaista merkintää tapahtumalokiin.
o) Ohikulkija näkee hänelle kuulumatonta tietoa työpöydällä, näyttöpäätteellä tai kuulee tietoja kuulemassaan puhelinkeskustelussa.
p) Työpöytiin kiinnittämättömiä kannettavia tietokoneita varastetaan.
q) Henkilöiden työasemiin leviää haittaohjelmia esimerkiksi selainkäytön tai sähköpostin välityksellä.
r) Työasemiin on asennettu luvattomia ohjelmistoja tai ohjelmistoja ilman asianmukaisia käyttöoikeuksia.
s) Sivullisilla on mahdollisuus lukea tulosteita, telefaxeja tai saapuvaa postia.
t) Luottamuksellisia tietoja sisältäviä papereita tai erilaisia tietovälineitä ei hävitetä asianmukaisesti.
u) Organisaation omaisuutta anastetaan lastausalueelta.
v) Laitteisto vikaantuu puutteellisen puhdistuksen takia.
w) Tietojärjestelmä vahingoittuu kuljetettaessa huoltoon.
x) Huoltohenkilö näkee hänelle kuulumatonta tietoa huollon yhteydessä.
y) Tietojärjestelmiä on sijoitettu tiloihin, joissa niihin kohdistuu ulkoisia rasitteita, kuten kosteutta, lämpöä tai pölyä.
z) Henkilöt vievät tietoja organisaation tilojen ulkopuolelle ilman asianmukaista lupaa, tarkoituksella tai vahingossa.
å) Henkilö ei huolehdi avaimistaan ja kulkukorteistaan.
ä) Kannettava tietokone tai muita tietoja varastetaan työmatkalla.
ö) Kannettavassa tietokoneessa olevat tiedot menetetään rikkoutumisen takia.
aa) Kotitietokoneelta leviää haittaohjelmia organisaation tietojärjestelmiin.
bb) Tietojärjestelmä vaurioituu sähkökatkoksen, ukonilman tai ylivirtapiikin yhteydessä.
cc) Tietojärjestelmä vaurioituu tulipalon tai vesivahingon takia.
dd) Varavoimajärjestelmä ei toimi.
ee) Tietojärjestelmä vioittuu ylikuumenemisen seurauksena.
ff) Tietoliikennettä salakuunnellaan.
gg) Tietoliikennekaapeleihin kohdistetaan ilkivaltaa.
hh) Tietoliikenneyhteydet katkeavat ja varareititys ei toimi.
ii) Käytöstä poistettu kovalevy sisältää tietoa, joka ei ole tuhoutunut.

## A5.1 Tilojen rakenteet ja työskentelytilojen ympäristö

### kontrolli

Turvatilojen, siis niiden tilojen, joissa säilytetään tietoja ja tietojärjestelmiä, on oltava riittävän tukevia ja suojattuja estämään valtuudeton pääsy tietoihin. Tämä sisältää sekä seinä-, lattia- ja kattorakenteet, ovet ja muut sisäänkäynnit sekä ikkunat. Näistä käytetään jatkossa yhteisesti termiä 'turvarakenteet'.

a) Turvarakenteet sekä niillä suojatut alueet ja tilat on määritelty selkeästi.
b) Turvarakenteiden vahvuus – esimerkiksi seinien paksuus, ovien, porttien ja lukkojen vahvuus, valvonta ja miehitys, ikkunoiden ja kalterien lujuus sekä hälytysmekanismien käyttö – vastaa tiloissa sijaitsevien tietojen turvatasoa ja riskianalyysin tuloksia.
c) Turvarakenteissa ei ole aukkoja, jotka mahdollistavat murtautumisen tiloihin tai tiloissa sijaitsevien tietojen tai siellä tapahtuvan tietojenvälityksen salakuuntelun.
d) Rakennussuunnittelussa otetaan tarpeen mukaan huomioon esimerkiksi tulvat ja maanjäristykset.
e) Terveydelliset ja henkilöiden turvallisuuteen liittyvät seikat ja määräykset otetaan huomioon. Vaarallisten ja riskialttiiden materiaalien käyttöä vältetään. Myös ympäröivistä rakennuksista ja esimerkiksi liikenteestä mahdollisesti aiheutuvat ongelmat huomioidaan.
f) Tiloissa on helposti saatavilla tarvittavat pelastustarvikkeet ja -välineet. Pelastamis- ja pelastautumisohjeet on helposti saatavilla.
g) Tarvittaessa on käytössä kassakaappeja, laitteistokassakaappeja tai lukittavia laitetelineitä tietojen ja tietojärjestelmien säilytystä varten.
h) Korkean turvallisuuden tiloja ei käytetä varastona eikä siellä säilytetä esimerkiksi suuria määriä tulostuspaperia tai varmistusnauhoja.
i) Korkean turvallisuuden tilat eivät sijaitse julkisesti avoinna olevien ja julkisessa käytössä olevien tilojen välittömässä läheisyydessä.
j) Turvatiloja, erityisesti korkean turvallisuuden tiloja, ei ole merkitty siten ja ne eivät muuten näytä ulkoisesti siltä, että ulkopuoliselle selviää kyseessä olevan tietojenkäsittelyyn tarkoitetut ja mahdollisesti arkaluonteisia tietoja sisältävät tilat.
k) Miehitetty vastaanotto huolehtii ulkopuolisten henkilöiden tunnistamisesta, tiloihin pääsystä ja kulkuoikeuksien jakamisesta.
l) Kaikille ulkopuolisille jaettavat kulkuoikeudet myönnetään etukäteen tehtyjen sopimusten perusteella.
m) Seinät, lattiat ja katto on rakennusteknisesti sellaiset, että ne suojaavat murtautumisen lisäksi ympäristössä tapahtuvilta tuhoilta, kuten tulipaloilta tai vesivahingoilta. Tarvittavista automaattisista palonsammutuksista ja veden, savun, kemikaalien ja muiden aineiden poistosta on huolehdittu.
n) Lattiat ovat korotettuja aina tarvittaessa. Kaapeleita ja johtoja varten rakennetaan erilliset hyllystöt tai kourut korotettujen lattioiden alle, seiniin tai kattorakenteisiin. Korotettujen lattioiden alla on viemäröinti estämässä mahdollisen veden pääsyn kaapelikouruihin ja tietojärjestelmiin.
o) Vesi-, ilmastointi-, tuli- ja sähkönsyöttöongelmille on asennettu hälyttimet. Kaikkia paloovia pidetään suljettuina ja niihin on asennettu hälyttimet.
p) On huolehdittu, että varauloskäynneistä pääsee kaikissa tilanteissa ulos, mutta asiaton sisäänkäynti on estetty.
q) Ulkopuolisten tunkeutujien havaitsemiseksi tiloihin on asennettu esimerkiksi liikkeen- tai lämmöntunnistimet, ovien ja ikkunoiden avautumisen tunnistimet ja muut tarvittavat murtohälyttimet.
r) Miehittämättömien tilojen hälytyskontrollin täytyy tarvittaessa olla aina valmiudessa. Tämä koskee esimerkiksi tietokone-, tietoliikenne- ja muita laitehuoneita, joissa ei normaalitilanteessa ole miehitystä. Hälytys voidaan kytkeä pois päältä esimerkiksi henkilön kulkiessa sisään huoneeseen. Tiloissa käytetään esimerkiksi sähköistä kulunvalvontaa ja ovien lukitusta sekä videonauhoitusta.
s) Samassa kiinteistössä sijaitsevat oman organisaation käyttämät tilat on fyysisesti eristetty kolmansien osapuolten käyttämistä tiloista. Tarvittaessa tilojen välillä siirtymistä kontrolloidaan kulunvalvonnalla.
t) Kulkemista erilaisilla turvallisuustasoilla olevien alueiden välillä kontrolloidaan kulunvalvonnalla.

u) Vastaanottotiskin ja niihin liittyvien turvatilojen (esimerkiksi tilojen, joissa myönnetään ulkopuolisille kulkuluvat tai -kortit) turvallisuuteen kiinnitetään erityinen huomio. Tiloja, joiden on tarkoitus olla miehitettyjä, ei saa koskaan jättää tyhjäksi ja ilman miehitystä niin, että sovittua minimihenkilöstöä ei ole paikalla.

## A5.2 Kulunvalvonta

### kontrolli

Kaikki turvatilat on suojattava riittävin kulunvalvontakontrollein.

On huomattava, että fyysistä kulunvalvontaa vastaavat mekanismit on syytä ottaa käyttöön myös kaikkeen pääsyyn sähköisessä muodossa oleviin tietoihin. Tämä koskee sekä oikeuksien määrittelyä että tapahtumien kirjausta. Nämä on kuvattu tarkemmin luvussa *pääsynhallinta*.

### käytännön ohjeita

a) Kaikille tiloissa liikkuville henkilöille on määritelty tarpeelliset kulkuoikeudet. Valtuudettomilla henkilöillä ei ole mitään pääsyä turvatiloihin ilman saattajan läsnäoloa.
b) Kaikkia kolmansia osapuolia ja vierailijoita varten on olemassa menetelmä henkilön tunnistamiseen ja kulkuoikeuksien myöntämiseen. Oikeudet myönnetään vain määrättyä ja etukäteen määriteltyä tarkoitusta varten.
c) Kulkuoikeuksien myöntämisen yhteydessä tarkistetaan henkilöllisyys ja kirjataan sen lisäksi tulo- ja lähtöajat sekä myönnetyt oikeudet. Tarvittaessa henkilö valokuvataan ja häneltä voidaan edellyttää pantin jättämistä vastaanottotiskille.
d) Vierailijoille jaetaan tarvittaessa ohjeet ja säännöt tiloissa liikkumiselle.
e) Vierailijoille nimetään ja osoitetaan saattaja aina tarpeen mukaan, esimerkiksi liikuttaessa organisaation toimistotiloissa, jossa voi olla näkyvillä luottamuksellisia tietoja.
f) Korkean turvallisuuden tiloihin ei myönnetä mitään kulkuoikeuksia valtuudettomille henkilöille.
g) Korkean turvallisuuden tiloissa liikuttaessa käytetään mahdollisuuksien mukaan aina henkilön sähköistä tunnistamista esimerkiksi kulkukortilta, sisäänpääsyyn oikeuttavaa PIN-koodia ja ovien sähköistä lukitusta. Kaikesta liikkumisesta jää tieto tapahtumalokiin ja mahdollisesti videovalvontaan.
h) Henkilöstö käyttää aina organisaation tiloissa liikkuessaan näkyvää tunnistetta.
i) Vierailijoilla on aina näkyvillä tunniste, joka osoittaa henkilön olevan vierailija tai ulkopuolinen.
j) Organisaation jokaisen henkilön vastuu on saattaa turvatiloissa liikkuva ilman tunnistetta oleva henkilö vastaanottotiskille.
k) Kolmannen osapuolen henkilöstölle, esimerkiksi asiantuntija- tai huoltohenkilöstölle, voidaan tarvittaessa myöntää rajoitettu pääsy korkean turvallisuuden tiloihin. Jos mahdollista, tällöin on mukana aina saattaja organisaation toimesta.
l) Korkean turvallisuuden tiloihin oikeuttavat kulkuoikeudet tarkastetaan ja päivitetään ajantasaisiksi määräajoin.

## A5.3 Toimistotilojen ja työhuoneiden suojaus

### kontrolli

Sen lisäksi, että toimistotilat täytyy suojata riittävin keinoin henkilöihin kohdistuvilta uhkilta, täytyy niissä oleva tieto suojata ulkopuolisten pääsyltä. Tiloissa vierailevan ulkopuolisen tahon ei tule saada mahdollisuutta päästä käsiksi, nähdä tai kuulla mitään hänelle kuulumatonta tietoa. Suojattaviksi tiloiksi on luettava esimerkiksi lääkäreiden työhuoneet ja niiden lisäksi kaikki sellaiset tilat, joissa käsitellään tai säilytetään potilastietoja ja joihin voi päästä potilaita, heidän omaisiaan tai muita ulkopuolisia henkilöitä.

Tällaisia tiloja voivat olla esimerkiksi hoito- ja toimenpidehuoneet ja osastot. Näihin on syytä noudattaa alla olevaa ohjeistusta sopivasti soveltaen.

## käytännön ohjeita

a) Työhuoneet ovat lukittavia. Työhuoneet pyritään pitämään lukittuina aina työajan ulkopuolella.
b) Sisäiset puhelinluettelot, organisaatiokaaviot ja muut organisaatiota koskevat dokumentit, joita ei ole tarkoitettu ulkopuoliseen jakeluun, säilytetään asianmukaisesti.
c) Paperit ja vastaavat tietovälineet (levykkeet, cd-levyt, nauhat, USB-avaimet) säilytetään ja tuhotaan asianmukaisesti. Säilytystila on tarvittaessa lukollinen. Kriittisen tiedon säilytystila voi olla erityissuojattu, esimerkiksi kassakaappi.
d) Työpöydän puhtaudesta, kaikkien työpöydillä näkyvissä olevien paperien ja tietovälineiden säilytyksestä on toimiva käytäntö ja ohjeet, *"clean desk policy"*.
e) Näyttöpäätteen puhtaudesta, kaikkien tietojenkäsittelylaitteilla ja näyttöpäätteillä olevan tiedon näkymisestä on toimiva käytäntö ja ohjeet, "*clear screen policy*".
f) Keskusteltaessa tiloissa, joissa on läsnä asiaankuulumattomia henkilöitä, varmistutaan siitä, etteivät asiaankuulumattomat henkilöt kuule keskusteluiden sisältöä.
g) Varotaan myös puhelinkeskustelujen kuulumista asiattomille. Puhelinvastaajaan ei jätetä arkaluonteisia tietoja sisältäviä viestejä.
h) Neuvottelu- ja kokoustilat ovat näkö- ja äänieristettyjä. Kokoustiloihin ei jätetä suojattavia tietoja vartioimatta. Neuvotteluissa syntyvää suojattavaa materiaalia (esimerkiksi kalvot, paperit ja taulupiirrokset) ei jätetä neuvottelutiloihin, vaan ne pyyhitään tai tuhotaan.
i) Henkilökohtaisia tietokoneita ei jätetä poistuttaessa lukitsemattomaan tilaan. Huolimattomuudesta koituvien vahinkojen estämiseksi on käytössä työaseman automaattinen lukitus ja näytönsäästäjä.
j) Jos tietokoneen käyttöön tarvitaan toimikorttia, korttia ei saa jättää toimikortinlukijaan poistuttaessa työpisteestä.
k) Tietokonelaitteisto voi tarvittaessa olla lukittavissa kiinni työpöytään.
l) Kovalevyn salausohjelmia käytetään tarpeen mukaan.
m) Työasemissa käytetään virustorjuntaa ja palomuuriohjelmistoja.
n) Työasemiin ei asenneta ulkopuolisia ohjelmistoja.
o) Sähköpostin käytöstä ja liitetiedostojen avaamisesta, Internet-käytöstä ja sallituista tai kielletyistä verkkosivustoista on olemassa säännöt, joita noudatetaan.
p) Sähköpostin lisäksi myös muiden yhteydenpitoon tarkoitettujen ohjelmistojen (esimerkiksi pikaviestintä, *instant messaging*) käytöstä on olemassa säännöt ja ohjeet, joita noudatetaan.
q) Tulostukset jaettuihin tulostimiin ja saapuva telefax-liikenne suojataan. Arkaluonteisten tietojen tulostukset noudetaan jaetuilta tulostimilta välittömästi tulostamisen jälkeen.
r) Organisaatioon tuleva posti ja muut lähetykset suojataan asianmukaisesti.
s) Mikäli tarpeellista, kopiokoneiden ja skannerien käyttöä valvotaan ja käyttö kirjataan. Tarvittaessa työajan ulkopuolinen käyttö estetään mahdollisen valtuudettoman kopioinnin estämiseksi.
t) Luottamuksellisia ja arkaluonteisia tietoja sisältäviä papereita ja tietovälineitä varten on olemassa erillinen lukittava roskakori ja tuhottavien tietovälineiden säilö. Roskakori ja säilö on merkitty asianmukaisin merkinnöin ja siitä on tiedotettu. Roskakorin ja säilön tyhjennykseen on luotu tietoturvallinen prosessi.
u) Tietojen käsittelyyn käytetään vain siihen tarkoitukseen tarkoitettuja tietojärjestelmiä, välineitä ja ohjelmistoja. Esimerkiksi potilastietojen käsittelyyn on syytä käyttää vain siihen tarkoitukseen varattuja työasemia.
v) Tietojärjestelmiä käytetään vain siihen tarkoitukseen, mihin ne on suunniteltu. Esimerkiksi potilastietojen käsittelyyn tarkoitettuja työasemia ei ole syytä käyttää sähköposti- tai selainkäytössä.

## A5.4 Työskentely korkean turvallisuuden tiloissa

### kontrolli

Korkean turvallisuuden tilat ja niissä työskentely täytyy suojata erityisellä huolellisuudella.

### käytännön ohjeita

a) Henkilöt saavat olla tietoisia korkean turvallisuuden tiloista, niissä työskentelystä ja niissä säilytettävistä tiedoista ainoastaan tarpeen mukaan.
b) Kaikkea tiloissa työskentelyä ja olosuhteita valvotaan ja tapahtumat kirjataan.
c) Miehittämättömät tilat ovat lukittuja ja jatkuvassa tai säännöllisessä valvonnassa.
d) Valokuvaus, nauhoitus tai muunlainen tallennus tiloissa on kiellettyä, ellei sitä ole nimenomaisesti valtuutettu.

## A5.5 Lastaus- ja purkualueet

### kontrolli

Lastaus- ja purkualueet on mahdollisuuksien mukaan oltava kontrolloituja. Ulkopuolisilla ei ole syytä päästä mainituille alueille ilman asianmukaista kulkulupaa.

### käytännön ohjeita

a) Pääsy lastaus- ja purkualueille on kulunvalvonnan piirissä.
b) Kaikilta alueilla asioivilta henkilöiltä tarkastetaan kulkuluvat. Kaikki kulku alueille rekisteröidään.
c) Alueilta ei ole suoraa kulkua organisaation muihin tiloihin.
d) Alueelle tehtävät toimitukset kirjataan.
e) Alueille toimitettavat tietojärjestelmät noudetaan organisaation tiloihin mahdollisimman nopeasti toimituksen jälkeen.
f) Kaikki toimitettavat tietojärjestelmät tarkastetaan. Ulkoinen tarkastus tehdään mahdollisuuksien mukaan lastausalueella ja tarkempi tarkastus organisaation tiloissa.
g) Uloimman portin, oven tai vastaavan on oltava suljettuna sen ajan, kun alueelta siirretään materiaalia organisaation tiloihin ja pääsy niihin lastausalueelta on mahdollista.

## A5.6 Laitteistojen huolto

### kontrolli

Huolletaan ja suojataan laitteistot huollon ajaksi asianmukaisesti. Huollon tarpeessa olevien, huollettavien tai huoltoon kuljetettavien laitteiden sisältämien tietojen tuhoutuminen, vahingoittuminen ja valtuudeton pääsy niihin on estettävä.

### käytännön ohjeita

a) Laitteita hoidetaan ja puhdistetaan säännöllisesti.
b) Laitehuollossa, sekä suoritettavissa toimenpiteissä että huoltoväleissä, noudatetaan valmistajien suosituksia.
c) Laitteiden puhdistus ja huolto tehdään vain siihen tarkoitukseen koulutettujen henkilöiden toimesta. Huoltohenkilökunnalle myönnetään kulkuoikeudet aina ja vain tarvittaessa.
d) Erityistä varovaisuutta noudatetaan, kun laitteita joudutaan huoltamaan ja lähettämään tai kuljettamaan huollettavaksi organisaation tilojen ulkopuolelle. Tällöin on kiinnitettävä huomiota sekä kuljetuksenaikaiseen suojaan (erilaiset fyysiset vahingot, tärinä, varkaudet, ja tapaturmat) sekä tietoihin pääsyn estämiseen valtuudettoman huoltohenkilökunnan tai muiden

henkilöiden toimesta. Tarvittaessa tiedot muistista ja kovalevyiltä kopioidaan muulle tietovälineelle, poistetaan kokonaan levyltä ja palautetaan levylle vasta huollon päätyttyä.

e) Jos huoltotoimiin käytetään ulkopuolista tahoa, varmistutaan kyseisen organisaation luotettavuudesta ja maineesta. Ulkopuolinen taho velvoitetaan sopimuksellisesti riittävään salassapito- ja vaitiolovelvoitteeseen mahdollisesti huollon aikana tai muuten saamistaan tiedoista.

## A5.7 Laitteistojen sijoitus ja suojaus organisaation tiloissa

### kontrolli

Suojataan laitteistot asianmukaisesti siten, että estetään mahdollisuudet niiden varastamiseen tai vahingoittamiseen sekä niiden vahingoittumiseen ympäristöstä johtuvista tekijöistä. Sijoituksessa kiinnitetään huomiota siihen, että valtuudeton tietoihin pääsy estyy kaikissa tilanteissa, myös korjaus- ja huoltotoimien yhteydessä.

### käytännön ohjeita

a) Laitteistot sijoitetaan niiden suojaustasoa ja niissä olevien tietojen kriittisyyttä vastaaviin tiloihin.

b) Laitteistokomponentit on tarpeen mukaan kahdennettu.

c) Palvelin- ja tietoliikennelaitteistot pyritään sijoittamaan siten, että samoissa tiloissa on mahdollisimman vähän päivittäistä työskentelyä.

d) Varmistusnauhat säilytetään tietojärjestelmistä erillisissä tiloissa. Varmistusnauhojen toimintaa testataan säännöllisesti.

e) Erityistä varovaisuutta ja suojaa vaativat laitteet eristetään muista laitteista. Tarvittaessa näissä laitetiloissa käynnistä tehdään kirjaus, joka voidaan esimerkiksi allekirjoittaa henkilökohtaisesti.

f) Varkauksien estämiseksi käytetään asianmukaisia hälyttimiä ja fyysisiä suojauksia, kuten laitteistojen kiinnittämistä vaijerein seiniin tai laitteistokaappeihin tai laitteistokaappien lukitsemista.

g) Ympäristön aiheuttamat ja muut ulkopuoliset fyysiset vahingot pyritään minimoimaan ja niiden torjuntaan varaudutaan etukäteen. Hälyttimiä käytetään mahdollisuuksien mukaan. Huomioon otetaan esimerkiksi tulipalot, räjähdysvaara, ukonilmat, haitalliset kaasut ja savu, kosteus, vesi ja jäähdytinnesteet, pöly, tärinä, erilaiset kemialliset aineet ja sammutusaineet, sähkövirta ja oikosulut, säteily ja EMP (sähkömagneettinen pulssi, *electromagnetic pulse*) sekä tahallinen vahingoittaminen ja terrorismi.

h) Tiloissa, joissa on runsaasti haitta-aineita (esimerkiksi pöly teollisuushalleissa), käytetään erilaisia suojia (kuten näppäinsuojat ja suodattimet laitekaapeissa).

i) Ruokailu, tupakointi ja muut vastaavat toimet on kielletty korkean turvallisuuden tiloissa tai niiden yhteydessä ja välittömässä läheisyydessä sekä muuallakin aina, kun se on turvallisuuden kannalta tarpeellista.

j) Ympäristön ja muiden ulkoisten tekijöiden aiheuttamat ongelmat ja viat kirjataan tapahtumalokiin.

## A5.8 Suojaus organisaation tilojen ulkopuolella

### kontrolli

Organisaation ulkopuolella sijaitsevien tietojen ja tietojärjestelmien suojauksesta on huolehdittava vastaavalla tavalla kuin huolehditaan organisaation tiloissa olevasta suojauksesta. Työskentelytavat on mukautettava ulkopuolisiin olosuhteisiin. On kiinnitettävä erityistä huomiota kannettavan tietokoneen käyttöön, säilytykseen ja tietojen suojaamiseen, mukana kuljetettavien paperitulosteiden säilytykseen ja

kommunikointiin esimerkiksi matkapuhelimella. Organisaation ulkopuolisissa tiloissa huollettavien laitteiden suojauksesta on mainittu kappaleessa *laitteistojen huolto*.

### käytännön ohjeita

a) Tietojen ja tietojärjestelmien vientiin organisaation ulkopuolelle on aina oltava valtuutus. Tähän valtuutetut henkilöt on selkeästi tunnistettava.
b) Ulkopuolisiin tiloihin tapahtuva laitteiden vienti ja tuonti on kirjattava, mikäli tarpeellista ja mahdollista.
c) Ulkopuolisissa tiloissa olevia laitteita varten tehdään yllätystarkastuksia, joiden mahdollisuus on tiedossa.
d) Jos tietojärjestelmiä, tietoja tai tietovälineitä viedään organisaation tilojen ulkopuolelle (tai yleensäkin niiden suojaustason edellyttämää heikommalle alueelle, vaikka väliaikaisesti), niitä ei jätetä yksin vartioimattomaan tilaan.
e) Tietojen viemisestä organisaation ulkopuolelle on laadittu erillinen opas, jossa on lueteltu noudatettavat ja hyväksytyt toimenpiteet esimerkiksi matkustukseen ja etätyöskentelyyn liittyen.
f) Organisaation ulkopuolelle vietävät tiedot on mahdollisuuksien mukaan tallennettava ja niitä on säilytettävä salakirjoitettuna. Kannettavan tietokoneen käyttö on oltava suojattu salasanalla.
g) Matkustettaessa kannettavat tietokoneet ja kaikki arkaluonteinen materiaali kuljetetaan käsimatkatavarana.
h) Jos esimerkiksi kannettavaa tietokonetta joudutaan säilyttämään hotelleissa tai erilaisissa kongressitiloissa, suojaukseen kiinnitetään erityistä huomiota.
i) Kannettavat tietokoneet ja arkaluonteisia tietoja sisältävä materiaali naamioidaan mahdollisuuksien mukaan, jotta se ei herätä huomiota ja kiinnostusta.
j) Käytettävät etäyhteydet ja ulkoiset yhteydet organisaation verkosta on suojattu asianmukaisesti.
k) Etätyöskentelyssä esimerkiksi kotona on noudatettava varovaisuutta. On tarvittaessa käytettävä lukittavia säilytystiloja, suojattua pääsyä tietokoneelle ja turvallisia tietoliikenneyhteyksiä. On kiinnitettävä erityistä huomiota sekä salakuuntelumahdollisuuteen että erilaisten haittaohjelmien leviämiseen, jos samaa tietokonetta käytetään sekä työ- että kotiasioiden hoitoon. Tämän ei pääsääntöisesti pidä olla sallittua.
l) Etätyöskentelyssä ja matkustettaessa on noudatettava tarkasti sekä työpöydän että näyttöpäätteen puhtaudesta. On varottava mahdollisuutta keskustelujen salakuunteluun esimerkiksi matkapuhelimen käytön yhteydessä ja yleensäkin kommunikoitaessa julkisissa tiloissa.
m) Organisaation ulkopuolella käytävissä neuvotteluissa ja kokouksissa syntyvä suojattava materiaali (esimerkiksi fläppitaulupaperit, piirrokset, kalvot) tuhotaan tai otetaan mukaan tuhottavaksi myöhemmin.
n) Jos on tarpeellista, organisaation ulkopuolella sijaitsevat tietojärjestelmät on vakuutettava erikseen.

## A5.9 LVIS ja ympäristö

### kontrolli

Laitteistot, tilat ja toiminta on suojattava sähkökatkoilta, ylikuumenemiselta, tulipaloilta, vesivahingoilta ja muilta vastaavilta tapahtumilta.

### käytännön ohjeita

a) Tilojen virransyöttö on asianmukaisesti suunniteltu ja toteutettu. Sähkövirtaa on käytettävissä riittävästi ja sen keskeytyminen on suojattu akuilla ja varavoimageneraattoreilla (*UPS, uninterruptable power supply*).

b) Sähkökatkostilanteita harjoitellaan. Akkujen ja generaattorien toimintakykyä ja kestoa testataan säännöllisesti.
c) Sähkökatkoja varten tiloissa on hätävalaistus ja hätäuloskäynnit selkeästi merkitty.
d) Tilat on suojattu ukkoselta. Virransyötössä on ylivirtasuojaus virtapiikkejä vastaan. Laitteet ja laitekaapit on maadoitettu ja laitteiden vioittuminen esimerkiksi oikosulussa (sähkövirta ja jäähdytysvesi) on estetty.
e) Tilat on jäähdytetty ja ilmastoitu ylikuumenemisen estämiseksi ja turvallisten työskentelyolosuhteiden turvaamiseksi.
f) Erityisesti ikkunallisissa tiloissa on tarvittavat ulkoiset lämmittimet, jotta laitteistot eivät jäähdy ja vioitu esimerkiksi talvella tapahtuvissa lämpökatkoksissa.
g) Tiloissa on asianmukainen sekä automaattinen (hälyttimet ja sammuttimet) että käsin käytettävä palontorjuntavälineistö.
h) Mikäli tarpeellista, tilat on EMP-suojattu voimakasta ulkopuolista sähkömagneettista pulssia vastaan.

## A5.10 Kaapelointi

### kontrolli

Tietoliikenne ja tietoliikennevälineet on suojattava. On turvattava tietoliikenteen katkottomuus ja tietojen saatavuus sekä estettävä salakuuntelu ja tietojen muuttuminen niitä siirrettäessä.

### käytännön ohjeita

a) Organisaation sisäinen tietoliikenneverkko on suojattu asianmukaisesti.
b) Tietoliikenne salataan mahdollisuuksien mukaan aina riippumatta, kuinka se on suojattu fyysisesti.
c) Kaapelit ja johdot sijoitetaan korotetun lattian alle, seinäkouruihin, maan alle tai muualle näkymättömiin aina, kun se on mahdollista. Niihin ei ole missään olosuhteissa pääsyä asiattomilla henkilöillä.
d) Kaapelit on varustettu tarvittavilla (esimerkiksi lähtöpiste ja kohdepiste sekä käyttötarkoitus) merkinnöillä.
e) Tietoliikennekaapelit erotetaan fyysisesti virtakaapeleista. Kaapelit suojataan sähkömagneettisesti.
f) Käytetään mahdollisuuksien mukaan valokaapelia.
g) Organisaation langaton tietoliikenneverkko (esimerkiksi WLAN) on suojattu asianmukaisesti, ja tarvittavia käyttäjien todennus- ja valtuutusmenettelyitä sekä tietoliikenteen salausta käytetään. Langattomien lähiverkkojen salakuuntelu ja niihin kytkeytyminen organisaation tilojen ulkopuolelta estetään. Suojaudutaan esimerkiksi yrityksiltä kytkeytyä langattomiin verkkoihin organisaation läheisistä tiloista tai kadulta *("war drivers"*).
h) Tietoliikennelaitteet, tietoliikenne- ja puhelinlinjat sekä kaapelit ja johdot on kahdennettu aina tarvittaessa. Pää- ja varayhteyksissä käytetään eri reittejä.
i) Kaapelien ja johdotusten kunto ja mahdollisesti valtuudeton pääsy johdotuksiin tarkastetaan säännöllisesti.

## A5.11 Puhelinverkot

### kontrolli

Kommunikointiin käytettävät puhelin-, kuvansiirto-, videoneuvottelu- ja muut verkot on suojattava niissä tarvittavine laitteineen (esimerkiksi puhelinvaihteet ja langattoman liikenteen tukiasemat). On turvattava välttämättömän ja tärkeän kommunikoinnin katkottomuus, suojauduttava verkkojen ylikuormitukselta sekä estettävä salakuuntelu.

### käytännön ohjeita

a) Sisäinen puhelinverkko laitteineen ja kaapeleineen suojataan asianmukaisesti.
b) Ulkoiset yhteydet suojataan asianmukaisesti. Julkiset telepalvelut hankitaan luotettavilta toimijoilta ja niiltä edellytetään tietoturvallisuusmääräysten noudattamista. Telepalvelujen tuottajan tietoturvapolitiikka evaluoidaan.
c) Puhelinverkosta, sen käytöstä, käyttäjistä (tilaajista) sekä tilaajalinjoista ja -yhteyksistä laaditaan riittävä dokumentaatio, jota voidaan käyttää myös esimerkiksi vikatilanteessa korvaavan menettelyn luomisessa tai vian korjauksessa.
d) Puhelinten ja muiden kommunikointivälineiden käytöstä laaditaan ohjeistus. Tämä koskee myös Internet-puheluita (esimerkiksi, kun Internetiä käytetään puhelinliikenteen välityksessä ja käyttäjän työasema toimii päätelaitteena).
e) Hätätilanteiden hoitoa ja puhelinpalveluita varten varataan sekä kiinteitä että kannettavia (mobiililaitteet) puhelinyhteyksiä ja puhelimia riittävä määrä. Esimerkiksi tietohallinnon käytössä olevat helpdesk-numerot tiedotetaan koko henkilöstölle.
f) Puhelinliikenteen ja puhelinvaihteiden kuormitusta seurataan, jotta puhelinjärjestelmät voidaan mitoittaa oikein ja suurta kuormitusta varten voidaan varata riittävä kapasiteetti.
g) Puhelinvaihteet kahdennetaan riittäviltä osiltaan. Avainhenkilöillä on käytössään vähintään kaksi puhelinliittymää (kannettava ja kiinteä).
h) Salakuuntelun estämiseksi pääsy puhelinvaihteisiin ja keskustiloihin rajataan ainoastaan valtuutetuille henkilöille.
i) Videoneuvotteluissa käytettävät laitteistot ja yhteydet suojataan asianmukaisin keinoin. Kaikki neuvotteluissa käyttäjiltä edellytettävät tietoturvatoimet on esitetty riittävän helppolukuisesti videoneuvottelutiloissa ja suojaukset on tarkastettavissa ennen neuvotteluyhteyksien avaamista.

## A5.12 Tietojen, tietovälineiden ja laitteiden poisto

### kontrolli

Kaikista organisaation käytöstä poistettavista tietojärjestelmistä on tutkittava esimerkiksi kovalevyille jääneet tiedot, kuten arkaluonteiset ja luottamukselliset tiedot sekä ohjelmistolisenssit. On varmistettava, että tietoa ei katoa eikä joudu asiattomiin käsiin. Sama varmistetaan myös tuhottavien tietovälineiden, kuten levykkeiden, cd-levyjen ja vastaavien osalta. Luvussa *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus* on lisää vaatimuksia tietovälineiden käytöstä ja poistoon liittyvistä toimenpiteistä.

### käytännön ohjeita

a) Jos mahdollista, tiedot tuhotaan sekä sähköisesti että fyysisesti. Tietovälineet, esimerkiksi kovalevyt, tuhotaan aina fyysisesti, mikäli ei voida olla varmoja, että tiedot ovat sähköisesti tuhoutuneet.
b) Arkaluonteisia tietoja sisältävät paperit tuhotaan aina fyysisesti, joko silppurilla tai laittamalla paperit lukolliseen roskasäiliöön, josta ne lähetetään tai noudetaan tuhottavaksi.
c) Muu arkaluonteisia tietoja sisältävä materiaali, kuten filmit ja kuvat, tuhotaan aina fyysisesti tarpeellista keinoa käyttäen.
d) Normaali tietojen poisto (*delete*) ei riitä, vaan levyillä olevat tiedot pitää ylikirjoittaa.
e) Vahingoittuneiden laitteiden poistossa, kun niissä sijainneet tiedot eivät ole käytettävissä, eikä tietojen olemassaolosta tai tuhoutumisesta voida varmistua, noudatetaan erityistä tarkkaavaisuutta.

# 8 Tietojärjestelmien käytön ja tiedonvälityksen turvallisuus

## 8.1 Yleistä

Yksi organisaation toiminnan ja toimintakyvyn varmistamisen oleellinen osa on varmistaa organisaation kaikkien henkilöiden oikeanlainen ja turvallinen tehtävien hoito ja tietojärjestelmien käyttö. Määrittämällä eri tehtävissä toimivien henkilöiden tarkat vastuut, velvollisuudet ja valtuudet luodaan pohja halutunlaiselle toiminnalle, joka täydennetään tarvittavilla käyttö- ja toimintaohjeilla. Jakamalla tarvittaessa vastuut osiin ja eriyttämällä ne eri henkilöille voidaan ehkäistä mahdollisuuksia tärkeiden ja kriittisten tietojen ja tietojärjestelmien väärinkäyttöön ja huolimattomuudesta aiheutuviin riskeihin.

Kaikkien tietojärjestelmien käyttäjien on siis tiedettävä, miten järjestelmiä pitää ja saa käyttää ja mihin tarkoitukseen niitä käytetään, sekä millainen käyttö on kiellettyä. Kaikkien henkilöiden, jotka käsittelevät järjestelmien sisältämiä tietoja, on tunnettava oikeanlaiset ja sallitut käsittelytavat ja käsittelysäännöt. Verkkopalveluiden ja tietoverkkojen käytöstä on oltava selkeät määräykset ja ohjeet, ja kaikkien verkkopalveluita käyttävien henkilöiden on tiedettävä säännöt ja noudatettava niitä.

Tietojärjestelmien kehityksessä, testauksessa ja tuotantoon otossa noudatetaan täsmällisiä ohjeita ja menettelyitä, jotta kehitystoiminta ei avaa portteja turvariskeille ja jotta voidaan varmistua, että käyttöön otettavat tuotteet ja palvelut eivät vaaranna tietoturvallisuutta. Myös toimittaessa kolmansien osapuolten kanssa luodaan sellaiset käytännöt, joilla voidaan taata, ettei organisaation tietoturvallisuus vaarannu.

Tietojärjestelmien ja tietoverkkojen hallinta ja hoito on oltava erityisen vastuullista toimintaa. Järjestelmäpäälliköt, pääkäyttäjät ja muut eri järjestelmistä ja sovelluksista vastaavat henkilöt, joilla yleensä on normaalikäyttäjää laajemmat valtuudet järjestelmien käyttöön, ovat soveltuvia vastuullisten tehtävien hoitoon. He ymmärtävät oikeuksien hallinnasta aiheutuvat uhkat, osaavat asennoitua vastuullisesti tehtäviinsä ja noudattaa tietoturvallisia menettelytapoja jokapäiväisissä toimissaan. Vastuuhenkilöiden koulutukseen ja osaamiseen kiinnitetään yleensä erityishuomio, koska epäpätevät henkilöt, esimerkiksi ne, jotka eivät ole tehtäviensä tasalla tai joiden osaaminen on vanhentunutta, aiheuttavat tietoturvariskin.

Verkkopalveluiden yleistyttyä on tavallista, että organisaatio laajentaa julkaisukäytäntöjään ja julkaisee erilaista materiaalia verkkosivuillaan. On helposti löydettävissä runsaasti esimerkkejä organisaatioista, joissa toimintaprosesseja ei muuteta tietoja verkkoon julkaistaessa, ja niinpä verkkojulkaisemista ei liitetä normaaleihin julkaisukäytäntöihin. Tästä syystä verkkosivustoja ja niiden sisältämiä tietoja ei ylläpidetä vaadittavalla tavalla, ja verkosta saatavat tiedot voivatkin usein olla vanhentuneita ja jopa virheellisiä. Tämä puolestaan aiheuttaa erilaisia uhkia sekä organisaatiolle että sen palveluita käyttäville. Liittyipä tietojen julkaiseminen sitten markkinointiin tai viranomaisen säätämään velvollisuuteen, julkaisemistoiminta on kuvattava ja määriteltyjä julkaisuprosesseja on noudatettava.

## 8.2 Uhkista ja riskeistä

Erilaisia uhkia tietojärjestelmien ja tietoliikenneverkkojen vääränlaisesta käytöstä ja puutteellisesta hallinnasta on lueteltu alla.

a) Organisaation toimintaprosessit eivät ole kuvattuja tai toiminta prosesseissa ei noudata sovittuja käytäntöjä.
b) Päivittäisistä tehtävistä ei ole riittävää ohjeistusta ja tehtäviä suoritetaan väärin ja väärien henkilöiden toimesta.
c) Kaikilla ei ole omat päivittäisen toimintansa vastuut tiedossa.
d) Arkaluonteisten tietojen käsittelystä ei ole selkeää ohjeistusta.

e) Organisaation tai kolmannen osapuolen henkilöt eivät noudata tietojen käsittelyohjeita ja väärinkäyttävät tietoja.
f) Tietojärjestelmään tehtävän muutoksen jälkeen joku oleellinen tietojärjestelmän hallintaan tai käyttöön liittyvä muutos jää dokumentoimatta ja ohjeistamatta. Tämä aiheuttaa myöhemmin järjestelmän sisältämien tietojen muuttumisen, tuhoutumisen tai valtuudettoman pääsyn tietoihin.
g) Muutoksia ei ole asianmukaisesti hyväksytty.
h) Muutoksessa tapahtuu virhe puutteellisesta muutoksen suunnittelusta ja väärästä ohjeistuksesta johtuen.
i) Muutoksen jälkeen ei voida palata ennen muutosta vallinneeseen tilanteeseen, vaikka muutos ei ole onnistunut. Paluun yhteydessä osa tärkeistä tiedoista tuhoutuu tai kaikkia varmistuksia ei onnistuta palauttamaan.
j) Tuotantokäytössä olevilla tietojärjestelmillä tehdään kehitys- ja testaustyötä.
k) Kehitystyötä tekeville henkilöille syntyy mahdollisuus lukea tuotannollisia tietoja, joihin heillä ei ole valtuuksia.
l) Kolmannelta osapuolelta saadut palvelut eivät noudata riittäviä laatu- ja tietoturvallisuusvaatimuksia tai näitä vaatimuksia ei ole määritelty.
m) Tietojärjestelmien ja tietoliikenneverkkojen hallintaa ja hoitoa ei ole ohjeistettu ja vastuutettu.
n) Järjestelmien toimintakykyä, suorituskykyä, kuormitusta, kapasiteettia tai niissä esiintyviä vikoja ei seurata.
o) Käyttäjille laadittu ohjeistus on puutteellinen, eivätkä käyttäjät ole tietoisia oman tietokoneensa, tietoverkkojen ja sähköpostin turvallisesta käytöstä.
p) Käyttäjillä on käytössään helposti arvattavia tai selvitettäviä salasanoja.
q) Organisaation tietojärjestelmiin leviää haittaohjelmia.
r) Haittaohjelmien tai verkkohyökkäyksien takia organisaation tietoja joutuu ulkopuolisiin käsiin.
s) Organisaation verkkopalvelut estyvät palvelunestohyökkäyksen takia.
t) Kryptografian ja PKI:n käyttömahdollisuuksia ei ole arvioitu. Hyödynnettävissä olevia menetelmiä ei käytetä.
u) Tietojärjestelmien tiedoista ei oteta varmuuskopioita, varmuuskopiot ovat virheellisiä tai osa tiedoista puuttuu.
v) Ulkopuolisille syntyy pääsy varmistuslaitteisiin tai tietovälineisiin, ja luottamukselliset tiedot joutuvat vääriin käsiin.
w) Erilaisten tietovälineiden käytöstä ja luottamuksellisten tietojen tallentamisesta niille ei ole ohjeistusta.
x) Tietovälineitä, joille on tallennettu luottamuksellisia tietoja, joutuu vääriin käsiin.
y) Tuhottavien tai poistettavien tietovälineiden tuhoamisessa kaikki talletetut luottamukselliset tiedot eivät tuhoudu.
z) Arkaluonteisia tietoja sisältävä sähköposti tai viesti lähetetään tai edelleen lähetetään väärään osoitteeseen.
å) Arkaluonteisia tietoja sisältävä telefax lähetetään väärään numeroon.
ä) Organisaation tietoliikennettä ja tietoliikenneyhteyksiä ei ole suojattu riittävästi tai suojaamista ei ole määritelty riittävän tarkasti.
ö) Organisaation lähettämät tai vastaanottamat tiedot muuttuvat tiedonsiirron aikana ja ovat virheellisiä.
aa) Fyysisesti lähetettävät tiedot hukkuvat tai vahingoittuvat kuljetuksen aikana.
bb) Verkkosivuilla julkaistavat tiedot sisältävät virheellisyyksiä tai julkaistuja, vanhentuneita tietoja ei poisteta sivuilta.

## kontrolli

Organisaation ja sen henkilöiden toiminta on kuvattava. Noudatettavien prosessien, niiden vaiheiden, tehtävien ja vastuiden kuvauksen on oltava riittävän yksityiskohtaista ja kattavaa. Oikeanlaisesta tai suositeltavasta toiminnasta ja tehtävien hoidosta on oltava riittävän yksityiskohtainen ohjeistus, jonka on oltava jokaisen sitä tarvitsevan henkilön hallussa ja ymmärtämä. Kaikkia kuvauksia ja ohjeita on ylläpidettävä ja niiden on vastattava kulloistakin toiminnallista tilannetta.

Tässä ei puututa eikä anneta ohjeita siihen, miten organisaation olisi prosessinsa suunniteltava, millaiset prosessit ovat toimivia, tehokkaita tai suositeltavia tai millä nimenomaisella tarkkuudella prosessit olisi kuvattava. Yleisesti voidaan kuitenkin todeta, että kulttuuri tietotekniikan hyödyntämiseen organisaatioiden prosesseissa on vielä nuorta. Tulevaisuudessa tietoteknistyminen ja tietotekniikan hyväksikäyttö lisäävätkin yhteistyötä organisaatioiden toiminnallisen, liiketoiminnan tietotekniikan johdon välillä. Tämä ohjannee prosessien kehitystä luonnostaan oikeaan suuntaan. Toisaalta voitaneen myös todeta, että sähköinen ja automaattinen tietojen käsittely sekä tehostaa toimintaa että vähentää inhimillisiä virheitä. Myös tietoturvallisuutta ja sen seurantaa voidaan parantaa sähköisillä järjestelmillä ja automaattisilla toimenpiteillä.

## käytännön ohjeita

a) Organisaation ydinprosessit määritellään ja kuvataan. Prosesseille määritellään omistaja ja muut vastuulliset henkilöt. Prosessikuvauksissa käytetään olemassa olevia ja hyväksyttyjä malleja ja menetelmiä.

b) Organisaation ydinprosessien lisäksi muut tärkeät prosessit kuvataan vaiheineen ja tehtävineen.

c) Varahenkilöillä on riittävä osaaminen tehtävien hoitoon. He tietävät olevansa varahenkilöitä ja ovat tietoisia varahenkilön vastuista. Varahenkilöille on tarvittaessa laadittu erillinen ohjeistus tehtävien hoitoon.

d) Prosesseissa suoritettavat tehtävät, joilla on kriittistä merkitystä tietoturvallisuuden toteutumiselle, jaetaan tarpeen ja mahdollisuuksien mukaan osiin ja eriytetään eri henkilöille. Yhdelle henkilölle ei ole tarkoituksenmukaista jättää laajoja valtuuksia tai mahdollisuuksia tahalliseen tai tahattomaan tietojen tai tietojärjestelmien väärinkäyttöön.

e) Prosesseissa suoritettavat tehtävät kuvataan ja niistä laaditaan tarvittava toimintaohjeistus toimenpide toimenpiteeltä. Ohjeistus on jokaisen sitä tarvitsevan henkilön saatavilla.

f) Tietojärjestelmien käytöstä laaditaan käyttöohjeet. Sekä käyttöohjeet että valmistajalta saadut manuaalit ovat jokaisen niitä tarvitsevan saatavilla.

g) Kaikkien tietojen käsittelystä ja säilytyksestä on olemassa säännöt ja ohjeistus. Sääntöjen ja ohjeistuksen laatimisesta ja ylläpidosta vastaa tietojen omistaja. Tähän liittyviä vaatimuksia löytyy enemmän luvusta *omaisuuden hallinta*.

h) Arkaluonteisten tietojen (esimerkiksi henkilö- ja potilastiedot) käsittelyohjeet ja käsittelyyn tarkoitettujen tietojärjestelmien käyttöohjeet sisältävät yksityiskohtaiset menettelyohjeet kaikkien tällaisten tietojen sallitusta ja hyväksyttävästä käsittelystä. Jokainen oikeutettu käsittelytoimenpide, ja missä olosuhteessa kyseinen toimenpide on sallittu, on listattu erikseen. Myös kaikista kielletyistä toimenpiteistä on laadittu lista.

i) Tietojärjestelmäkuvaukset ja järjestelmien ohjeet sisältävät riittävät tiedot ainakin vastuista ja vastuuhenkilöistä sekä tietojen käsittelystä ja siihen liittyvistä toimista.

j) Järjestelmien vastuuhenkilöille tarkoitetut ohjeet sisältävät tarvittavat tiedot ainakin varmistuksista, eräajoista, tietoturvallisuuden ja käytön tarkkailusta sekä toimista vika- ja poikkeustilanteissa.

k) Kuvaukset, ohjeet ja manuaalit ovat osa tietojärjestelmää, ja niiden ylläpito on tietojärjestelmästä vastaavan henkilön vastuulla. Muutosten osalta noudatetaan normaalia tietojärjestelmämuutosten hyväksymismenettelyä.

l) Organisaation toiminta- ja liiketoimintaprosesseja suunniteltaessa ja kuvattaessa huomioidaan tietojärjestelmät, niiden käyttö ja osallisuus prosessin kulkuun. Tietojärjestelmien käytöstä saatavat edut otetaan mahdollisuuksien mukaan huomioon jo prosesseja suunniteltaessa.

## A6.2 Muutoksen hallinta

### kontrolli

Tietojärjestelmiin ja tietojenkäsittely-ympäristöihin tehtäviin muutoksiin on oltava tarkasti kuvattu menettelytapa, jota noudatetaan kaikissa muutostilanteissa. Kaikki muutokset on dokumentoitava. Muutoksenhallintamenettelyt koskevat myös kolmansilta osapuolilta hankittavia palveluita ja tuotteita. Muutoksen hallintaan liittyviä ohjeita on lisää jäljempänä luvun *tietojärjestelmien kehitys ja ylläpito* kappaleessa *muutoksen hallinta*.

### käytännön ohjeita

a) Tärkeät ja merkitykselliset muutokset tunnistetaan. Muutoksista pidetään kirjaa. Kirjattavia muutoksia ovat esimerkiksi tietoihin (tietojen rakenteisiin), tietojärjestelmiin (ohjelmistot, laitteistot ja uudet versiot), kokonaisiin tietojenkäsittely-ympäristöihin (fyysiset tilat, tietoverkot ja mahdolliset kolmansien osapuolten palvelut) ja tietojenkäsittelytapoihin (prosessi- ja toimintatapamuutokset sekä uudet käyttöönotettavat ohjelmistot) tehtävät muutokset.
b) Muutoksista aiheutuvat riskit analysoidaan ennen muutosten toteutumista.
c) Muutosten hyväksymiseen käytetään olemassa olevaa menettelyä.
d) Tehtävistä ja tehdyistä muutoksista tiedotetaan sovitun käytännön mukaisesti kaikille tarvittaville osapuolille.
e) Muutostoimien edetessä varmistetaan, että toimenpiteet voidaan keskeyttää ja palata alkuperäiseen, ennen muutostoimenpiteiden aloitusta vallinneeseen tilanteeseen.
f) Muutokset dokumentoidaan kaikkiin tarvittaviin asiakirjoihin ja järjestelmäkuvauksiin. Muutoksista dokumentoidaan kaikki oleellinen tieto, mukaan lukien muutoksen ajankohta ja vastuulliset henkilöt. Muutoksen yhteydessä vanhentuneita tietoja ei säilytetä aktiivistatuksella vaan ne päivätään vanhentuneiksi.
g) Muutokset dokumentoidaan tarvittavilta osin myös muihin organisaation asiakirjoihin. Järjestelmäkuvausten lisäksi muutokset aiheuttavat päivitystarpeita myös esimerkiksi käyttöohjeisiin, riskianalyyseihin tai muihin tietoturvadokumentteihin, kuten tietoturvapolitiikkaan. Ne voivat aiheuttaa päivitystarpeita myös organisaation omien palveluiden kuvauksiin.
h) Muutosten jälkeen ympäristön ja järjestelmien tilannetta seurataan erityisen tarkasti. Varmistetaan, että tarvittaessa voidaan palata vanhaan, ennen muutoksia vallinneeseen tilanteeseen.
i) Muuttunut tilanne päivitetään tietoturvallisuuskontrolleihin, joilla seurataan tietojärjestelmiä ja niiden toimintaa.
j) Kolmansien osapuolten tuottamien palveluiden muutokset ja niiden vaikutukset dokumentoidaan tarpeen mukaan. Tällaisia tilanteita ovat hankittaessa esimerkiksi tietojärjestelmien käyttöpalveluita, tietoliikennepalveluita tai varmennepalveluita kolmansilta osapuolilta. Myös muutosten vaikutukset hankittavien palveluiden laatuun dokumentoidaan. Myös ne tilanteet huomioidaan, joissa palveluntuottaja vaihdetaan kokonaan toiseen.

## A6.3 Kehitysjärjestelmät

### kontrolli

Kehitykseen, testaukseen ja tuotantoon käytettävät tietojärjestelmät ja tiedot on eriytettävä. Kehityksessä ei käytetä järjestelmiä eikä tietoja, joita käytetään samanaikaisesti myös tuotannossa. Jos kehitykseen tai testaukseen joudutaan käyttämään oikeita tietoja tai niiden kopioita, on huolehdittava tietojen

riittävästä suojaamisesta. Ohjelmistokehitykseen liittyviä ohjeita on löydettävissä myös luvun *tietojärjestelmien kehitys ja ylläpito* kappaleessa *lähdekoodi* ja testaukseen liittyviä ohjeita kappaleessa *muutoksen hallinta*.

### käytännön ohjeita

a) Kehitettävien ohjelmistojen käyttötarkoituksesta ja kriittisyydestä riippuen määritetään sopiva taso, jolla kehitysjärjestelmien ja tuotannollisten järjestelmien toisistaan eriyttäminen toteutetaan. Erityisesti kriittisissä järjestelmissä tai kriittisten tietojen käsittelemiseen tarkoitetuissa järjestelmissä (esimerkiksi potilastietojärjestelmät) eriyttäminen on ensiarvoisen tärkeää.

b) Eriyttäminen toteutetaan tarpeen mukaan valituilla keinoilla – käyttämällä erillisiä prosessoreita ja kovalevyjä, kokonaan eri laitteistoja ja jopa erillisiä tai eristettyjä tietoverkkoja.

c) Kehityshenkilöiden pääsy tuotannollisiin järjestelmiin estetään riittävillä menetelmillä ja suojauksilla, koska tällainen pääsy saattaa luoda huomattavan riskin tietoturvallisuudelle, erityisesti voidaan vaarantaa tietojärjestelmissä käytettävien tietojen luottamuksellisuus ja mahdollistaa järjestelmien (tahalliset tai tahattomat) valtuudettomat muutokset.

d) Kun kehitysjärjestelmä siirretään tuotantokäyttöön, käytetään sovittuja muutoksenhallintamenettelyitä. Siirto dokumentoidaan sovitun käytännön mukaisesti.

e) Kehitysjärjestelmiin, kehitystyökaluihin, kehityksessä käytettävään dataan ja lähdekoodiin ei ole suositeltavaa avata mitään pääsyä tuotannollisesta tietoverkosta, ellei se ole välttämätöntä.

f) Testattaessa kehitettyjä ohjelmistoja emuloidaan tuotantoympäristöä ja tuotannonomaista käyttöä mahdollisimman tarkasti (esimerkiksi hyväksyntätestauksessa).

g) Jos tuotanto-ohjelmistoissa käytetään mahdollisuutta testata ohjelmiston toimintoja (esimerkiksi testikäyttäjät ja koekäyttö), kaikista valikoista ja käyttöliittymistä ilmenee yksiselitteisesti, että kyseessä on testi- tai koekäyttö. Tällöin käytetään testidataa ja vältetään kaikkea tuotannollisen tiedon käyttöä.

## A6.4 Kolmansien osapuolten palvelut

### kontrolli

Käytettäessä kolmansien osapuolten palveluita ja tuotteita on huolehdittava, että kaikessa toiminnassa ja yhteistyössä otetaan huomioon tietoturvallisuus ja noudatetaan laadittuja toimintamalleja. Kolmannen osapuolen on osaltaan noudatettava kaikkia niitä käytäntöjä, joita siltä edellytetään. Turvallisuus täytyy huomioida sekä sopimuksellisesti, käytännön toiminnassa ja tietojen vaihdossa että käytettävissä teknisissä ratkaisuissa (sähköposti, kulunvalvonta, huolto ym.). Turvallisuutta täytyy tarkkailla ja rikkeisiin puuttua sovitun mukaisesti. Kolmansien osapuolten kanssa toimimista on käsitelty myös luvussa *fyysisen ympäristön turvallisuus*.

### käytännön ohjeita

a) Kolmansien osapuolten toiminta, palvelutaso ja laatu määritellään ja sovitaan osapuolten välisissä sopimuksissa. Mahdollisiin uhkiin varaudutaan ja niiltä suojaudutaan sopimuksellisesti määrittämällä riittävät sanktiot, korvaukset ja rangaistukset väärästä tai haitallisesta toiminnasta.

b) Kolmannen osapuolen kanssa tehtävän yhteistyön ohjaamiseksi perustetaan ohjausryhmä, joka hallinnoi yhteistyötä ja puuttuu mahdollisiin väärinkäytöksiin. Ryhmä raportoi tarvittaessa sekä tietoturvajohdolle, tietohallinnolle että kyseistä palvelua koskevan toimialan, toiminnon tai liiketoiminnan johdolle. Vastuu kolmannen osapuolten tuottamien palveluiden laadun ja turvallisuuden tarkkailusta säilytetään kaikissa olosuhteissa omassa organisaatiossa.

c) Jos olemassa olevia toimintamalleja muutetaan esimerkiksi ulkoistamalla toimintoja kolmannelle osapuolille (kuten järjestelmien tai tietoliikenteen hoito), riittävää turvallisuuden tasoa noudatetaan myös toimintojen siirron ja palveluiden käyttöönoton ("yliheitto") aikana. Tällöin noudatetaan myös normaaleita muutoksen hallinnan menettelyitä ja turvallisuuden jälkiseurantaa.

d) Ulkoistettaessa kriittisiä toimintoja tai hankittaessa tuotteita tai palveluita kriittiseen käyttöön tai erittäin tärkeiden tietojen käsittelyä varten (esimerkiksi organisaation sisäisen tietoliikenteen toteuttavat laitteet ja komponentit sekä potilastietojärjestelmät), noudatetaan erityistä varovaisuutta toimittaessa kolmansien osapuolten kanssa. Yhteistyökumppania valittaessa tältä voidaan myös edellyttää riittävän tasoisia takuita ja valmiuksia toiminnan jatkumisesta (esimerkiksi vakavaraisuus, riittävä henkilöstömäärä ja liikevaihto, hyvä maine, luotetut tuotteet, sertifioitu toiminta). Tarvittaessa voidaan laatia luettelo hyväksytyistä yhteistyökumppaneista tai palveluntuottajista.

e) Varmistetaan, että kolmansilta osapuolilta hankitut tuotteet ovat kaikkien oleellisten standardien ja de facto -standardien mukaisia.

f) Kolmannen osapuolen on raportoitava määrävälein havaituista tietoturvaloukkauksista ja toiminnan laadusta. Jos tietoturvaloukkauksia ei ole, raportoinnin kohteena on oltava ainakin saavutettu palvelun laatutaso (vasteajat, suorituskyky) ja kolmannen osapuolen sisäisistä toimista johtuvat mahdolliset vaikutukset yhteistyöhön tai palveluihin.

g) Kolmannen osapuolen toiminta ja toiminnan laatu auditoidaan määrävälein ja tarkastetaan muulloinkin tarpeen mukaan (esimerkiksi, kun on havaittu tai raportoitu tietoturvaloukkauksia).

h) On suositeltavaa, että kolmansien osapuolten kanssa järjestetään säännöllisiä tapaamisia ("ylläpitokokous" tai vastaava), jossa arvioidaan edellisen kauden toiminnan taso, käsitellään mahdolliset poikkeukset, määritellään sanktiot ja sovitaan seuraavan kauden tavoitteet ja tehtävät, mikäli nähdään, että sellaisista on tarpeellista sopia.

i) Palveluiden laatua määritettäessä käytetään tarpeen mukaan standardoituja vaatimuksia (ISO, SFS).

## A6.5 Tietojärjestelmien ja tietoverkkojen hoito

### kontrolli

Tietojärjestelmien ja tietoverkkojen hallinnan ja hoidon vastuut on oltava riittävän asiantuntemuksen omaavilla henkilöillä, ja hallintatehtävien hoitoon on varattu riittävästi henkilö- ja muita resursseja sekä tarvittavia apuvälineitä ja työkaluja. Vastuuhenkilöt tuntevat ja tietävät järjestelmät ja toimintaohjeet, joita noudattamalla ylläpidetään järjestelmien ja tietoverkkojen turvallisuutta, toimintakuntoa, käytettävyyttä ja hallitaan järjestelmien käyttäjiä. Järjestelmien toimintaa seurataan ja erilaisissa vika-, ongelma- ja kuormitustilanteissa ryhdytään asianmukaisiin toimiin. Seurantatietoa käytetään hyväksi suunnittelutehtävissä.

### käytännön ohjeita

a) Säännölliset, esimerkiksi päivittäiset ja viikoittaiset tietojärjestelmien ja tietoliikenneverkkojen hallintatoimet on määritelty, vastuutettu ja ohjeistettu yksityiskohtaisesti.

b) Järjestelmien hallinnasta ja hoidosta vastuulliset henkilöt (esimerkiksi järjestelmäpäälliköt ja sovellusten pääkäyttäjät) ovat soveltuvia vastuullisiin tehtäviin ja he ovat saaneet tehtäviinsä riittävän koulutuksen. Osaamista täydennetään tarpeen mukaan lisäkoulutuksella.

c) Tietojärjestelmillä toteutettavat palvelut ja niiltä vaadittava palvelutaso on määritelty. Alihankkijoiden ja palveluntuottajien kanssa solmituissa palvelutasosopimuksissa huomioidaan vaatimukset.

d) Uudet järjestelmät testataan huolellisesti ennen käyttöönottoa. Hyväksymistestaus ja hyväksyminen noudattavat virallista menettelyä. Järjestelmien hallinnoimiseksi ja hoitamiseksi py-

ritään soveltamaan jo käytössä olevia menettelyitä. Kaikki uudet järjestelmät lisätään relevantteihin olemassa oleviin dokumentteihin, toiminta- ja käyttöohjeisiin. Asennuksissa käytetään valmistajilta saatuja ohjeita, suosituksia ja tarkastuslistoja.

e) Käyttöjärjestelmien asetukset noudattavat järjestelmillä toteutettavien palveluiden tietoturvavaatimuksia. Tarvittaessa "kovennetaan" käyttöjärjestelmien ja sovellusten turvatasoa. Ainoastaan sellaisia järjestelmiä käytetään, joilla voidaan toteuttaa vaadittava tietoturvataso.

f) Sovelluksia käytetään minimioikeuksilla ja minimiresursseilla; toisin sanoen suoritettava ohjelmistokoodi ei saa käyttöjärjestelmältä yhtään sellaisia oikeuksia ja resursseja, joita se ei tarvitse.

g) Järjestelmien toimintakykyä ja kuormitusta seurataan ja seurannassa käytetään apuna tarvittavia työkaluja. Kuormituksen mittareita voivat olla esimerkiksi prosessien toiminta-ajat, vasteajat, levytilan ja muistin täyttöasteet, prosessorin kuormitus sekä verkkoliikenteen, tapahtumien ja käyttäjien määrä. Seurantatietojen perusteella selvitetään suorituskyvyn pullonkaulat ja suoritetaan tarvittavat ennalta sovitut ja ohjeistetut toimenpiteet, esimerkiksi kapasiteettia voidaan lisätä tarpeen mukaan. Seurantatietoja käytetään hyväksi myös tietojärjestelmäarkkitehtuurin edelleen suunnittelussa.

h) Järjestelmissä esiintyviä vikoja ja tietoturvaongelmia seurataan. Mahdollisten vikojen, turvaloukkausten tai niistä annettujen hälytysten perusteella ryhdytään asianmukaisiin ennalta sovittuihin toimiin.

i) Järjestelmien käyttäjien hallinta on vastuutettu. Käyttäjien hallinnasta ja pääsyoikeuksista on tarkemmin määritelty luvussa *pääsynhallinta*.

j) Järjestelmien kuormitukseen, vikoihin ja käyttäjien hallintaan liittyviä tietoja ja numeerisia arvoja seurataan. Tietoja käytetään hyväksi järjestelmien suunnittelussa ja järjestelmien huoltoon ja ylläpitoon liittyvissä tehtävissä ja kolmansien osapuolten kanssa solmittavissa sopimuksissa.

k) Tietoliikenneverkkoihin kytketyt laitteet nimetään yksiselitteisesti. Kaikissa järjestelmissä on sopivat verkkotunnisteet ja verkko-osoitteet, joilla järjestelmät voidaan tunnistaa käyttäjien ja muiden järjestelmien toimesta.

l) Tietojärjestelmien etähallintaa varten on luotu toimintasäännöt ja asianmukaisesti suojatut yhteydet. Järjestelmien etädiagnostiikka on tarkoin suojattu ja mahdolliset käyttöoikeudet jaettu vain järjestelmien hoitajille tai muille sopiville teknisille henkilöille.

m) Tietoliikenneverkon rakenne, eri verkkokomponenttien asetukset ja kaikki käytettävät yhteydet on dokumentoitu yksityiskohtaisesti.

n) Verkkoliikenteen reititys suunnitellaan siten, että tietoliikennetoteutukset ja tietojen siirto verkoissa ei muodosta uhkaa tietoturvallisuudelle. Verkkolaitteiden tunnistamisessa käytetään tarvittavia ja turvallisia tunnisteita ja osoitteita. Sanomien lähde- ja kohdeosoitteet varmistetaan tarvittaessa. Langattomien lähiverkkojen käyttö tietojen siirrossa suunnitellaan erityisen turvalliseksi.

o) Organisaation tietoliikenne on suojattu käyttämällä turvallista arkkitehtuuria (esimerkiksi puolueettomat vyöhykkeet, *dmz*) ja turvaamalla verkko riittävin palomuurein, virustorjunnoin sekä tunkeutumisen havainnointi- ja esto-ohjelmin. Tarvittaessa erityyppiset, erilaisen tietoturvallisuuden vaatimat palvelut ja käyttäjät voidaan eriyttää omiin verkkoihinsa tai vyöhykkeisiinsä sopivilla teknisillä ratkaisuilla.

p) Verkkoliikenteen määrää seurataan, jotta kapasiteetti voidaan suunnitella oikeaksi ja jotta mahdolliset palvelunestohyökkäykset tunnistetaan. Standardissa *ISO/IEC 18028 Network Security* määritellään tietoliikenteen turvaamisen vaatimuksia.

q) Organisaation sähköpostipalvelimet konfiguroidaan siten, että tietoturvallisuus on huomioitu. Tarvittaessa käytetään esimerkiksi kryptografisia menetelmiä (sähköinen allekirjoitus, salakirjoitus), virusten ja roskapostien (*spam*) torjuntaa sekä kapasiteetin ja käyttäjien toimien rajoituksia (yksittäisen käyttäjän postilaatikon koko, viestien koko, liitetiedostojen määrä, jakelulistojen koko, luuppien ja ketjukirjeiden tunnistus ja esto). Riittävästä varmuuskopioinnista huolehditaan.

r) Organisaation muille tarjoamia palveluita ja niitä tarjoavien järjestelmien ja verkkojen toimintakykyä hallitaan ja tarkkaillaan erikseen määritellyllä tavalla. Menetelminä voivat olla vastaavat menetelmät, kuin mitä käytetään myös organisaation muiden tuotannollisten järjestelmien hallinnassa.

s) Käyttäjien työasemat ja ohjelmistot konfiguroidaan siten, että käyttäjällä ei ole mahdollisuutta tehdä valtuudettomia muutoksia, ohjelmistoasennuksia tai muita toimenpiteitä. Työasemissa on käytössä riittävät haittaohjelmien tunnistuskäytännöt, ja virustietokannat päivitetään säännöllisesti. Tarvittaessa mahdollisuus esimerkiksi levyke- tai cd-asemien, USB-muistien ja itse lisättävien tietoliikenneyhteyksien (kuten ulkoiset modeemit) käyttöön on estetty.

t) Salasanallinen näytönsäästäjä aktivoidaan kaikissa käyttäjien työasemissa. Näytönsäästäjä aktivoituu automaattisesti sopivaksi katsotun ajan kuluttua, kun työasemaa ei ole käytetty.

u) Tarvittaessa käyttäjä todennetaan työasemassa käyttäjätunnuksen ja salasanan sijasta toimikortilla. Käyttäjien työasemien tietojen varmuuskopiointi määritellään tallennettujen tietojen kriittisyyden perusteella.

v) Verkkoyhteyksien ja tietojärjestelmien käyttöä ja käyttäjien tietojärjestelmiin kytkeytymistä seurataan. Tarvittaessa käyttämättömiä ja ei-aktiivisia verkkoyhteyksiä ja käyttäjien istuntoja voidaan lopettaa automaattisella katkaisulla (*timeout*). Ulkoiset tietoliikenneyhteydet, joita ei enää tarvita, poistetaan käytöstä. Ulkoisissa modeemiyhteyksissä, kun käyttäjä on organisaation tilojen ulkopuolella, pyritään käyttämään takaisinsoittoperiaatetta.

w) Korkean turvatason vaativien verkkoyhteyksien yhteysaikaa voidaan tarvittaessa rajoittaa tai se voidaan asettaa määrämittaiseksi. Tällaisia yhteyksiä voivat olla esimerkiksi tietojen varmistuksiin tai eräajotyyppisiin suurten tietomäärien automaattisiin siirtoihin käytettävät yhteydet.

x) Oletuskäyttäjätunnukset poistetaan käytöstä (esimerkiksi 'guest' tai 'manager'), ja ei-henkilöityjä tunnuksia käytetään ainoastaan silloin, kun se on välttämätöntä (esimerkiksi 'demo' tai 'vieras').

## A6.6 Käyttäjien velvollisuudet: tietoturvaohjeistuksen laadinta käyttäjille

### kontrolli

Käyttäjien velvollisuudet päivittäisissä toimissa on ohjeistettava. Ohjeiden täytyy olla kaikkien niitä tarvitsevien henkilöiden tiedossa ja omaksumia. Riittävät ja kattavat ohjeet täytyy laatia kaikista niistä toimista, joiden tekemisestä tai tekemättä jättämisestä voi muodostua uhka tietoturvallisuudelle. Tietojärjestelmien päivittäisen käytön ja tietojen päivittäisen käsittelyn lisäksi erityisesti ulkoisten verkkopalveluiden käyttö organisaation tietojärjestelmillä saattaa aiheuttaa vakavia uhkia organisaation tietoturvallisuudelle. Erilaiset haittaohjelmat leviävät organisaation verkkoon usein joko sähköpostien liitetiedostoista tai erilaisilta verkkosivuilta. Tästä syystä tällaisten palveluiden ja verkkosivujen käyttö ja sen salliminen on määriteltävä ja ohjeistettava tarkasti. Tarvittaessa voidaan estää pääsy tietyille verkkosivuille, tyypillisesti esimerkiksi aikuisviihde- ja uhkapelisivustoille.

### käytännön ohjeita

Ainakin alla olevista asioista on syytä mainita käyttäjille jaettavassa tietoturvaohjeistuksessa ja niitä on myös syytä käsitellä henkilöstölle annettavassa tietoturvakoulutuksessa. Erilaisia ohjeissa mainittavia asioita löytyy useista tämän dokumentin kohdista.

a) Salassa pidettävistä asioista ja tiedoista (esimerkiksi henkilö- ja potilastiedot) laaditaan luettelo ja niiden käsittelystä ohje, jossa on kuvattuna myös tietojen luovutusta koskevat säännöt. Ohje voi sisältää myös käytännön ohjeita, kuten "*älä lue tietoja, joihin sinulla ei ole oi-*

*keutta*" tai "*älä luovuta mitään tietoja, ellet ole varma, että vastaanottajalla on oikeus tietoihin*".

b) Henkilön mahdollinen pääsy omiin terveys- tai potilastietoihinsa toteutetaan tietoturvallisella tavalla. Sähköpostin käyttöä potilastietojen lähetykseen tai siirtoon ei sallita, koska pääsääntöisesti henkilöiden yksityiset sähköpostilaatikot ovat salaamattomia ja sähköpostipalvelut sellaisten kolmansien osapuolten tuottamia, joiden tietoturvallisuustasoa ei ole sertifioitu tai joka ei vastaa terveydenhuollon tietojenkäsittelyn palveluntuottajille asettamia vaatimuksia.

c) Turvallisen tietokoneen käyttö ohjeistetaan. Ohjeessa on syytä mainita ainakin virustorjunnan, näytönsäästäjien ja niiden salasanojen käyttö sekä "*clear screen policy*". Työasema lukitaan, kun työpisteestä tai työaseman äärestä poistutaan. Istunnot suljetaan, kun yhteyksiä ei tarvita.

d) Etäyhteyksien, kannettavien tietokoneiden, kotitietokoneen ja matkapuhelimen turvallinen käyttö ohjeistetaan. Samassa yhteydessä on syytä ohjeistaa myös tietoturvallinen käyttäytyminen matkustettaessa, oltaessa julkisissa tiloissa ja puhuttaessa puhelimessa ("*clear air policy*"). Organisaation ulkopuolisissa tietoverkoissa kytkettynä olevan kannettavan tietokoneen uudelleenkytkeminen organisaation verkkoon ja kytkemistä edeltävät välttämättömät suojaustoimenpiteet on ohjeistettu.

e) Tietojen tallentaminen ja luottamuksellisia tietoja sisältävien asiakirjojen ja tietovälineiden tuhoaminen ohjeistetaan. On syytä ohjeistaa erikseen suositeltavat tallennustavat oman tietokoneen paikalliselle kovalevylle, verkkolevyille sekä henkilökohtaisten, siirrettävien ja kertakäyttöisten tietovälineiden käyttäminen tallennukseen (cd-levyt, levykkeet, USB-muistit, paperitulosteet). Ohje sisältää tarvittavan tiedon salattavien tietojen säilytyksestä ja "*clean desk policy*" -ohjeen.

f) Tietoverkkojen käyttö ohjeistetaan.

g) Internet-käyttö ohjeistetaan, erityisesti selailu organisaation verkossa olevalla tietokoneella. Ohjeessa on mainittu kielletyt sivustot ja aihealueet (kuten aikuisviihde, uhkapeli ja verkkopelaaminen).

h) Salasanamenettelyt ohjeistetaan. Tämä sisältää vaatimukset esimerkiksi salasanojen ja PIN-koodien minimipituuksille ja muille laadullisille ominaisuuksille, esimerkiksi isojen kirjainten, erikoismerkkien ja numeroiden käytölle, salasanan vaikealle arvattavuudelle ja selvitettävyydelle (salasana ei sisällä läheisten nimiä, puhelinnumeroita ym., ei ole identtinen käyttäjätunnuksen kanssa eikä ole altis "sanakirjahyökkäyksille"). Käyttäjätunnukset ja salasanat on pidettävä omassa tiedossa eikä niitä saa missään tapauksessa kirjoittaa muistiin tai säilyttää sähköisessä muodossa (esimerkiksi tiedostossa). Jos salasanan paljastumista on syytä epäillä, on salasana vaihdettava uuteen välittömästi. Organisaatiossa käytettävien käyttäjätunnusten ja salasanojen kanssa identtisten tunnusten käyttö organisaation ulkopuolella, esimerkiksi julkisissa verkkopalveluissa tai henkilökohtaisissa sähköpostipalveluissa, on ehdottomasti kiellettyä.

i) Käyttäjä ei anna tunnuksiaan ja salasanojaan muiden käytettäväksi. Mitään salasanoja ei lähetetä tietoverkossa selkokielisenä eikä tallenneta automaattisiin sisäänkirjautumistiedostoihin, erilaisiin makroihin tai funktionäppäimiin. Yhteiskäyttöisiä tunnuksia ei ole käytössä.

j) Sähköpostin ja muiden yhteydenpito-ohjelmistojen (kuten pikaviestinnän, *instant messaging*) käyttö ja kielletyt sähköpostin käyttötavat ohjeistetaan. Ohje sisältää säännöt esimerkiksi viestien edelleen lähetyksen tai automaattisen koko sähköpostin edelleen lähetyksen toiselle työntekijälle sekä salaus- ja allekirjoitussäännöt, esimerkiksi "*vain julkista tietoa saa lähettää sähköpostilla salaamatta*". Ohjeessa on syytä mainita myös käytännön ohjeita, kuten "*työviestien lähettäminen yksityispostista ja työpostin edelleen lähetys yksityiseen sähköpostilaatikkoon on kielletty*", "*yksityispostilaatikon käyttö työviestien vastaanottamiseen on kielletty*" sekä "*organisaatiolle haitallisten viestien, esimerkiksi myynti- ja markkinointiviestien sekä kiertokirjeiden lähetys on kielletty*".

k) Henkilökohtaisten työasemien käyttö muiden kuin työasioiden hoitoon määritellään ja ohjeistetaan.

l) Toiminta väärinkäytöstilanteissa ja havaittaessa uhkia ohjeistetaan. Väärinkäytösten ja uhkien ilmoittamismenettelystä on ohje.
m) Vieraiden ja ulkopuolisten henkilöiden (esimerkiksi huolto- ja ylläpitohenkilöt) vastaanotto organisaation tiloissa ohjeistetaan.
n) Avainten, kulku- ja toimikorttien käytöstä ja säilytyksestä laaditaan ohje, jossa kuvataan myös toiminta esimerkiksi toimikortin kadotessa tai vikaantuessa.
o) Työntekijältä edellytettävät toimet työsuhteen alkaessa (esimerkiksi rekisteröinnit ja henkilökorttikuvaukset) ja loppuessa (omaisuuden palautus) ohjeistetaan.

## A6.7 Haittaohjelmilta suojautuminen

### kontrolli

Erilaisilta haittaohjelmilta ja verkkohyökkäyksiltä on suojauduttava asianmukaisin keinoin, esimerkiksi käyttämällä virustorjuntaa, palomuureja ja verkkohyökkäysten havainnointiohjelmistoja (IDS, *intrusion detection software*). Havaittujen haittaohjelmien tuhoaminen ja normaalitilaan paluu on oltava suunniteltua. Tuotantokäyttöön otettavien ohjelmistojen virheellisyyksistä on suojauduttava jo ohjelmistojen vaatimusmäärittely-, kehitys- ja testausvaiheissa ja niitä on tarkkailtava tuotantokäytön alettua. Tähän liittyvät vaatimukset on mainittu luvussa tietojärjestelmien kehitys ja ylläpito.

Tietojärjestelmien ja työasemien käyttäjät on koulutettava ja ohjeistettava oikeanlaiseen tietojärjestelmien käyttöön, jotta haittaohjelmat eivät pääse organisaation tietojärjestelmiin eivätkä jatka leviämistään. Käyttäjien on oltava tietoisia riskeistä, osattava havainnoida uhkatilanteita, tunnistaa mahdollisten virusten ja muiden vastaavien haittaohjelmien toiminta ja osattava toimia tilanteessa siten, että korjaustoimiin voidaan ryhtyä pikaisesti ja ongelmat saadaan ehkäistyä ja korjattua.

### käytännön ohjeita

a) Otettaessa tietojärjestelmiä ja ohjelmistoja käyttöön suojaudutaan haittaohjelmilta jo ennalta: laaditaan kunnolliset, haittaohjelmilta suojautumisen huomioivat järjestelmien vaatimusmäärittelyt, noudatetaan riittäviä, tehokkaita ja dokumentoituja kehitys- ja testausprosesseja sekä käytössä olevia muutoksenhallintamenettelyitä.
b) Käyttäjien tietoturvakoulutuksessa käydään säännöllisesti läpi haittaohjelmat, niiden aiheuttamat uhkat ja riskit sekä oikeanlainen toiminta. Käyttäjät koulutetaan ja ohjeistetaan toimintaan, millä haittaohjelmat eivät leviä: ohjeet koskevat esimerkiksi sähköpostin käyttöä, liitetiedostojen avaamista, virustorjuntaa, Internetin käyttöä ja kiellettyjä verkkosivuja, tietovälineiden (kuten cd- ja dvd-levyt) käyttöä sekä pakollisia työasemien tietoturvapäivityksiä. Kannettavien tietokoneiden käyttö, etä- ja kotikäyttö sekä tietoliikenteen ja langattomien lähiverkkojen käyttö ohjeistetaan, kuten myös ohjelmistojen asennus työasemiin. Ainoastaan niiden ohjelmistojen käyttö ja asennus on sallittua, joihin on laillinen käyttöoikeus ja jotka ovat nimenomaisesti sallittujen ohjelmistojen listalla.
c) Käyttäjille on koulutettu, kuinka pitää toimia havaittuaan viruksen. Käyttäjiä varten on perustettu palvelupiste sekä ongelmia että kysymyksiä varten. Käyttäjille on tiedotettu palvelupisteen (puhelinnumero, verkko-osoite ym.) yhteystiedot.
d) Kaikissa käyttäjien työasemissa (mukaan lukien kannettavat työasemat, PDA:t ja älypuhelimet) on aktivoitu virustorjunta, joka on aktiivinen aina työaseman virran ollessa kytkettynä.
e) Virustorjuntaohjelmiston päällä oloa ja ajantasaisuutta tarkkaillaan ja tarvittaessa suoritetaan hälytys vastuuhenkilölle.
f) Virustorjunta kattaa tietokoneen kovalevyt ja verkkolevyt, muistin, ulkoisten tietovälineiden, tietoverkon ja eri ohjelmistojen (esimerkiksi sähköposti, liitetiedostot tai verkkoselain) virustarkastuksen. Tunnistetuista viruksista ilmoitetaan ja virukset tuhotaan tai tehdään toimintakyvyttömäksi.
g) Virustorjuntaohjelmistot ja niiden käyttämät virustietokannat päivitetään säännöllisesti. Ohjelmistoina ja tietokantoina käytetään uusimpia julkaistuja versioita, jotta tiedot ovat ajan ta-

salla ja uusimmilta viruksilta voidaan suojautua. Päivitys on mahdollisuuksien mukaan automaattinen.

h) Käyttäjien työasemissa käytetään tarpeen mukaan verkkosensuuriohjelmistoja, joilla estetään käyttäjien pääsy mahdollisesti vaarallisille sivustoille (esimerkiksi uhkapeli, aikuisviihde ja tekijänoikeuksia rikkovat viihde- tai musiikkipalvelut).

i) Kaikista tiedoista otetaan säännöllisesti varmuuskopiot riittävän usein. Varmuuskopiointi on kuvattu tarkemmin kappaleessa *varmistukset ja palautukset*. Työasemissa olevat tiedot varmistetaan tarpeen mukaan. Työasemissa ei ole suositeltavaa säilyttää kriittisiä tietoja.

j) Virusten, muiden haittaohjelmien ja verkkohyökkäysten esiintymistä seurataan ja niistä raportoidaan.

k) Käyttäjien vastaanottamien sähköpostien sisältö ja liitetiedostot tarkastetaan automaattisesti virusten ja muiden haittaohjelmien varalta jo vastaanotettaessa viestejä sähköpostijärjestelmään.

l) Tietoturvallisuutta vaarantavista haittaohjelmista ja verkkohyökkäyksistä on olemassa vastuutettu toimintasuunnitelma, jota noudatetaan kaikissa havaituissa ja aiheelliseksi katsotuissa tilanteissa. Toimintasuunnitelma kattaa suojautumisen haitoilta ja paluun normaalitilaan, mikäli esimerkiksi tietojärjestelmiä tai tietoliikenneyhteyksiä joudutaan sulkemaan väliaikaisesti.

m) Toimintaohjeita uudistetaan tarvittaessa havaittujen ongelmatilanteiden (oma organisaatio tai esimerkiksi tiedot muista organisaatioista) perusteella.

n) Organisaation kannalta kriittinen ja tärkeätä tietoa sisältävä tietoverkko suojataan ulkoisista verkoista ja vähintäänkin eristetään riittävän tasoisilla palomuuri- ja verkkohyökkäyksen tunnistusohjelmistoilla (IDS).

o) Palomuuriohjelmistoilla estetään kaiken tarpeettoman tietoliikenteen pääsy ja riskialttiiden tietoliikenneprotokollien käyttö (esimerkiksi *ftp, rlogin* ja *rsh*) organisaation tietoverkon ja ulkoisen verkon välillä.

p) Hyökkäyksen tunnistusohjelmistoa ja suojautumisohjelmistoa (IPS, *intrusion protection software*) käytetään ainakin tunnetuilta hyökkäystavoilta, kuten palvelunestohyökkäyksiltä ja erilaisilta puskurien ylivuotohyökkäyksiltä suojautumiseen ja hyökkäysten analysointiin. Hyökkäyksestä analysoidaan esimerkiksi lähde ja kohde, hyökkäysmenetelmä ja hyökkäyksen status (kellonajat ja laajuus). Ohjelmisto päivitetään säännöllisesti uusimpaan versioon.

q) Vakavista verkkohyökkäyksistä suoritetaan hälytys ylläpitohenkilökunnalle. Tarvittaessa käytetään kaksinkertaisia, eri ohjelmistovalmistajien tekemiä palomuuri- ja IDS-ohjelmistoja.

r) Kriittisiä tietoja sisältävien järjestelmien tietojen eheyttä tarkkaillaan, ja mahdolliset muutokset eheydessä (esimerkiksi muuttuneet tai väärät tarkastussummat ja tiivisteet) käynnistävät tarkemmat tutkimukset.

s) Organisaation verkkoon ei sallita ulkopuolisten, esimerkiksi vierailijoiden työasemien kytkemistä. Tällaisia työasemia varten rakennetaan erilliset yhteydet, jotka on tarvittaessa otettavissa käyttöön. Esimerkiksi neuvottelutiloihin voidaan rakentaa kiinteästi ulkoiseen Internetiin kytkettyjä yhteyksiä.

## A6.8 Kryptografia ja PKI

### kontrolli

Kryptografiaa ja julkisen avaimen menetelmän käyttö on arvioitava ja menetelmät otettava aina tarvittaessa käyttöön, kun tietojen eheys, luottamuksellisuus, alkuperä ja alkuperäisyys on oltava taattu. Myös silloin, kun tietoja käyttävät henkilöt pitää todentaa varmuudella, täytyy arvioida tarjolla olevien julkisen avaimen menetelmien käyttö. Tämä aihe on tarkemmin kuvattu luvussa *pääsynhallinta*.

Alla olevat käytännön ohjeet sisältävät esimerkkejä, joissa kryptografiaa ja PKI:ta voidaan hyödyntää. Menetelmien käyttö täytyy arvioida tapaus- ja tietojärjestelmäkohtaisesti, kun määritellään eri tietojärjestelmien tietojen suojaaminen ja käyttäjien todentaminen.

## käytännön ohjeita

a) Verkkopalveluiden ja -palvelinten vahvaksi todentamiseksi hankitaan palvelinvarmenne tarvittaessa kaikkiin verkkopalveluihin. Palvelinvarmenne takaa, että loppukäyttäjä voi luottaa palvelimen kuuluvan organisaatiolle, jolle palvelinvarmenne on myönnetty. Lisäksi selaimen ja palvelimen välinen tietoliikenne voidaan salata ja siirrettyjen tietojen luottamuksellisuus säilyy.

b) Palveluita tai tietojärjestelmiä käyttäville henkilöille voidaan myöntää varmenne (tai voidaan käyttää hänelle myönnettyä varmennetta), jonka avulla henkilö voidaan todentaa luotettavasti. Tällöin hänelle voidaan myöntää käyttövaltuudet juuri oikeisiin tietoihin ja tietojärjestelmiin.

c) Tietojärjestelmiin tallennettavat tiedot voidaan allekirjoittaa sähköisesti tallentavan henkilön toimesta (esimerkiksi käyttämällä toimikortilla olevaa salaista avainta), jolloin tietojen myöhempi väärentäminen tai muuttuminen vahingossa ei ole mahdollista. Sähköisellä allekirjoituksella taataan myös tietojen alkuperä: tekijä ei voi kiistää, että tiedot olisivat häneltä peräisin.

d) Kaikkiin käytettäviin ohjelmistoihin pyritään liittämään tekijän (esimerkiksi ohjelmistotoimittaja tai alihankkija) sähköinen allekirjoitus, jolloin voidaan estää ohjelmiston tahallinen vaihtaminen toiseksi.

e) Henkilöiden todentamisessa ja sähköisessä allekirjoituksessa käytettävät varmenteet hyväksytään tapauskohtaisesti. Varmenteiden luotettavuus perustuu varmentajan noudattamaan varmennepolitiikkaan. Ennen kuin tietyn varmentajan myöntämiä varmenteita hyväksytään todentamisen välineiksi, kyseisen varmennepolitiikan käyttökelpoisuus organisaatiossa arvioidaan.

f) Kryptografian käyttö tietojen luottamuksellisuuden suojaamisessa ja salauksessa arvioidaan ja tarvittavat menetelmät otetaan käyttöön. Tietojen salauksella tiedot suojataan niiltä työntekijöiltä, joilla ei ole oikeutta lukea tietoja, mutta joilla on siihen halu tai mahdollisuus (uteliaisuus, järjestelmänhoitajat, epäluotettavat henkilöt) sekä kaikilta ulkopuolisilta (verkkomurtautumiset, tietoliikenteen kuuntelu, pääsy organisaation tiloissa oleviin tietojärjestelmiin).

g) Organisaatio käyttää olemassa olevan varmentajan palveluita tai perustaa itse varmentajan, joka myöntää ja hallinnoi käyttäjien tarvitsemia varmenteita sekä tuottaa hakemisto- ja muita tarvittavia palveluita.

h) Käyttäjien rekisteröinti (tunnistaminen, todentaminen sekä avainten, tunnuslukujen ja varmenteiden luonti ja luovutus), rekisteröinnissä käytettävät menetelmät ja turvallisuustaso on sovitettava siihen turvallisuustasoon, mikä koskee tietoja ja niiden käsittelyä. On huomattava, että käytettäessä julkista varmentajaa (jonkun muun organisaation toimiessa varmentajana), organisaatiolla ei välttämättä ole mahdollisuutta tunnistaa ja todentaa käyttäjiksi rekisteröitäviä henkilöitä itse.

i) Avainten mahdollista varmuuskopiointia varten luodaan tarvittavat menetelmät. Varmuuskopioita säilytetään sellaisessa paikassa, ja niiden käyttöön on oltava tarkkaan määritellyt proseduurit ja valtuudet, että vain etukäteen sovitussa kriisitilanteessa varmuuskopio voi olla käytettävissä varsinaisen avaimen sijasta.

j) Avaintenhallintamenetelmien yhteydessä huolehditaan, että käyttäjien salausavaimesta (salauksen purkuavain) otetaan tarvittavat varmuuskopiot, jotta salattuja tietoja ei menetetä avaimen vioittuessa tai hukkuessa. Tiedon salattuna säilyttämisen ja selkokielisen säilyttämisen uhkat ja riskit analysoidaan ja tiedon säilyttämisen menetelmistä valitaan "pienempi paha". Selkokielisenä säilyttäminen saattaa vaarantaa säilytettävien tietojen luottamuksellisuuden. Tietojen säilyttäminen salattuna parantaa luottamuksellisuutta: se estää salakuuntelun ja

tietoihin pääsyn sellaisilta ulkopuolisilta, joilla ei ole tarvittavaa salauksen purkuavainta. Toisaalta salattuna säilyttäminen edellyttää, että salauksen purkuavaimesta on olemassa sellainen kopio, että avaimen (tai esimerkiksi toimikortin) vioittuminen ei estä tietojen lukua.

k) Käytettävät kryptografiset menetelmät ovat riittävän vahvoja käsiteltävien tietojen suojataso huomioon ottaen. Kryptografiset menetelmät (esimerkiksi allekirjoitus-, salaus- ja tiivistefunktiot) ovat vaihdettavissa toisiksi kohtuullisella työllä, koska tietokoneiden laskentatehon kasvaessa ja purkualgoritmien parantuessa käytetyt menetelmät voivat vanhentua ja muodostaa täten tietoturvariskin.

l) Jos organisaatio myöntää ja julkaisee itse varmenteet (esimerkiksi rekisteröi henkilöt, luo avainparit, jakaa toimikortit, ylläpitää hakemistoa ym.), organisaatio luo käyttöönsä soveltuvan varmennepolitiikan. Yleissääntönä voidaan pitää, että myönnetyt varmenteet sisältävät mahdollisimman vähän muuttuvaa tietoa ja että varmenteiden voimassaoloaika on riittävän rajoitettu, muttei silti organisaation toimintaa liikaa rajoittava. Liian lyhyt voimassaoloaika voi aiheuttaa ongelmia varmenteiden uusimismenettelyissä, kun taas liian pitkä voimassaoloaika tuo turvallisuusriskin avainten paljastumiselle. Dokumentissa *CIHI/ICIS: 2001 Model Digital Signature and Confidentiality Certificate Policies for Health Public Key Infrastructure* on suosituksia varmennepolitiikalle. Tämän dokumentin kanssa yhteneviin Väestörekisterikeskuksen varmentamiseen liittyviin dokumentteihin (katso luku *standardeja ja kirjallisuutta*) kannattaa myös tutustua.

m) Organisaatio voi myös halutessaan tarjota myöntämiään varmenteita ja myöntämismenettelyitä (esimerkiksi käyttäjien rekisteröinti ja hakemistopalvelut) muiden organisaatioiden käyttöön ja sopia tästä organisaatiokohtaisesti. Tällä voidaan luoda mahdollisuuksia organisaatioiden väliseen turvalliseen yhteistyöhön.

n) Perusteet organisaation oman varmentajan perustamisen tarpeelle arvioidaan. Perusteita voivat olla esimerkiksi

- erityiset turvallisuusvaatimukset, joita ei ole tarjolla olemassa olevilla varmentajilla ja PKI-palveluiden tuottajilla (esimerkiksi avainten varmuuskopiointimenetelmät, ei-julkisen hakemiston käyttö, sekä käyttäjien palvelut, kuten rekisteröinti, toimikorttien, avainten ja PIN-koodien jakelu ja varmenteiden mitätöinti)
- laajennettavuus-, skaalautuvuus- ja muunnettavuusvaatimukset (erityisen suuri tai suorituskykyinen ympäristö tai toiminnaltaan rajoitettu ympäristö) sekä hoitoon liittyvät vaatimukset, kun järjestelmään tehdään muutoksia tulevia tarpeita varten *("future needs")*
- yhteistoimintamahdollisuus muiden PKI-toimijoiden kanssa (muut varmentajat, muut organisaatiot, jotka eivät käytä julkisia varmennepalveluita sekä erilaisten ulkoisten palveluiden, kuten hakemisto-, aikaleima- ja verkkonotaaripalveluiden tuottajat)
- tekniset ja teknologiset vaatimukset (erityiset client-ohjelmistot, kryptologiset algoritmit, avainten pituus- ja laatuvaatimukset, varmenteiden tietosisältöön, käyttötarkoitukseen ja voimassaoloon liittyvät vaatimukset, tarve biometrian tai mobiililaitteiden käyttöön sekä vaatimukset käytettäville varmennemedioille, kuten toimikorteille tai USB-avaimille).

## A6.9 Varmistukset ja palautukset

### kontrolli

Erilaisia vikatilanteita varten tietojärjestelmistä on otettava varmistukset, joilla voidaan tarpeen mukaan palautua vikaa edeltäneeseen tilanteeseen. Varmistustoimet ovat mahdollisuuksien mukaan automatisoituja, mutta palautustoimissa noudatetaan aina etukäteen sovittuja proseduureja ja hyväksymismenettelyitä. Vikatilanteita voivat olla esimerkiksi laitteiden ja levyjen vikaantumiset, tietojen tahaton korruptoituminen ohjelmisto- tai tietoliikennevirheiden vuoksi sekä käyttäjien tekemät tahattomat tiedostojen poistot tai ylikirjoitukset.

a) Kaikkien tietojen osalta arvioidaan varmistustarve. Tietojen varmistuksessa otetaan huomioon tietojen tärkeys ja turvaluokitus.

b) Kunkin tiedon ja tietojärjestelmän osalta luodaan varmistuskäytäntö, joka määrittelee varmuuskopioinnin menettelyt, vastuut, määräajat ja aikataulut, varmuuskopioiden merkinnän, säilytyksen ja tuhoamisen, toimivuuden testauksen ja menettelytavat palautustilanteessa.

c) Varmistusprosessissa kirjataan esimerkiksi, mitkä tiedot on varmuuskopioitu, mille ja millaiselle tietovälineelle, miten tieto(väline) on merkitty ja missä tietoväline fyysisesti sijaitsee.

d) Varmistuksissa käytetään asianmukaisia ja riittävän turvallisia järjestelmiä, laitteistoja ja tietovälineitä. Organisaatiossa voi olla käytössä useita erilaisia varmistusmenettelyitä erityyppisten järjestelmien ja tietojen varmuuskopiointiin, esimerkiksi varmistuksiin käytettäviä levyjärjestelmiä (online-varmistukset), tietokantojen reaaliaikaisia eheydenvarmistusmenettelyitä (backlog), nauhavarmistuksia ja varmuuskopiointia tietoverkon yli. Myös erillisten yksittäisten tiedostojen ja tietojen varmuuskopiointi saattaa olla soveltuva menetelmä.

e) Myös käyttäjien työasemien varmistuksista on huolehdittu. Kaikkien työasemille tallennettavien tietojen varmistustarve on tiedossa ja varmistusten otto on suunniteltu varmistustarpeen mukaiseksi.

f) Käytetyistä ohjelmistoista ja käyttöjärjestelmistä on olemassa toimivat varmuuskopiot.

g) Järjestelmä- ja ohjelmistoparametreista ja muista asetuksista otetaan varmuuskopiot. Varmistusmenettely on riittävän tiheä ja aina tarvittaessa reaaliaikainen, etteivät esimerkiksi päivän aikana tehdyt muutokset asetuksiin tai konfiguraatioihin pyyhkiydy mahdollisessa varmistusten palautustilanteessa (ettei palautettavia tietoja ylikirjoiteta uudempien määrittelyiden päälle). Palautusprosessi suunnitellaan siten, että palautusten yhteydessä järjestelmien ja ohjelmistojen konfiguroinnissa ei tarvitse tehdä turhaa tai ylimääräistä työtä.

h) Tietokantojen varmistuksissa hyödynnetään olemassa olevia tietokantatyökaluja ja menetelmiä.

i) Tiedostojen nimeämisessä käytetään versionumerointia, jotta vahingossa tapahtuvalta ylikirjoitukselta vältytään. Versionumeroinnin käytöstä laaditaan ohjeistus.

j) Tietojärjestelmistä on olemassa riittävän tuore varmistuskopio fyysisessä paikassa, joka on riittävän etäällä tietojärjestelmistä. Tällä estetään esimerkiksi tulipalon tai vesivahingon yhteydessä tapahtuva sekä tietojärjestelmien että varmistuskopioiden yhtaikainen tuhoutuminen.

k) Suojattavia tietoja (esimerkiksi henkilö- ja potilastietoja) sisältävät varmuuskopiot ja tietovälineet suojataan vähintään samantasoisesti kuin varsinaisia tietoja sisältävät tietojärjestelmät.

l) Selvitetään, voidaanko tietojen varmistamisessa käyttää kryptografiaa ja varmuuskopiot säilyttää salattuina. Mahdolliset menetelmät arvioidaan ja valittujen salausperiaatteiden toteuttamiseksi käytetään tarvittavia teknisiä ja hallinnollisia toimia.

m) Varmistusten toimivuus testataan säännöllisesti, jotta voidaan luottaa sekä varmistusmenettelyiden, prosessien, laitteistojen että tietovälineiden toimintaan mahdollisessa palautustilanteessa. Palautustestauksen yhteydessä myös mahdolliset aikavaatimukset testataan, erityisesti palautettaessa koko tietojärjestelmä. Palautusprosessissa huomioidaan, että käyttöjärjestelmän ja ohjelmistojen, tietokantojen ja päivittäisten varmistuskopioiden palauttaminen saattaa kestää pahimmillaan tietojärjestelmän koosta, käytetyistä laitteistoista, verkoista ja tietovälineistä riippuen tunteja tai jopa vuorokausia.

n) Kunkin yksittäisen tietojärjestelmän varmistuspolitiikka laaditaan siten, että se täyttää toiminnan jatkuvuudelle asetetut vaatimukset. Näitä vaatimuksia on luvussa *toiminnan jatkuvuus*.

o) Automaattisten varmistusten onnistumista seurataan ja se integroidaan mahdollisuuksien mukaan automaattisiin hälytysjärjestelmiin, joilla tietojärjestelmien vastuuhenkilöt seuraavat järjestelmien tilaa ja toimintakuntoa.

## kontrolli

Tietovälineiden, kuten asiakirjojen ja dokumenttien, nauhojen, cd-levyjen, levykkeiden, USB-muistien ja muiden tietokoneisiin liitettävien medioiden sekä järjestelmädokumentaation täytyy olla suojattu asianmukaisesti katoamiselta ja varkauksilta, valtuudettomalta pääsyltä ja valtuudettomalta muuttamiselta. Erityisesti arkaluonteisia tietoja sisältävät tietovälineet on suojattava; näitä tietoja sisältävät tietovälineet on suojattava vähintään sen tasoisesti kuin tietojen turvaluokitus edellyttää ja tietovälineiden käytöstä on oltava yksityiskohtainen ohjeistus.

Tietovälineiden, erityisesti siirrettävien tietovälineiden (paperi, levykkeet, cd-levyt, USB-muistit) käytölle on oltava ohjeistus eivätkä tällaisille tietovälineille talletetut suojattavat tiedot saa prosessin missään vaiheessa vaarantua. Tästä aiheesta on mainittu lisää luvussa *fyysisen ympäristön turvallisuus*. Luvun *omaisuuden hallinta* kappaleessa *merkitseminen* on vaatimuksia tietovälineiden merkitsemiseen liittyen.

## käytännön ohjeita

a) Tietovälineiden hallintaan, käyttöön ja käsittelyyn luodaan toimintatavat ja tarkka käytännön ohjeistus.

b) Tietovälineiden käytöstä pidetään kirjaa, josta selviää riittävän tarkasti tietovälineiden käyttö ja tuhoaminen.

c) Arkaluonteisia tietoja sisältävien tietovälineiden käyttö ohjeistetaan yksityiskohtaisesti erityistä huolellisuutta noudattaen. Arkaluonteisten tietojen tallettaminen siirrettäville tietovälineille (cd-levyt, levykkeet, paperi, USB-muistit) kirjataan.

d) Jos tietoja tallennetaan väliaikaista säilytystä varten siirrettävälle tai kertakäyttöiselle tietovälineelle, ja tältä tietovälineeltä tiedot siirretään myöhemmin tuotannolliseen tietojärjestelmään, varmistutaan erityistä huolellisuutta noudattaen sekä siirtoprosessin onnistumisesta ja oikeellisuudesta että siirrettävien tietojen eheydestä ja oikeellisuudesta.

e) Tarvittaessa ja mahdollisuuksien mukaan tietovälineiden sisältöä ja kiertoa seurataan (tietovälineen fyysinen sijainti, kenellä hallussa, kuka on vastuussa tuhoamisesta sekä milloin ja miten tuhoaminen tapahtuu).

f) Pääsääntöisesti pyritään siihen, että arkaluonteisia tietoja ei tallenneta tai tulosteta siirrettävälle tai kertakäyttöisille tietovälineille ilman erityistä tarvetta, koska tällaisten tietovälineiden hallinta on teknisesti vaikeaa tai jopa mahdotonta, ja tietoturva on täten poikkeuksellisen altis vaarantumiselle.

g) Tuhottaessa tietovälineitä noudatetaan aina ennalta sovittuja proseduureja, joilla varmistetaan, etteivät tiedot voi tuhoamisprosessissa joutua valtuudettoman osapuolen haltuun. Luvun *fyysisen ympäristön turvallisuus* kappaleessa *tietojen, tietovälineiden ja laitteiden poisto* on tarkempia vaatimuksia tietovälineiden tuhoamiseen liittyen.

h) Tietovälineitä käsitellään ja käytetään ainoastaan valmistajan ohjeiden ja suositusten mukaisesti.

i) Tietovälineitä säilytetään siten, että niiden sisältämät tiedot eivät vaarannu. Esimerkiksi ohjeessa "*clean desk policy*", josta on mainittu esimerkiksi luvussa *fyysisen ympäristön turvallisuus*, voidaan määritellä suositeltavat tai pakolliset tavat tietovälineiden oikeaan säilytykseen.

j) Järjestelmädokumentaatiota, prosessikuvauksia ja vastaavia asiakirjoja säilytetään ja käytetään siten, että valtuudettomilla henkilöillä ei ole pääsyä dokumentaatioon. Järjestelmien ja prosessien vastuuhenkilöt myöntävät valtuudet dokumentaation käyttöön vain niille, jotka dokumentaatiota välttämättä tarvitsevat. Väärän henkilön käsissä oleva dokumentaatio voi vaarantaa tietojärjestelmän turvallisuuden.

## kontrolli

Sekä organisaation sisäinen että organisaatiosta ulos tehtävä tietojen välitys on oltava asianmukaisesti suojattua. Tietojen välitykseen on määritettävä politiikat ja menettelyt, joita on kaikissa tilanteissa noudatettava. Käytettävien menettelyiden noudattamista täytyy edellyttää myös kolmansilta osapuolilta. Tarvittaessa tämä voidaan vahvistaa sopimuksellisesti. Erityisesti arkaluonteisten tietojen välityksessä (esimerkiksi henkilötiedot ja potilastiedot) on noudatettava erityistä varovaisuutta, ja tästä on oltava erillinen ohjeistus. Tietojen välityksestä ja luovutuksesta sekä lokitietojen tallentamisesta säädetyt lait on otettava huomioon kaikissa tilanteissa.

Erityisesti julkiseksi määritellyn tiedon ja sen julkaisemisen – esimerkiksi organisaation verkkosivuilla – politiikkojen ja käytäntöjen on oltava tarkoin määritellyt, ettei luottamuksellista tietoa joudu vääränlaisen julkaisemismenettelyn johdosta asiattomiin käsiin ja ettei virallisena julkaistuja tietoja voida asiattomasti muuttaa vääriksi.

Organisaation henkilöiden käyttämien organisaation ulkopuolisten verkkopalveluiden (esimerkiksi ulkoiset verkkosivustot, sähköpostit, verkkopankit ja muut verkkopalvelut) käytöstä on oltava politiikka ja ohjeistus. Tästä on tarkempi kuvaus kappaleessa *käyttäjien velvollisuudet: tietoturvaohjeistuksen laadinta käyttäjille*. Organisaation tietoverkkoihin ja puhelinliikenteeseen sekä esimerkiksi henkilöiden etäyhteyksien käyttöön liittyen löytyy lisää toimenpidesuosituksia myös luvusta *fyysisen ympäristön turvallisuus*.

## käytännön ohjeita

a) Tiedonvälitystä koskevat politiikat, menettelytavat ja ohjeet ottavat huomioon kaikki erilaiset tiedonvälityskeinot sähköisistä menettelyistä (kuten sähköposti, verkkosivut ja verkotetut tuotantokäytössä olevat tietojärjestelmät) fyysisiin menettelyihin (paperimuotoiset asiakirjat, telefaxit, suullinen viestintä ym.). Yleisimpiä tiedonvälitystapoja varten laaditaan oma, yksityiskohtainen ohjeistus, esimerkiksi "sähköpostiohje" ja "ulkoisten verkkopalveluiden käyttöohje".

b) Kaikki organisaation verkkopalvelut ja tietoliikennemenetelmät pyritään suojaamaan palvelunestohyökkäyksiltä *(DoS, denial of service*). Hyökkäyksiin varaudutaan riittävillä hyökkäyksentunnistusmenetelmillä, kapasiteetin varauksella ja varayhteyksien käytöllä. Tarvittaessa sisäinen tietoliikenne voidaan eristää ulkopuolisesta, ja kriittiset yhteydet muihin organisaatioihin voidaan reitittää omiin tiedonsiirtokanaviin.

c) Organisaation sisäinen tietoliikenne ja palvelut suojataan asianmukaisesti. Esimerkiksi Intranet-sivustoihin tai verkkokalentereihin ei päästetä ulkopuolisia. Oman organisaation henkilöt tunnistetaan ja todennetaan luotettavaa menetelmää käyttäen. Tunnistamiseen ja todentamiseen käytetyistä menetelmistä on tarkemmin mainittu luvussa pääsynhallinta. Ulkopuolisille henkilöille, esimerkiksi yhteistyökumppaneiden, alihankkijoiden ja asiakasorganisaatioiden henkilöille pyritään käyttämään samoja todennusmenetelmiä kuin oman organisaation henkilöille.

*d)* Organisaation sisäisessä käytössä oleva, mutta ulkoisia tietoliikenneyhteyksiä käyttävä, verkko (*extranet*) suojataan asianmukaisesti esimerkiksi VPN-yhteyksillä (*virtual private network*).

e) Kielletään vaaralliset tai haitalliset verkkoyhteydet ja palvelut, kuten vertaisverkot (*p2p, peer-to-peer*). Jos tällaisia palveluita tarvitaan, niitä varten suositellaan perustettavaksi oma verkko, johon ei kytketä tuotannollisen tietoliikenneverkon työasemia ja jonka työasemia ei kytketä tuotannolliseen verkkoon.

f) Organisaatiosta toiseen organisaatioon tapahtuvaa tietojen siirtoa varten käytettävistä menettelyistä sovitaan tarvittaessa kirjallisesti organisaatioiden välillä. Sopimuksissa määritellään esimerkiksi käytettävät tiedonsiirto- ja suojausmenetelmät, teknologiat ja tekniset standardit, viestien kuittaukset, vastaanottotiedotukset ja jäljitettävyys, omistus ja valtuudet sekä vastuut

ja hallinnointimenettelyt. Viimeiset sisältävät myös menettelytavat ongelma- ja vikatilanteita varten. Tarvittaessa myös kryptografian käytöstä sovitaan tietojen suojauksen ja henkilöiden todentamisen yhteydessä. Tekninen toteutus ja noudatettavat käytännöt voidaan kuvata esimerkiksi varmennepolitiikassa.

g) Tietojen siirron yhteydessä kommunikoivat osapuolet tunnistetaan ja todennetaan riittävän vahvasti. Todennuksen taso voi määräytyä esimerkiksi siirrettävien tietojen kriittisyyden tai luottamuksellisuuden perusteella. Myös silloin, kun siirrettävät tiedot ovat esimerkiksi lasku-, maksu- tai luottotietoja, osapuolten välinen todentaminen ja siirrettävien tietojen eheys varmistetaan erityisellä huolellisuudella.

h) Käytettävien tietojenvälityskanavien uhkat analysoidaan ja mahdollisuudet esimerkiksi salakuunteluun, kopiointiin, varastamiseen (esimerkiksi muuttamalla viestien kohdeosoite) välitettävien tietojen valtuudettomaan muuttamiseen tai tietojen tuhoamiseen tai tuhoutumiseen kartoitetaan.

i) Organisaation viestinnässä käytettävät tietojärjestelmät suojataan. Verkkopalvelut, sähköpostipalvelut ja tuotannolliset verkossa olevat tietojärjestelmät (esimerkiksi potilastietojärjestelmät) suojataan siten, että ulkopuolisilla ei ole mahdollisuuksia lukea tietoja, joihin he eivät ole valtuutettuja. Järjestelmistä lähetettävät viestit menevät oikeisiin kohteisiin ja niihin vastaanotettuja viestejä pääsevät lukemaan vain ne henkilöt, keille viestit on tarkoitettu.

j) Tuotannollisten tietojärjestelmien välinen tiedonsiirto (esimerkiksi potilastietojärjestelmästä tapahtuva tietojen siirto tai vastaanotto toisen organisaation vastaavaan järjestelmään) suojataan riittävillä menetelmillä. Kaikki tietoliikenneyhteydet jotka perustuvat julkisen verkon käyttöön tulee salata (esimerkiksi ssl, https), ja järjestelmät tunnistavat ja todentavat toisensa luotettavasti (esimerkiksi käyttämällä palvelinvarmenteita). Tietoliikenteessä käytetään standardiprotokollia ja järjestelmien väliset rajapinnat on mahdollisuuksien mukaan standardoitu ja dokumentoitu.

k) Tietojen siirrossa käytettävät fyysiset tietovälineet suojataan asianmukaisesti ja siirtomenetelmänä käytetään vain luotettavia menettelyitä ja palveluita. Lähetettävän tiedon kriittisyydestä ja turvatasosta riippuen voidaan turvautua esimerkiksi postiin, kirjattuun postiin tai kuriiripalveluihin. Luotettavista palveluntarjoajista, joiden palveluita on sallittua käyttää, laaditaan tarvittaessa lista. Kuriiri todennetaan ennen tietojen luovuttamista kuljetukseen.

l) Fyysisesti lähetettävä materiaali on aina syytä sinetöidä ja käyttää tarvittaessa lukittavia tai muutoin luotettavasti suljettavia pakkauksia. Pakkauksista voidaan selvittää, onko niitä murrettu tai yritetty murtaa kuljetuksen aikana. Tietovälineet pakataan siten, että ne eivät vahingoitu fyysisesti kuljetuksen aikana. Jos tietovälineenä käytetään esimerkiksi cd-levyä tai levykettä, kaikki lähetettävät tiedot on syytä salata tarpeen mukaan. Salausavain voidaan toimittaa vastaanottajalle käyttäen eri lähetystapaa, esimerkiksi sähköpostia, telefaxia tai tekstiviestiä.

m) Sähköinen tiedonvälitys suojataan haittaohjelmilta, joita tietoliikenteen yhteydessä voi siirtyä organisaatioon.

n) Tiedonvälitys piilossa olevia kanavia pitkin estetään. Näiden olemassaolon estäminen jo tietojärjestelmien kehitysvaiheessa pyritään estämään. Tämä on tarkemmin kuvattu luvussa tietojärjestelmien kehitys ja ylläpito.

o) Organisaatiosta ulos välitettävien tietojen alkuperäisyys ja muuttumattomuus varmistetaan riittävillä menetelmillä, esimerkiksi allekirjoittamalla tiedot ja asiakirjat sähköisesti. Verkkosivujen aitous voidaan varmentaa käyttämällä palvelinvarmennetta, jolloin myös verkkosivun ja organisaation ulkopuolella käytettävän verkkoselaimen välinen tietoliikenne voidaan salata.

p) Laaditaan menettelyt ja ohjeet niiden viestien tarkemmaksi tutkimiseksi, joiden alkuperäisyyttä ei voida selvittää.

q) Lähetettäessä arkaluonteisia tietoja organisaatiosta ulos noudatetaan riittävää huolellisuutta kohdeosoitteen kirjaamisessa. Tarpeen mukaan käytetään automaattista osoitteen tarkastusta osoitekirjasta (esimerkiksi käytettäessä sähköpostia). Käytettäessä ennalta määrättyjä lyhyt-

valintoja lähetettäessä viesti telefaxilla on varmistuttava, että lyhytvalintanumero osoittaa oikeaan ulkoiseen numeroon. On myös varmistuttava, että lähetetty viesti ei jää telefax-laitteen muistiin.

r) Tietojen yleiseen jakeluun tai yleisiin medioihin julkaisemista varten on olemassa ennalta sovitut käytännöt ja virallinen menettelytapa. On selkeästi sovittu, ketkä ovat oikeutettuja julkaisemaan tietoja organisaatiosta. Esimerkiksi verkkosivujen ylläpito, päivitys ja uutisten julkaiseminen ovat ennalta sovittuja ja vastuutettuja prosesseja. Kaikkien julkaistavien tietojen lainmukaisuus tarkastetaan ja tiedot hyväksytään julkaistavaksi sovitulla menettelyllä. Vanhentuneet tiedot poistetaan asianmukaisesti.

s) Sähköisesti, esimerkiksi verkkosivuilla, julkaistavat tiedot suojataan asianmukaisesti. Palvelimen luotettavassa todennuksessa käytetään palvelinvarmennetta. Julkaistavat tiedot voidaan tarvittaessa allekirjoittaa sähköisesti. Henkilöt, jotka ovat oikeutettuja kirjoittamaan tietoja sähköisiin julkaisujärjestelmiin, tunnistetaan ja todennetaan riittävän luotettavalla menetelmällä.

# 9 Pääsynhallinta

## 9.1 Yleistä

Yksi tietoturvallisuuden oleellisimmista osa-alueista on pääsynhallintaan liittyvät määrittelyt ja toimenpiteet – kuinka tietojärjestelmien ja niissä olevien tietojen käyttö ja käyttäjät määritellään, kuinka käyttöoikeuksia ja käyttövaltuuksia hallitaan ja millaisilla menetelmillä käyttäjät tunnistetaan ja heidän henkilöllisyytensä todennetaan.

Useissa muissa tämän ohjeen luvuissa sivutaan käyttäjien määrittelyyn, oikeuksien ja valtuuksien määrittelyyn, käyttäjien todennukseen ja hallinnointiin liittyviä asioita, mutta tässä luvussa pääasiat on tiivistetty kolmeen kokonaisuuteen.

Ensimmäinen kokonaisuus käsittää pääsyn hallinnoinnin: millaisia politiikkoja, sääntöjä ja käytäntöjä hallinnointiin on käytettävissä ja käytettävä. Hallinnointi käsittää esimerkiksi oikeuksien määrittelyn: millaisia pääsyoikeuksia tietoihin luodaan ja millaisia oikeuksia voidaan valtuuttaa erityyppisille käyttäjille ja käyttäjäryhmille. Osa hallinnointia on valvonnan ja seurannan menettelytavat, joihin liittyvät määrittelyt on kuitenkin tarkemmin kuvattu luvussa *poikkeustilanteet*, joka sisältää käyttäjien toiminnan lisäksi myös muiden tietojärjestelmien käyttöön liittyvien suureiden seurannan ja valvonnan.

Toinen kokonaisuus, käyttäjänhallinta, sisältää määritykset käyttäjien hallintaan liittyen: kuinka ja millä menetelmillä tietojärjestelmien käyttäjät rekisteröidään ja millaista rekisteriä käyttäjistä pidetään, millaisia ominaisuuksia kustakin käyttäjästä kirjataan (esimerkiksi käyttäjälle myönnettävän varmenteen attribuuteiksi) ja kuinka hallinnoidaan sitä, että kukin käyttäjä saa nimenomaan hänelle kuuluvat käyttövaltuudet tietoihin. Lisäksi luonnollisesti käyttäjien ja käyttövaltuuksien poistaminen on osa käyttäjien hallinnointia.

Kolmas kokonaisuus käsittää käyttäjien tunnistamisen ja todentamisen. Hyväksytyt menettelytavat ja ratkaisut erilaisten käyttäjien todennusmenetelmien käytölle määritellään, tarvittaessa kunkin turvatason tiedoille erikseen. Tiettyihin järjestelmiin voidaan esimerkiksi hyväksyä käyttäjätunnus-salasanamenettelyn käyttö, kun taas pääsy tiettyihin järjestelmiin voidaan valtuuttaa vain käyttäjien vahvalla tunnistamisella ja toimikortin käytöllä. Myös määrättyjen ja tietoturvallisesti vaarallisten menetelmien käyttökiellot mainitaan, esimerkkinä jaettujen osastokohtaisten käyttäjätunnusten ja salasanojen käyttökielto.

## 9.2 Uhkista ja riskeistä

Tehokkaalla ja hyvin määritellyllä pääsynhallinnalla sekä asianmukaisella käyttäjien ja heille myönnettävien valtuuksien hallinnoinnilla voidaan tehokkaasti ehkäistä niitä uhkia, joita syntyy valtuudettomasta tietoihin pääsystä. Sellaisten henkilöiden päästessä käsiksi tietoihin ja tietojärjestelmiin, jotka eivät ole niihin valtuutettuja, voi tietojen luottamuksellisuuden menetyksen lisäksi aiheutua vakavia uhkia myös tietojen olemassaololle ja oikeellisuudelle. Alla on lueteltuna vain muutamia esimerkkejä uhkista.

a) Tietojärjestelmiä pääsee käyttämään sellaiset henkilöt, joilla ei ole valtuuksia tietoihin eikä tietojärjestelmiin.
b) Tietojärjestelmien käyttäjillä on pääsy sellaisiin tietoihin tai järjestelmäresursseihin, joihin heillä ei ole valtuuksia.
c) Käyttäjiä ei tunnisteta rekisteröintiprosessissa henkilökohtaisesti.
d) Rekisteröintiprosessissa käyttäjälle ei selvitetä hänen tietojenkäsittelyoikeuksiaan. Hän ei joudu allekirjoittamaan vastaanottaneensa oikeudet ja ymmärtävänsä vastuutaan tietojen suojaamisesta.

e) Tietojärjestelmissä on käyttövaltuuksia sellaisilla henkilöillä, jotka ovat jo poistuneet organisaatiosta.
f) Tietojärjestelmien käyttäjistä ei ole rekisteriä.
g) Myönnetyistä valtuuksista ei ole rekisteriä.
h) Valtuuksien myöntöprosessissa ei tietojen omistajalta varmisteta, että henkilölle voidaan myöntää kyseiset käyttöoikeudet tietoihin.
i) Käyttäjätunnusten ja erityisesti laajoilla valtuuksilla olevien tunnusten käyttöä ei seurata.
j) Käyttäjille on myönnetty oikeuksia käyttöjärjestelmien tai tietokantojen oletusprofiilien mukaisesti.
k) Järjestelmien oletuskäyttäjätunnuksia ei ole poistettu käytöstä tai niiden oletussalasanoja ei ole muutettu.
l) Käyttäjien tunnistamisessa ja todentamisessa käytettävät menetelmät ja tunnisteet eivät ole yksiselitteisiä, josta johtuen tietojen käyttöoikeuksia ja valtuuksia ei voida määritellä riittävän tarkasti eikä käyttöä voida valvoa riittävän tehokkaasti.
m) Salasanojen hallintajärjestelmällä ei pystytä kontrolloimaan esimerkiksi käytössä olevien salasanojen minimipituuksia, käytettäviä merkkejä, vakiosalasanojen käyttöä ja salasanojen vaihtoväliä.
n) Käyttäjillä on käytössään turvattomia (esimerkiksi helposti arvattavia tai selvitettäviä) salasanoja.
o) Järjestelmien vastuita ei ole eriytetty riittävästi. Vastuita kasaantuu tietyille henkilöille, ja hallintatoimia ei pystytä tai osata tehdä riittävällä varmuudella esimerkiksi sairastapauksen sattuessa.

## A7.1 Pääsyn hallinnointi

### kontrolli

Pääsynhallintamenetelmät on määriteltävä tarkoin etukäteen. Niiden vahvuuden ja turvallisuuden on vastattava tietojärjestelmien ja tietojen turvatasoa. Tarvittaessa jokaiseen tietojärjestelmään on määriteltävä erillinen politiikka, jossa määritellään käyttäjien tunnistamisen menetelmät, millaisia tunnisteita käytetään, millaisia yhteyksiä tietojärjestelmiin on käytössä ja miten tietojärjestelmien käyttöä tarkkaillaan. Kaikista politiikkojen ja ohjeiden mainitsemista menetelmistä ja teknisistä yksityiskohdista ilmenee tarkkaan, onko kyseessä pakollinen ominaisuus, suositus tai hyväksyttävä (mutta ei suositeltava) vaihtoehto. Pääsynhallinta perustuu ja noudattaa organisaation tietoturvapolitiikkaa.

### käytännön ohjeita

a) Käyttäjien tunnistamisen menetelmistä ja käytettävistä tunnisteista määritellään politiikka. Vain riittävän vahvat ja turvalliset menetelmät hyväksytään. Tunnisteina hyväksytään vain sellaiset, joiden väärentäminen ei ole mahdollista ja joiden avulla tietojärjestelmiä ei voi väärinkäyttää.
b) Määritellään politiikka pääsyoikeuksista. Politiikassa määritellään, millaisia oikeuksia erilaisiin tietoihin ja resursseihin voidaan jakaa (esimerkiksi luku-, kirjoitus-, muutos-, poisto-, suoritus- ja hallintaoikeus). Oikeudet voivat tarvittaessa olla myös aikaan ja paikkaan sidottuja. Esimerkiksi varmuuskopioinnissa varmistusjärjestelmään (kuten nauharobotti tai online-levyjärjestelmä) voidaan kirjoittaa tietoja – toisin sanoen ottaa varmistuksia tai siirtää varmuuskopioita – vain tiettyinä kellonaikoina ja tietyistä tietojärjestelmistä.
c) Pääsyoikeudet määrittävässä politiikassa kuvataan, kuka käyttövaltuuksia myöntää ja miten niitä hallinnoidaan; mitkä menetelmät ovat hyväksyttäviä käyttäjien rekisteröinnissä (kuka tunnistaa henkilöt, miten käyttäjätunnukset ja salasanat myönnetään sekä miten jaetaan toimikortit, PIN-koodit ja vastaavat) ja millä menetelmillä kullekin käyttäjälle määritellään ja myönnetään hänelle kuuluvat valtuudet (kuka myöntää yksityiskohtaiset käyttöoikeudet, millaisella prosessilla henkilön valtuudet myönnetään ja poistetaan sekä esimerkiksi millai-

sia lomakkeita ja seurantaa käytetään hallinnoinnissa). Valtuuksien myöntö varmistetaan tietojen omistajalta, joka on vastuussa niiden käsittelyyn tarvittavien oikeuksien jaosta. On huomattava, että valtuuksien myöntäjälle itselleen (hallinnoinnin teknisen toimenpiteen suorittaja, esimerkiksi järjestelmän tukihenkilö) ei välttämättä ole myönnetty mitään käyttövaltuuksia kyseisiin tietoihin.

d) Tietojärjestelmien käyttäjät voidaan jakaa tarvittaviin ja sopiviin käyttäjäryhmiin, joille määritellään yhdenmukaiset valtuudet tietoihin. Tällä voidaan sekä vähentää inhimillisiä virheitä esimerkiksi valtuuksien määrittelyssä ja käytön seurannassa että helpottaa käytännön hallinnointityötä. Jos käyttövaltuuksia myönnetään organisaation ulkopuolisille henkilöille (muiden organisaatioiden työntekijät, asiakkaat ja potilaat), noudatetaan erityistä varovaisuutta ja riittäviä tarkastus- ja valvontamenettelyitä.

e) Verkkopalveluiden ja -yhteyksien käytöstä määritellään politiikka. Organisaation käyttäjät pääsevät vain niihin verkkoihin ja verkkoyhteyksiin, joihin heille on nimenomaisesti myönnetty pääsy. Tarvittaessa arkaluonteisiin tietoihin pääsystä verkkoyhteyksien takaa määritellään yksityiskohtaiset säännöt ja ohjeet. Yksityiskohtaisia määrittelyitä on mainittu esimerkiksi luvun *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus* kappaleessa *tiedonvälitys*.

f) Kriittisten tietojärjestelmien käyttöjärjestelmä- ja muiden resurssien käytöstä määritellään politiikka. Sovellusten käyttäjät saavat käyttöönsä vain ne resurssit, joihin heille on nimenomaisesti myönnetty pääsy. Tämä koskee käyttöjärjestelmän resursseja kaikilta sellaisilta osin, joihin pääsy voidaan hallinnoida (muistin, levytilan ja prosessoriajan käyttö, verkkotulostimien ja oheislaitteiden käyttö ym.). Pääsy hallinnoidaan sopivilla menetelmillä esimerkiksi käyttöjärjestelmä-, sovellus- ja käyttöliittymätasoilla.

g) Käyttöjärjestelmien ja sovellusten oletusprofiileja (käyttäjät, oikeudet, verkkoyhteydet ja resurssien suojaukset) ei ole syytä käyttää, vaan ottaa kaikissa järjestelmissä käyttöön itse määritellyt profiilit, joiden oikeudet on tarkkaan määritelty vastaamaan tietojen suojauksen tarvetta ja vaatimuksia. Jos oletusprofiilit sattuvat täsmällisesti sopimaan organisaation käyttöön, voidaan niitä käyttää, mutta tässäkin tapauksessa profiilit ja oikeudet on syytä nimetä uudelleen, eikä oletusnimiä ole virheiden ja väärinkäsitysten välttämiseksi missään tapauksessa syytä käyttää.

h) Pääsyn hallinnoinnin prosessilla on tarkkaan tiedossa, keillä käyttäjillä on mitäkin valtuuksia tietoihin. Myönnetyt käyttövaltuudet arvioidaan säännöllisellä prosessilla. On suositeltavaa, että korkean tietoturvan vaatimissa järjestelmissä valtuudet katselmoidaan vähintään kerran vuodessa. Valtuudet katselmoidaan myös muutostoimien yhteydessä. Havaitut poikkeamat korjataan ja kaikki sellaiset valtuudet, joihin on tehtävä muutoksia, päivitetään. Jos katselmoinneissa löydetään virheellisyyksiä, vanhentuneita tietoja tai esimerkiksi jo poistuneita käyttäjiä, käyttäjänhallintaprosessia korjataan siten, että valtuudet säilyvät vastaisuudessa ajantasaisina.

## A7.2 Käyttäjänhallinta

### kontrolli

Käyttäjien hallinnointi on määriteltävä tarkoin etukäteen. Hallinnointimenetelmät voivat olla tietojärjestelmäkohtaisia, mutta yksinkertaisuuden saavuttamiseksi ja virhemahdollisuuksien vähentämiseksi menetelmien on oltava keskenään mahdollisimman yhdenmukaisia. Käyttäjät ja heille myönnettävät valtuudet on määriteltävä riittävän turvallisesti, tehokkaasti ja tarkasti, jotta niillä voidaan toteuttaa tietojen ja tietojärjestelmien turvatason edellyttämät vaatimukset.

### käytännön ohjeita

a) Käyttäjien rekisteröinti (tunnistaminen ja todentaminen) ja valtuuksien määrittely (yksityiskohtaisten pääsy- ja käyttöoikeuksien määrittely) noudattaa etukäteen sovittua ja dokumen-

toitua prosessia. Rekisteröinti tapahtuu esimerkiksi otettaessa henkilö organisaation palvelukseen, henkilön tehtäväkuvan tai hänen tarvitsemiensa valtuuksien muuttuessa tai henkilön lopettaessa työsuhteensa organisaation palveluksessa.

b) Rekisteröinti on suositeltavaa tehdä henkilökohtaisesti. Henkilö, jolle ollaan myöntämässä pääsy tietojärjestelmiin ja antamassa tarvittavat valtuudet, tunnistetaan ja todennetaan henkilökohtaisesti. Samassa yhteydessä on syytä kertoa tietojen käsittelyyn ja suojaamiseen liittyvät säännöt ja henkilön vastuu näiden sääntöjen noudattamisessa sekä varmistaa ymmärtäminen ja vastuun otto henkilökohtaisella allekirjoituksella.

c) Rekisteröinnin ja valtuuksien myönnön prosessi noudattaa riittävää turvallisuustasoa ja tarpeen mukaan voidaan määritellä erityisiä järjestelmäkohtaisia tietoturvavaatimuksia. Tarpeen mukaan käytetään esimerkiksi allekirjoitettavia lomakkeita tai sähköistä hyväksyntäprosessia. Vastaavaa prosessia käytetään myös muutettaessa käyttäjän valtuuksia tai poistettaessa käyttäjän valtuudet. Työsuhteen loppuessa kaikkien valtuuksien poisto tapahtuu välittömästi.

d) Käyttäjätunnusten, salasanojen, toimikorttien, USB-avainten, kertakäyttöisiä salasanoja tuottavien laitteiden ja muiden vastaavien jakelu käyttäjille tapahtuu turvallista menetelmää noudattaen. Salasanoja ja käyttäjätunnuksia ei koskaan lähetetä selkokielisinä sähköpostitse, vaan annetaan käyttäjälle joko henkilökohtaisesti tai toimitetaan esimerkiksi suljetussa kirjeessä.

e) Kryptografisia tunnisteita (kuten salainen avain) sisältävää toimikorttia tai USB-avainta ei koskaan toimiteta samalla menetelmällä kuin käyttöön oikeuttavaa PIN-koodia, paitsi jos molemmat annetaan käyttäjälle rekisteröinnin yhteydessä. Jos esimerkiksi toimikortti toimitetaan käyttäjälle kirjeessä, PIN-koodit voidaan toimittaa esimerkiksi sähköisessä muodossa tai tekstiviestinä. Tämä prosessi kuvataan yksityiskohtaisesti organisaation julkaisemassa varmennepolitiikassa.

f) Tilanteissa, joissa käyttäjälle myönnetään laajoja käyttövaltuuksia (kuten järjestelmänhoitajat) tai valtuuksia ohittaa oikeuksien tarkistus tai järjestelmäsuojaukset, kiinnitetään erityinen huomio oikeuksien hallinnointiprosessin kulkuun ja siihen, että laajat valtuudet eivät kirjaudu sellaiselle henkilölle, jolla ei ole niihin oikeutta. Tällaisten valtuuksien käyttöä tarkkaillaan tarvittaessa tehostetusti (esimerkiksi *administrator*, *root*, *dba* tai *system*).

g) Rekisteröinnin yhteydessä henkilölle luodaan yksiselitteinen ja uniikki tunniste, jolla henkilö tunnistautuu tietojärjestelmän käyttäjäksi. Tunnuksia ja niiden tietoja käytetään myös tietojärjestelmien käytön seurannassa. Tunnisteesta ei käy selville käyttäjän asema, joka voisi indikoida myös käyttäjän valtuudet (esimerkiksi *palkanlaskenta*, *operator*, *manager*, *administrator*, *supervisor*, *netmgr*, *sysmgr*, *db_admin*).

h) Kaikista myönnetyistä tunnuksista pidetään yksityiskohtaista ja ajantasaista luetteloa, jota päivitetään aina tarpeen mukaan. Tietojärjestelmä ylläpitää järjestelmän sisäistä luetteloa (esimerkiksi käyttöjärjestelmä-, tietokanta- tai sovellustasolla), jolla järjestelmä tunnistaa käyttäjät ja myöntää kullekin ne valtuudet, jotka tietojen käyttöön on määritelty.

i) Jokaisella käyttäjällä on oma uniikki tunnisteensa. Tunnisteesta ilmenee, kuka henkilö on kyseessä. Tunnisteen avulla käyttäjälle myönnetään hänelle kuuluvat valtuudet ja estetään pääsy niihin tietoihin, joihin hänellä ei ole valtuuksia. Yhteiskäyttöisiä tunnuksia ei tietojärjestelmiin ole käytössä kuin ainoastaan poikkeustapauksissa. Tunnukseton käyttö (esimerkiksi Internet- ja Intranet-palveluissa) hyväksytään ja myönnetään vain julkisiin tietoihin.

j) Jos käyttäjän tunnisteena käytetään varmennetta, on tarkoituksenmukaista kirjata varmenteeseen vain mahdollisimman muuttumatonta tietoa, jotta varmenteiden hallintaprosessia ei turhaan vaikeuteta ja varmenteita ja toimikortteja ei jouduta uusimaan esimerkiksi henkilöiden tehtäväkuvan, aseman tai organisaatioyksikön vaihtuessa. Varmennetta on syytä käyttää vain henkilön todentamiseen (toisin sanoen henkilöllisyyden varmistamiseen). Muut henkilöä koskevat tiedot voidaan tallentaa esimerkiksi käyttäjähakemistoon. Varmenteen tietosisältönä voi olla esimerkiksi varmentajan (organisaatio) tiedot, henkilön nimi tai henkilönumero, henkilön julkinen avain, varmenteen voimassaoloaika (alku ja loppu) ja käyttötarkoitus (to-

dennus, salaus, allekirjoitus) sekä henkilön sähköpostiosoite. Henkilön rooliin tai tehtävään liittyvät tiedot voidaan hakea esimerkiksi LDAP-hakemistosta, kun tiedetään henkilön nimi ja organisaatio.

k) Käyttäjätunnusten käyttöä seurataan. Jos järjestelmään on määritelty tunnuksia, jotka ovat aktivoituja ja voimassa olevia mutta eivät ole aktiivissa käytössä, tunnusten käyttö on syytä asettaa käyttökieltoon, estää niiden käyttö tai poistaa ne kokonaan käytöstä. Seuranta ja valvonta on tarkemmin kuvattu luvussa *poikkeustilanteet*.

l) Jokaiselle käyttäjälle myönnetään täsmälliset ja yksityiskohtaiset valtuudet kuhunkin tarvitsemaansa tietoon ja tietojärjestelmäresurssiin. Valtuudet sisältävät kaikki asianmukaiset ja tarvittavat luku-, kirjoitus-, poisto- ja suoritusoikeudet. Käyttäjällä ei ole muihin tietoihin mitään oikeuksia. Järjestelmän vastuuhenkilölle määritellään tyypillisesti hallintaoikeus, jonka omaavat henkilöt voivat määritellä järjestelmän tietojen käsittelyyn liittyvät oikeudet ja järjestelmän käyttäjien valtuudet. Myönnettävistä oikeuksista on vastuussa tietojen omistaja.

m) Käyttäjille myönnettävät valtuudet myönnetään mahdollisia poikkeuksia lukuun ottamatta "vain tarvittaessa" -periaatteella *("on-a-need-to-know basis"*) Tässä yhteydessä on syytä huomata, että sosiaali- ja terveydenhuollon työntekijälle saattaa syntyä tarve sellaiseen tietoon, mihin hänelle ei ole myönnetty valtuuksia. Jotta potilaan tai asiakkaan hoito ei vaarannu, tällaisia tilanteita varten saattaa olla syytä luoda hoitohenkilölle mahdollisuus myöntää itselleen esimerkiksi tilapäiset käyttövaltuudet tai ohittaa myönnetyt valtuudet. Mikäli näin toimitaan, on seurannan oltava erityisen tiukkaa.

n) Myönnetyistä valtuuksista pidetään yksityiskohtaista ja ajantasaista luetteloa, jota päivitetään aina henkilöiden valtuuksien muuttuessa ja aina muulloinkin, kun se on tarpeellista, esimerkiksi kun organisaatio on ottanut käyttöön uusia teknologioita tai kun uusia tietoturvallisuusriskejä on ilmaantunut.

o) Käyttövaltuuksia voidaan hallinnoida esimerkiksi jakamalla käyttäjät ryhmiin, joihin kuuluville on myönnetty yhtäläiset valtuudet kuhunkin tietoon tai resurssiin. Arkaluonteiseen tietoon voidaan myöntää yksityiskohtaisempia valtuuksia, esimerkiksi potilastietoihin pääsy vain hoitoprosessissa mukana oleville henkilöille. Tällaisia valtuuksia määritettäessä on kuitenkin kiinnitettävä erityinen huomio siihen, että tietoihin pääsyä ei estetä liikaa. Usein pelkkä valvonta saattaa tuottaa riittävät keinot torjumaan tietoihin kohdistuvat uhkat. Tämä myös takaa, että kiireellisessä tilanteessa välttämättömät toimenpiteet voidaan suorittaa viiveettä, kun tietoihin on pääsy, eikä yksittäisiä käyttöoikeuksia tarvitse erikseen myöntää tai olemassa olevia käyttövaltuuksia määritellä ylitettäväksi ("*override*").

p) Vastuut jaetaan tarvittaessa osiin ja eriytetään ne eri henkilöille. Näin ehkäistään mahdollisuus liian suurten vastuiden kasautuminen yksittäisille henkilöille, ja voidaan vähentää tästä aiheutuvaa riskiä tärkeiden ja kriittisten tietojen väärinkäyttöön ja huolimattomuuteen tietojen käsittelyssä. Esimerkiksi vastuut tietojärjestelmien ja tietoliikenneverkkojen hoidossa on syytä eriyttää.

## A7.3 Käyttäjien todentaminen

### kontrolli

Käyttäjien todentamisessa käytettävät menetelmät on oltava yhdenmukaiset ja niillä on voitava toteuttaa sellainen turvataso, mitä edellytetään tietojärjestelmien ja niiden sisältämien tietojen suojaamisessa. Käytettävien käyttäjätunnusten ja salasanojen hallintamenetelmien on tuettava riittäviä keinoja, joilla käyttäjien salasanat voidaan asettaa tai edellyttää riittävän turvallisiksi. Tarvittaessa todentamiseen on käytettävä vahvoja menetelmiä, kuten vaihtuvia salasanalistoja (haaste-vastalukulistat, *challenge-response)* tai kertakäyttöisiä tunnisteita, toimikortteja, USB-avaimia tai biometrisia tunnisteita.

a) Tietojärjestelmiin kirjaudutaan aina riittävän turvallisella menetelmällä. Ainoastaan julkisiin tietoihin (esimerkiksi Internet-palveluissa) voidaan päästä ilman kirjautumista. Tällöinkin tiedot on suojattava asianmukaisesti esimerkiksi väärentämiseltä tai tuhoutumiselta. Kirjautumismenetelmä varoittaa ja kieltää ulkopuolisia yrittämästä kirjautumista ilman asianmukaisia valtuuksia.

b) Kirjautumismenetelmä näyttää kirjautujalle vain sellaiset identifiointitiedot, joita käyttäjä välttämättä tarvitsee kirjautuessaan tietojärjestelmään. Yhtään ylimääräisiä tietoja ei näytetä, ennen kuin kirjautumisprosessi on valmis. Näytettävät tiedot ovat kuitenkin vähintäänkin sellaiset, että käyttäjä tietää kirjautuvansa oikeaan järjestelmään.

c) Virheen sattuessa kirjautumisprosessissa menetelmä ei kerro käyttäjälle, mikä vaihe kirjautumisessa oli virheellinen. Kirjautumisyritysten määrä on rajoitettu (esimerkiksi maksimissaan kolme väärää yritystä, jonka jälkeen uusi yritys voidaan tehdä vasta tietyn, mahdollisesti kumuloituvan ajan kuluttua). Lisäksi kirjautuminen tämän jälkeen kyseiseltä verkkoyhteydeltä voidaan estää määräajaksi. Riittävän monta väärää kirjautumista havaittaessa voidaan kyseinen käyttäjätunnus esimerkiksi lukita automaattisesti, jolloin esimerkiksi vain järjestelmän vastuuhenkilö voi avata pääsyn aktivoimalla käyttäjätunnuksen. Virheellisten yritysten seurannasta ja valvonnasta on tarkempi kuvaus luvussa *poikkeustilanteet*.

d) Esimerkiksi verkkoyhteyden katketessa käyttäjä uloskirjataan järjestelmästä (*auto-logout*) automaattisesti. Mahdolliset istunnon tiedot erilaisista välimuisteista tuhotaan. Tämän jälkeen noudatetaan normaalia käyttäjän sisäänkirjautumismenettelyä.

e) Jos käytetään käyttäjätunnus-salasanamenettelyä, kirjautumissovellus on suunniteltu siten, että tietoverkossa ei lähetetä yhtään käyttäjätunnusta tai salasanaa selkokielisenä. Kaikki tunnusten käsittely tehdään salattuna. Käyttäjätunnuksia ja salasanoja ei tallenneta mihinkään väliaikaiseen muistiin tai tiedostoon (*memory cache*, *disk cache*, *network cache*).

f) Onnistuneessa kirjautumisessa ilmoitetaan käyttäjälle edellinen onnistunut kirjautuminen ja mahdolliset virheelliset yritykset. Jos käyttäjä havaitsee, että hän itse ei ole mainittuja kirjautumisia tai yrityksiä tehnyt, on hänen ilmoitettava mahdollisesta tietoturvauhkasta noudattaen asianmukaista prosessia.

g) Ensimmäinen järjestelmään kirjautuminen mahdollisella väliaikaisella salasanalla on ohjeistettu ja tarvittaessa valvottu. Käyttäjä pakotetaan vaihtamaan salasana ensimmäisen kirjautumisen yhteydessä, mikäli käyttäjä itse määrittelee salasanansa.

h) Tietojärjestelmien käyttäjät, jotka kirjautuvat verkkoyhteyksien takaa, todennetaan asianmukaisilla menetelmillä. Tarvittaessa voidaan käyttää esimerkiksi toimikorttipohjaista todentamista, kertakäyttöisiä tunnisteita tai vaihtuvia salasanalistoja. Julkisessa käytössä olevista tietokoneista ei ole syytä sallia mitään pääsyä tärkeisiin tietoihin tai kriittisiin tietojärjestelmiin. Etäyhteyksissä on suositeltavaa käyttää ennalta sovittuja laitteistoja (kuten kotikoneet tai kannettavat tietokoneet) ja yhteyksiä. Verkkoyhteyksistä ja niiden salaamisesta on mainittu tarkemmin luvussa *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus*.

i) Salasanojen hallintamenetelmä on turvallinen. Sillä voidaan määrittää laatutaso käytettäville salasanoille. Käyttäjät eivät voi alittaa salasanan laatuvaatimuksia määrittäessään itselleen salasanan, jos käyttäjälle ylipäätään sallitaan salasanan itse asettaminen. Salasanoja asetettaessa tai niillä tunnistauduttaessa salasana ei koskaan näy näyttöpäätteellä selkokielisenä. Vaihdon yhteydessä virhemahdollisuudet minimoidaan esimerkiksi antamalla salasana kahdesti. Käyttäjien salasanaohjeesta on tarkemmin mainittu luvussa *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus*.

j) Salasanojen hallinnointimenetelmä sisältää mahdollisuuden määritellä käyttäjille salasanat järjestelmän toimesta. Jos käyttäjä saa itse määritellä salasanansa, menetelmällä on mahdollista pakottaa käyttäjä vaihtamaan salasanansa määrävälein automaattisesti, estää samojen salasanojen käytön toistuvasti sekä huolehtia, että käyttäjän määrittelemät salasanat täyttävät laadulliset vaatimukset (pituus, käytettävät merkit, isot kirjaimet ja numerot). Järjestelmä tal-

lentaa käytössä olevat salasanat sellaisessa muodossa, että niiden selvittäminen järjestelmää tutkimalla on mahdotonta tai riittävän vaikeaa (esimerkiksi salattuna).

k) Korkean turvatason edellyttämiin toimiin (järjestelmien hallinta, korkean turvatason tietojen käsittely) käytetään tarvittaessa vahvempia menettelyitä kuin käyttäjätunnusta ja salasanaa.

l) Vahvoja tunnistamistapoja käytetään aina silloin, kun käsiteltävien tietojen tai käytettävien tietojärjestelmien turvataso edellyttää käyttäjien vahvaa tunnistamista. Suositeltavia tunnistamisvälineitä ovat toimikortit ja USB-avaimet varmenteineen sekä erilaiset haaste-vastalukuun perustuvat tunnistamisvälineet (kertakäyttötunnisteet, salasanalistat, matkapuhelin).

m) Toimikortin ja USB-avaimen käyttö oikeutetaan esimerkiksi PIN-koodilla tai biometrisellä tunnisteella (kuten sormenjälki). Biometrista tunnistetta tai tietoja siitä ei koskaan tallenneta tietojärjestelmään tai mihinkään rekisteriin, vaan sitä käytetään nimenomaisesti ainoastaan toimikortin tai USB-avaimen käytön "avaamisessa", jolloin käyttäjä todentautuu toimikortille käyttämällä henkilöllisyytensä todisteena sormenjälkeään PIN-koodin asemesta. Tietojärjestelmä tai sovellus tunnistaa käyttäjän varmenteesta. Sormenjälkitodennus perustuu tyypillisesti siihen, että rekisteröinnin yhteydessä toimikortille tallennetaan matemaattinen malli käyttäjän sormenjäljestä, jolla toimikortti todentaa käyttäjän. Kortille ei tallenneta kuvaa sormenjäljestä, eikä matemaattisesta mallista ole mahdollista luoda kopiota sormenjäljestä.

n) Käyttäjän allekirjoittaessa tiedon tai asiakirjan sähköisesti jokainen allekirjoitus yleensä hyväksytään ja vahvistetaan erillisellä PIN-koodin tai sormenjäljen syötöllä.

o) Käytettäessä kertakirjautumista (SSO, *single sign-on*) on syytä käyttää käyttäjien vahvaa todennusta. Käyttöoikeuksien jako eri tietojärjestelmiin toteutetaan riittäviä turvallisuusvaatimuksia noudattaen. Kertakirjautuminen vähentää riskejä käyttäjätunnusten ja salasanojen paljastumiseen ja helpottaa tietojärjestelmiin kirjautumista. Toisaalta onnistunut pääsy (esimerkiksi murtautuminen) tietojärjestelmään takaa pääsyn kaikkiin niihin järjestelmiin, jotka ovat kertakirjautumisen piirissä.

p) Käyttäjien lisäksi myös tietoverkon laitteet, palvelut ja sovellukset ovat todennettavissa sekä käyttäjien että muiden laitteiden, palveluiden ja sovellusten toimesta. Todentamiseen voidaan käyttää esimerkiksi palvelinvarmenteita ja ohjelmistovarmenteita, joilla ohjelmakoodi allekirjoitetaan.

# 10 Tietojärjestelmien kehitys ja ylläpito

## 10.1 Yleistä

Organisaation tietoturvallisuustason ylläpitämiseksi ei riitä, että organisaation toiminnassa, tietojen käsittelyssä ja tiedonvälityksessä noudatetaan turvallisia tapoja ja menetelmiä. Myös käytettävien tietojärjestelmien ja sovellusten turvallisuudesta on huolehdittava. Tietojärjestelmät täytyy suunnitella ja toteuttaa siten, että turva-aukkoja ei ole sovellusten ja järjestelmien sisällä. Käytettävien tietojen oikeellisuus täytyy taata koko käsittelyprosessin ajan: oikeellisuus täytyy taata aina järjestelmään käsiteltäväksi tai käytettäväksi vastaanotettavista tiedoista (syötetietojen tarkastus, *input data validation*) järjestelmän tuottamiin tietoihin (tulostustietojen tarkastus, *output data validation*) asti kaikissa käsittelyn vaiheissa. Tieto voi olla mitä tahansa esimerkiksi tietojärjestelmän sisäisesti toiselta prosessilta vastaanotettavaa tietoa, toisesta tietojärjestelmästä vastaanotettavaa tietoa, tiedostosta luettavaa tietoa tai käyttäjän järjestelmään syöttämää tietoa. Erityisesti sähköpostitse vastaanotettavan tiedon alkuperästä tulee varmistua.

Tietojärjestelmät on suunniteltava siten, että ne toteuttavat automaattisesti lakien vaatimukset – esimerkiksi henkilö- ja potilastietojen käsittelyssä ja suojaamisessa – ja että mahdolliset lakimuutokset on otettavissa riittävän helposti huomioon esimerkiksi järjestelmien määrityksiä ja konfiguraatioita muuttamalla. Lakien noudattaminen ja noudattamatta jättäminen ei saa olla käyttäjän toimista kiinni, vaan tietojärjestelmän on aina mahdollisuuksien mukaan ohjattava tai pakotettava käyttäjä oikeanlaiseen toimintaan. Edellä mainittu koskee myös kaikkia kansallisia ja kansainvälisiä standardeja.

Turvallisuudesta tulee huolehtia kaikkien organisaation käytössä olevien kriittisten ja tärkeiden tietojärjestelmien ja sovellusten osalta, tuotettiinpa niillä sitten organisaation omassa käytössä olevia palveluita (esimerkiksi erilaiset toiminnanohjausjärjestelmät), tietojärjestelmäarkkitehtuuriin ja -infrastruktuuriin liittyviä palveluita (koko tietoliikenneinfrastruktuuri ja erilaiset verkkopalvelimet), liiketoiminnan tarvitsemia palveluita, loppukäyttäjän sovelluksia tai asiakkaiden ja yhteistyökumppaneiden käyttämiä palveluita (esimerkiksi asiakaspalvelun sovellukset ja tilausjärjestelmät).

Terveydenhuollossa on huolehdittava erityisesti potilaan hoitoon ja potilaan tietojen käsittelyyn tarkoitettujen tietojärjestelmien turvallisuudesta. Potilaan hoidossa tarvittavien tietojen on oltava eheitä ja saatavilla. Potilaan yksityisyydensuoja on turvattava: on pystyttävä takaamaan, että käsiteltävien ja tallennettavien hoitotietojen luottamuksellisuus säilyy käytettävissä tietojärjestelmissä. Tietojärjestelmissä on käytettävä tarpeen mukaan riittäviä kryptografisia menetelmiä tietojen eheyden ja luottamuksellisuuden takaamiseksi.

Ohjelmistokehitysprosessin sekä uusien ohjelmistoversioiden käyttöönoton on oltava määritelty siten, että ohjelmiston lähdekoodi on turvattu sekä kehitysvaiheessa että tuotannossa. Käyttöön otettavat ohjelmistot on testattava asianmukaisesti, jotta voidaan etukäteen varmistua oikeanlaisesta toiminnasta ja vaadittavasta laadusta. Uusien ohjelmistoversioiden käyttöönoton jälkeen on tarkkailtava, että uusi versio toimii moitteetta. Hyvästä ohjelmistokehityksen prosessista on olemassa lukuisia esimerkkejä ja standardeja, eikä tässä dokumentissa puututa ohjelmistokehitykseen tarkemmin. Ohjelmistokehitystä ja ohjelmistojen hankintaa koskien kannattaa tutustua esimerkiksi standardeihin *ISO/IEC 12207: 1995 "Software Life Cycle Processes"*, *IEEE/EIA 12207 "Industry Implementation of International Standard ISO/IEC 12207"*, *ISO/IEC 15504: "Measures of Software Development Process Capability"* sekä *ISO/IEC 13335*.

Valmiiden sovellusten (erityisesti käyttöjärjestelmät, tietokannat ja tietoliikenne) osalta asiakkaalla ei välttämättä ole muuta vaihtoehtoa kuin luottaa tarjolla olevien ohjelmistojen turvallisuuteen. Vain erittäin harvalla organisaatiolla on mahdollisuutta esittää sellaisia erityisvaatimuksia, joita suuret ohjelmistotoimittajat ottaisivat huomioon. Silti riskianalyyseissä kannattaa analysoida erilaiset riskit, joita näihin edellä mainittuihin ohjelmistokomponentteihin liittyy. Näin myös niissä esiintyviin ongelmiin voidaan varautua. Esimerkkejä tällaisista organisaation toiminnan vaarantavista ongelmista ovat esimerkiksi erilaiset käyttöjärjestelmissä olevat tietoturva-aukot ja takaportit, sovellusten vikaantuminen ja ilmi

tulevat ohjelmistoissa olevat virheet sekä ylläpitotoimintojen järjestely edellä mainittujen virheiden ja vikatilanteiden korjaamisessa.

Tuotantokäytössä olevien ohjelmistojen käyttöä testaustarkoituksessa on suotavaa välttää. Myöskään ohjelmiston kehityksessä käytettävä järjestelmä ei ole testaukseen sopiva ympäristö. On suositeltavaa käyttää testaukseen tähän tarkoitukseen nimenomaisesti varattua järjestelmää. Käytettäessä tuotannollista tietojärjestelmää testitarkoituksessa on tyypillistä, että testiolosuhteet vaarantavat tuotantojärjestelmän turvallisuuden. Usein esimerkiksi ohjelmistotestaajille voi syntyä mahdollisuus päästä käsiksi luottamuksellisiin tietoihin. Testauksessa käytettävä tieto saattaa myös sekoittua oikeaan tietoon, jolloin varmuus tiedon laadusta ja käyttötarkoituksesta voi kadota, esimerkiksi oikeaa tietoa voi tuhoutua testitietona ja toisaalta testitietoa saatetaan käyttää oikean tiedon asemesta.

## 10.2 Uhkista ja riskeistä

Puutteet ja virheet tietojärjestelmissä ja sovelluksissa voivat aiheuttaa vakavan uhkan organisaation toiminnalle ja käytettävien tietojen turvallisuudelle. Alla on mainittu esimerkkejä uhkista, joihin varautumalla voidaan torjua tietojärjestelmien ja ohjelmistojen puutteellisuudesta ja virheellisyydestä aiheutuvia riskejä.

a) Tietojärjestelmille ja ohjelmistoille ei ole määritelty turvallisuustasoa ja turvallisuuden toteuttavia vaatimuksia, joita järjestelmien on noudatettava.
b) Ohjelmistoihin ei ole toteutettu riittäviä kryptografisia menetelmiä.
c) Kryptografiset menetelmät eivät ole lainmukaisia.
d) Vaatimukset määritellään vasta myöhäisessä vaiheessa kehitysprosessia, joka estää vaatimusten toteuttamisen tai aiheuttaa ylimääräisiä kustannuksia.
e) Tietojärjestelmien käyttämä kellonaika ei vastaa todellisuutta.
f) Tietojärjestelmään syötettävät tiedot ovat kokonaan tai osittain vääriä, puutteellisia, sisältävät virheitä tai eivät muuten sovi käyttötarkoitukseen.
g) Tietojärjestelmässä käsiteltävät tiedot muuttuvat vääriksi tai virheellisiksi tai poistetaan luvatta.
h) Tietojärjestelmässä käsiteltäviin tietoihin syntyy luvaton pääsy.
i) Tietojärjestelmistä tulostettavat tiedot ovat puutteellisia, sisältävät virheitä tai niitä ei ole asianmukaisesti suojattu.
j) Salakirjoitetun tiedon salausta ei saada purettua ja tieto on käyttökelvotonta.
k) Lähdekoodi vaarantuu ulkopuolisen henkilön päästyä kehitysympäristöön.
l) Lähdekoodista ei ole varmuuskopiota, se tuhoutuu tai on tallennettu käyttökelvottomalle tietovälineelle.
m) Alihankkijalta hankittua ohjelmistoa ei voida käyttää alihankkijan konkurssin takia, kun lähdekoodia ei ole käytettävissä escrow-sopimuksen puuttuessa. Ohjelmiston ylläpitoa ei voida järjestää.
n) Tietojärjestelmiin tehtäville muutoksille ei ole määritelty hyväksymismenettelyitä.
o) Muutoksia ei hallita: ei ole sovittuja käytäntöjä ja menetelmiä, toiminta ja muutokset eivät ole dokumentoituja, muutosprosessia ei ohjata ja valvota, muutokset eivät ole valtuutettuja ja niitä tekevät henkilöt, joilla ei ole valtuuksia eikä muutosten toteuttamiseen vaadittavaa osaamista.
p) Tietojärjestelmiin ja ohjelmistoihin tehdään tarpeettomia muutoksia ja ohjelmistopäivityksiä.
q) Muutoksia ei huomioida muiden järjestelmien toiminnassa.
r) Muutoksia ei huomioida liiketoiminta- ja jatkuvuussuunnitelmissa eivätkä ne vastaa tietoturvallisuusvaatimuksia.
s) Käyttäjädokumentaatio ei vastaa tehtyjä muutoksia.
t) Muutoksista ei tiedoteta.
u) Muutoksia ei testata riittävän tarkasti ja riittävällä laajuudella. Testauksesta ei kirjata tuloksia.

v) Testauksessa käytetään kehitysympäristöä tai tuotannollista ympäristöä ja lähdekoodi tai tuotannollinen tieto vaarantuvat.
w) Testauksen ja käyttöönoton jälkeen muutosten toiminnallisuutta ei katselmoida ja vaatimusten toteuttamista ei varmisteta.
x) Tehtyjä muutoksia ei päivitetä hälytysjärjestelmiin.
y) Vanhoja ohjelmistoversioita ei säilytetä. Uusilla ohjelmistoversioilla luotu tieto ei ole käyttökelpoista vanhoilla ohjelmistoversioilla.
z) Muutokset luovat piilossa olevan kanavan, jota käyttämällä ulkopuoliselle syntyy pääsy organisaation tietoihin.
å) Muutoksia ei ole huomioitu ylläpitosopimuksissa tai alihankkijat eivät sitoudu muutosten ylläpitoon.

## A8.1 Vaatimukset tietojärjestelmien turvallisuudelle

### kontrolli

Tietojärjestelmille ja sovelluksille on asetettava tietoturvallisuuteen liittyvät vaatimukset, jotka on otettava huomioon ohjelmiston toimintoja suunniteltaessa, määriteltäessä ja ohjelmistokehityksessä sekä valmisohjelmistojen hankinnassa.

Erityisesti on kiinnitettävä huomiota myös siihen, että hankittavilla tai kehitettävillä tietojärjestelmillä voidaan ohjata tai pakottaa käyttäjät automaattisesti lainmukaiseen toimintaan, eikä tietojärjestelmän käyttäminen lisää riskiä tai mahdollisuuksia vahingossa tai tahallisesti tapahtuviin väärinkäytöksiin tai laittomuuksiin. Tietojärjestelmän on aina mahdollisuuksien mukaan ohjattava käyttäjä oikeanlaiseen toimintaan ilman, että käyttäjälle itselleen muodostuisi mahdollisuutta väärään tai virheelliseen toimintaan ja siten kohtuutonta lisävastuuta. Tietojärjestelmät on suunniteltava siten, että niiden käytöllä voidaan vähentää riskejä sen sijaan, että riskit lisääntyisivät.

### käytännön ohjeita

a) Organisaation toiminnan ja riskianalyysin tuloksia käytetään määritettäessä tietojärjestelmille ja ohjelmistoille asetettavien turvallisuusvaatimusten yleinen taso. Turvallisuusvaatimukset ovat linjassa organisaation (liike)toiminnan vaatimusten kanssa.
b) Käytettävät tietojärjestelmät noudattavat lakien vaatimuksia. Ne ohjaavat ja tarvittaessa pakottavat käyttäjät oikeanlaisiin toimenpiteisiin siten, että käyttäjälle ei aiheetta anneta mahdollisuuksia laittomaan, virheelliseen tai väärään toimintaan. Mahdolliset lakimuutokset on otettavissa huomioon riittävän helpoilla järjestelmien määrittelytoimenpiteillä.
c) Määritellään tarpeelliset loki- ja seurantamenetelmät sekä automaattista että manuaalista tapahtumaseurantaa varten (esimerkiksi järjestelmien toiminta, tietoliikenne- ja tietokantatapahtumat sekä käyttäjien toimet).
d) Kehitystyössä sovelletaan dokumentoitua ohjelmistokehitysmetodologiaa. Tietoturvattomien menetelmien ja teknologioiden käyttö kehitystyössä on kielletty ja tarvittavalla tavalla estetty. Kehitystyötä varten on luotu riittävät turvakontrollit ja laaduntarkkailumenetelmät.
e) Määritellään kaikki ohjelmistossa tarvittavat tietoturvallisuuden toteuttavat toiminnot, esimerkiksi käyttöoikeuksien ja hälytysten hallinnassa käytettävät menetelmät.
f) Määritellään tarpeelliset kryptografiset menetelmät tietojen turvallisuuden suojaamiseksi.
g) Määritellään tarpeelliset toimet, joilla arvioidaan kaupallisten valmisohjelmistojen kyky toteuttaa yllä mainitut vaatimukset.
h) Tarvittaessa tietojärjestelmät sertifioidaan (esimerkiksi *ISO/IEC 15408*) tai käytetään jo sertifioituja tietojärjestelmiä.
i) Vaatimukset toteutetaan ohjelmistoihin kehitysprosessin mahdollisimman varhaisessa vaiheessa, jotta ne olisivat ylipäätään toteutettavissa ja jotta niiden toteuttaminen olisi riittävän helppoa.

j) Kaikista käyttöön otettavista tietojärjestelmistä, ohjelmistoista ja niiden osista (mukaan lukien käyttöjärjestelmät ja varusohjelmat) laaditaan testaussuunnitelma ja hyväksymiskäytäntö.

k) Käytettäessä kolmansia osapuolia alihankkijoina tietojärjestelmien tai ohjelmistojen kehittäjinä ja toimittajina varmistetaan, että alihankkijan toiminta ja hankitut tuotteet vastaavat laadultaan niitä vaatimuksia, joita on asetettu organisaation omalle toiminnalle. Varmistutaan erityisesti yrityksen maineesta, taloudellisesti vakaasta asemasta ja tulevaisuudennäkymistä, kyvystä tuottaa tarvittavia ylläpito- ja huoltopalveluita sekä organisaation toiminnan laadusta. Tarvittaessa voidaan edellyttää laatusertifikaatin (esimerkiksi *ISO9000*) olemassaolo. Hyväksytyistä alihankkijoista voidaan tarpeen mukaan laatia luettelo.

l) Kriittisessä käytössä olevilta tietojärjestelmiltä ja ohjelmistoilta edellytetään, että ne on turvaluokiteltu ja että niistä on laadittu turvaprofiili, joka täyttää järjestelmiltä vaadittavat ominaisuudet. Turvaprofiilina voidaan käyttää esimerkiksi *ISO/IEC TR 15446*:n mukaista profiilia. Esimerkkejä profiileista löytyy dokumentin liitteestä *Annex B (informative) Generic examples*.

## A8.2 Tietojärjestelmien ja sovellusten sisäinen tietoturva

### kontrolli

Tietojärjestelmiin käsiteltäväksi vastaanotettavien tietojen, syötetietojen (*input data*), on oltava eheitä ja oikeellisia. Eheys ja oikeellisuus on tarkastettava. Ohjelmiston on pystyttävä takaamaan tietojen käsittelyn aikainen luottamuksellisuus, eheys ja oikeellisuus. Sen on estettävä valtuudeton pääsy tietoihin, tietojen tahalliset valtuudettomat muutosyritykset ja ohjelmiston viallisesta toiminnasta johtuva tietojen turmeltuminen. Sovelluksen tallentamien ja tuottamien tietojen (*output data*), käytetäänpä niitä sitten muissa tietojärjestelmissä tai tulostetaan esimerkiksi paperimuotoon, on oltava eheitä ja oikeellisia.

Sovelluksen on tarvittaessa kyettävä vastaanottamaan, käsittelemään ja tuottamaan sähköisesti allekirjoitettua ja sopivalla kryptografisella menetelmällä salattua tietoa. Tietojärjestelmien ja sovellusten omien tietojen (systeemitiedostot, lokitiedostot ym.) on oltava suojattuja.

### käytännön ohjeita

a) Määritellään kaikille käsittelyprosessissa mukana oleville henkilöille tarpeelliset ja riittävät vastuut ja valtuudet, kun tietojen oikeellisuus tarkastetaan manuaalisesti. Hälytysten käsittelyssä tarvittavat toimet ja vastuut määritellään. Tämä on tarkemmin määritelty luvussa *poikkeustilanteet*.

b) Varmistetaan, että järjestelmän sisäinen kello tuottaa oikeaa aikaa. Käytetään mahdollisuuksien mukaan reaaliaikaa esimerkiksi ulkoisesta lähteestä.

c) Varmistetaan, että käytettäessä kryptografisia menetelmiä noudatetaan kaikkien niiden maiden lakeja, joissa salattuja tai sähköisesti allekirjoitettuja tietoja on tarkoitus käyttää.

d) Syötetietojen eheys tarkastetaan: käytetään esimerkiksi sähköistä allekirjoitusta tai pariteetin, tiivisteen tai muun tarkastussumman tarkastusta.

e) Syötetietojen kattavuus tarkastetaan: vastaanotettu tieto on kattava ja yhtenäinen kokonaisuus. Tietoja tai tiedon osia ei puutu syötteestä.

f) Syötetietojen oikeellisuus tarkastetaan: käytetään oikeantyyppistä tietoa (ei esimerkiksi kirjaimia numerokentässä), oikeaa merkistöä (vain hyväksytyt kirjaimet ja merkit) ja tiedot ovat oikealla vaihteluvälillä (esimerkiksi vain sallitut päivämäärät).

g) Tarkastetaan, että syötetiedon määrä ei ole liian suuri käsiteltäväksi.

h) Varmistetaan, että syötetiedon alkuperä on oikea ja lähettäjä on aito ja omaa riittävät valtuudet.

i) Luettaessa tietoja järjestelmään käytetään sopivia menetelmiä varmistamaan lukutapahtuman ja tiedon virheettömyys, havaitsemaan mahdolliset virheet ja suorittamaan hälytys.

j) Huolehditaan käsiteltävän tiedon eheydestä käsittelyprosessin aikana ja siirrettäessä tietoa tietojärjestelmän sisällä prosessilta toiselle. Tieto ei saa muuttua tahallisesti eikä korruptoi-

tumalla esimerkiksi ohjelmistovirheen tai tiedonsiirtovirheen seurauksena. Erityisesti niiden ohjelmiston ominaisuuksien, joilla muutetaan tallennetun tiedon sisältöä ("lisää"-, "muuta"- tai "poista"-ominaisuudet), on oltava erityistarkkailun piirissä. Ohjelmiston on syytä varoittaa käyttäjää eri toimenpiteistä aina tarvittaessa (esimerkiksi '*Haluatko muuttaa tallennettuja tietoja?*' tai '*Haluatko poistaa tallennetut tiedot?*').

k) Huolehditaan, että sovellusten sisäiset rakenteet ovat sopivia ja tarkoituksenmukaisia (esimerkiksi puskurointi ja ylivuotosuojat).

l) Tarkastetaan määräajoin käsiteltävän ja talletetun tiedon eheys ja muuttumattomuus kulloisenkin tarpeen mukaan.

m) Huolehditaan, että on menetelmä oikeiden tietojen palautukseen, jos tietoja on muuttunut tai tuhoutunut (tietokantojen backlog-menetelmät, levy- tai nauhavarmistukset).

n) Tarkastetaan määräajoin tallennetun tiedon sähköisen allekirjoituksen voimassaolo kulloisenkin tarpeen mukaan ja uusitaan allekirjoitus sopivalla menetelmällä (esimerkiksi uudelleen allekirjoitus, järjestelmäallekirjoitus, aikaleiman uusiminen).

o) Siirrettäessä tietoja järjestelmästä toiseen käytetään riittäviä menetelmiä takaamaan tiedonsiirron turvallisuus.

p) Varmistetaan, että tietoon ei ole valtuudetonta pääsyä käsittelyprosessin aikana.

q) Varmistetaan, että tallennettuun tietoon ei ole valtuudetonta pääsyä koko tiedon elinkaaren aikana.

r) Varmistetaan, että eräajoina ajettavat sovellukset käynnistyvät ja suoriutuvat oikeaan aikaan ja oikeilla valtuuksilla.

s) Tulostustiedon eheys varmistetaan sopivalla menetelmällä, esimerkiksi sähköisellä allekirjoituksella tai käyttämällä tarkastussummaa.

t) Varmistetaan, että tulostustieto on kattava kokonaisuus ja kaikkien sovittujen määrittelyiden mukainen.

u) Lähetettäessä tietoa varmistetaan, että vastaanottaja on aito ja että tietoa ei lähetetä kohteeseen, joka ei ole oikeutettu tietoa vastaanottamaan.

v) Varmistetaan, että salattu tieto säilyy luettavana myös salauksen jälkeen. Salakirjoitusavaimen tuhoutuessa salakirjoitettua tietoa ei ole mahdollista käyttää, ellei tietoa voi tuottaa uudelleen tai ellei salakirjoitusavaimen varmuuskopiota ole olemassa tai saatavilla. Organisaatio määrittelee avainten varmuuskopiointimenetelmän julkaisemassaan varmennepolitiikassa.

w) Varmistetaan, että ohjelmiston (väliaikaisesti tai pysyvästi) tallentamia tietoja ei pystytä valtuudettomasti lukemaan, kun tallennustilaa vapautetaan. Esimerkiksi tiedon tallentuminen erilaisiin välimuisteihin (kuten *memory cache, disk cache* tai *network buffers*) tai levytilan käyttö muistina (sivutus; *paging* tai *swapping*) ei vaaranna tallennetun tiedon luottamuksellisuutta; ei myöskään sen jälkeen, kun välimuistin käyttämä tila vapautuu. Tämä koskee myös normaalia tietokoneen käyttömuistia tai levytilaa: kun levytilaa vapautuu uudelleen käytettäväksi esimerkiksi tiedoston tuhoamisen seurauksena, huolehditaan siitä, että muistiin tai levylle tallennetut tiedot eivät ole luettavissa sille, joka tilan ottaa uudelleen käyttöön.

## A8.3 Lähdekoodi

### kontrolli

Lähdekoodiin pääsyn on oltava tarkassa kontrollissa. Kehitysvaiheessa olevan ohjelmistokoodin on oltava riittävän suojattua. Tuotantokäytössä olevan ohjelmiston lähdekoodiin pääsyn on oltava tarkoin suojattua ja vain oikeutetuilla henkilöillä. Lähdekoodin kopioiminen ja muuttaminen tulee suojata ja niitä varten on noudatettava sovittuja muutoksen hallinnan prosesseja. Kehitysjärjestelmiin liittyviä vaatimuksia on mainittu luvun *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus* kappaleessa *kehitysjärjestelmät.*

### käytännön ohjeita

a) Noudatetaan ohjelmistokehitykseen ja sen laatuun sopivia standardeja.
b) Ohjelmiston kehitysvaiheessa noudatetaan sopivia menetelmiä estämään valtuudettomien henkilöiden pääsy (esimerkiksi lukeminen tai muuttaminen) lähdekoodiin.
c) Kehitysjärjestelmä on erillinen, ei-tuotannollinen järjestelmä.
d) Käytössä olevan ohjelmiston lähdekoodi säilytetään siten, että vain valtuutetuilla henkilöillä on pääsy lähdekoodiin. Säilytysmenetelmänä voi olla esimerkiksi tarkoitukseen sopiva tietoväline (cd-levy ja kopiot, paperitulosteet) kassakaapissa. Säilytyspaikkana voi toimia myös esimerkiksi turvallinen pankkiholvi, esimerkiksi kriittisessä käytössä olevan ohjelmiston lähdekoodin varmuuskopion säilytyksessä.
e) Kaikki lähdekoodiin pääsyyn liittyvät tapahtumat (luku, talletus ym.) kirjataan.
f) Jos ohjelmisto hankitaan alihankkijalta, huolehditaan, että ohjelmistotoimittajaan kohdistuvan mahdollisen vahingon varalta lähdekoodi on tallessa. Yleisesti käytetään escrow-sopimusta ja luotettua tahoa lähdekoodin säilytykseen siten, että lähdekoodi on saatavissa käyttöön sopimuksen perusteella esimerkiksi alihankkijan konkurssin sattuessa.
g) Alihankkijan toimittamat tietojärjestelmät ja ohjelmistot alistetaan tarkalle testausprosessille ja niiltä vaadittavasta laadusta on sovittu toimitus- tai hankintasopimuksissa.
h) Tietojen siirtyminen piilossa olevien, piilotettujen tai tahattomien, tiedonvälityskanavien *(covert channel*) kautta estetään. Mahdollisten kanavien olemassaoloa testataan esimerkiksi lähetettävän materiaalin, tiedon, tietovälineiden ja tietoja käsittelevien henkilöiden toiminnan analysoinnilla ja säännöllisellä tarkastamisella.

## A8.4 Muutoksen hallinta

### kontrolli

Muutoksen hallinnan on oltava suunniteltua, dokumentoitua ja ohjattua. Tarpeettomia muutoksia on vältettävä. Kaikkien tuotannollisiin järjestelmiin tehtävien muutosten ja järjestelmien käyttöön ottojen on oltava etukäteen suunniteltuja ja testattuja. Muutostoimenpiteet on ohjattava, toteutettava ja testattava valtuutetun ja osaavan henkilöstön toimesta. Muutostoimien jälkeen tietojärjestelmien toimintaa ja mahdollisesti aiheutuvia ongelmia ja hälytyksiä on seurattava erityisellä tarkkuudella. Alihankkijoilta ja kolmansilta osapuolilta on edellytettävä sellaista toimintaa ja laadukkuutta, mikä noudattaa käytössä olevia muutoksen hallinnan käytäntöjä. Tarvittaessa käyttöön otettavat järjestelmät ja ohjelmistot on sertifioitava. Muutoksen hallintaan liittyviä seikkoja on löydettävissä myös luvusta *tietojärjestelmien käytön ja tiedonvälityksen turvallisuus* kappaleesta *muutoksen hallinta.*

### käytännön ohjeita

a) Käytettävät ja hyväksytyt muutoksenhallintatoimet ja -menetelmät dokumentoidaan. Muutoksissa noudatetaan ainoastaan hyväksyttyjä toimia ja ainoastaan valtuutetut henkilöt ovat mukana muutosten toteuttamisessa.
b) Muutosten suunnittelussa käytetään sopivaa muutospyyntö- ja tarvekartoitusmenetelmää, jolla arvioidaan tarve kehitystyölle ja muutoksille.
c) Kaikkien käyttöön otettavien ohjelmistojen osalta varmistetaan, että organisaatiolla on käyttöön tarvittavat lisenssit.
d) Ainoastaan tarpeelliset muutokset toteutetaan. Esimerkiksi käyttöjärjestelmistä ja muista valmisohjelmistoista julkaistavat uudet versiot otetaan käyttöön ainoastaan silloin, kun siihen on todellinen tarve (esimerkiksi tiedossa olevien ohjelmistovirheiden korjaukset, parantuneet ominaisuudet tai suorituskyky, ylläpitotoiminnan loppuminen vanhoihin versioihin).
e) Suunnitellut muutokset, niiden piirteet ja toiminnot kuvataan. Kaikki muut järjestelmät, joihin muutokset vaikuttavat, dokumentoidaan ja niissä mahdollisesti tarvittavat muutokset kuvataan.

f) Jos muutokset vaikuttavat olemassa oleviin jatkuvuussuunnitelmiin, tietoturvallisuus- tai muihin määrityksiin tai käytäntöihin, nämä on ensin päivitettävä vastaamaan tai vähintään varautumaan muutosten jälkeiseen tilanteeseen.

g) Muutoksenhallintasuunnitelmat edellyttävät riskien analysoinnin, muutosten vaikutusten arvioinnin ja muutosten jälkeen vaadittavien uusien tietoturva- ja muiden määrittelyiden kuvaamisen.

h) Muutoksenhallintatoimista kuvataan ainakin vaadittavat toimenpide- ja ohjaussuunnitelmat ja -käytännöt, muutosmäärittelyt, dokumentaatio, testausmenettelyt ja laaduntarkastus.

i) Huomiota kiinnitetään tarpeellisiin dokumentaatioon tehtäviin uudistuksiin: erityisesti käyttäjän dokumentaation, erilaisten toimintaohjeiden ja järjestelmädokumentaation muutoksiin.

j) Muutoksissa käytetään asianmukaista versionhallintaa.

k) Muutoksille on olemassa hyväksymismenettely, joka on mukana muutoksen ohjausprosessissa.

l) Muutoksista tiedotetaan sovitun käytännön mukaisesti sekä etukäteen että jälkikäteen. Käyttäjien mahdollisesti tarvitsema ohjeistus toimitetaan etukäteen ja koulutus järjestetään tarvittaessa.

m) Tietojärjestelmät testataan suunnitelmien mukaan. Testauksessa noudatetaan riittävää tarkkuutta ja laajuutta. Kaikki testaustoimet kirjataan ja hyväksytään ennen tietojärjestelmän käyttöönottoa.

n) Testauksessa huomioidaan mahdollisuuksien mukaan kaikki tietoturvallisuuteen vaikuttavat tekijät, myös esimerkiksi käyttöliittymän sopivuus ja käyttökelpoisuus.

o) Testausta varten on varattu oma testijärjestelmä. Erilaisia uusia toimintoja voidaan testata kehitysjärjestelmissä, mutta kokonaisuus testataan erillisessä testijärjestelmässä ennen käyttöönottoa.

p) Tietojärjestelmien uusien piirteiden käyttöönoton tai muutosten toteuttamisen jälkeen hälytysjärjestelmät konfiguroidaan vastaamaan muuttunutta tilannetta.

q) Käyttöönoton jälkeisenä aikana noudatetaan tehostettua tarkkailua ja valvontaa. Käyttöönotetut järjestelmät ja muutokset katselmoidaan ja katselmoinnin tulokset kirjataan ja hyväksytään osana hyväksymismenettelyä.

r) Käyttöönoton tai päivityksen uuteen versioon tekee henkilö, jolla on toimenpiteeseen tarvittava koulutus, osaaminen ja riittävät valtuudet.

s) Kaikista järjestelmän muutoksista pidetään lokia.

t) Järjestelmän konfiguraatiotiedot talletetaan ja muutoksen yhteydessä päivitetään vastaamaan uutta tilannetta.

u) Vanhat ohjelmistoversiot ja tarvittavat konfiguraatiotiedot säilytetään mahdollista palautusta varten.

v) Varmistetaan, että uudella ohjelmistoversiolla luotu tieto on käytettävissä tai konvertoitavissa käytettäväksi myös vanhalla ohjelmistoversiolla.

w) Alihankkijat ja kolmannet osapuolet sitoutuvat toimimaan käytössä olevien muutoksenhallintamenettelyiden mukaisesti. Osapuolten sitoutuminen varmistetaan sopimuksellisesti.

x) Muutosten jälkeen tarkastetaan muutosten yhteydessä mahdollisesti syntyneet piilossa olevat kommunikointikanavat (*covert channel*), joita ei ole suunniteltu. Tällaisia voivat olla esimerkiksi henkilöiden toimintaan liittyvät kanavat (uusien ylläpitomenetelmien yhteydessä ylläpidossa tarvittavien tietojen välityksessä siirretään vahingossa arkaluonteisia tietoja) tai erilaiset haittaohjelmat (Troijan hevonen, *Trojan horse*: ohjelma, jonka tarkoitus on välittää salaa tietoja organisaation ulkopuolelle tai luoda ylimääräinen sisäänpääsy organisaation tietojärjestelmiin Internetistä).

# 11 Toiminnan jatkuvuus

## 11.1 Yleistä

Toiminnan jatkuvuussuunnittelun tarkoitus on yhtäältä estää organisaation toiminnan, liiketoiminnan ja ydinprosessien keskeytyminen tai vahingoittuminen. Mahdolliset kriisitilanteet ja niiden vaikutukset torjutaan mahdollisuuksien mukaan. Toisaalta toteutuneista riskeistä ja kriisitilanteista, joilta ei ole onnistuttu suojautumaan, toivutaan normaalitilaan suunnitellusti ja mahdollisimman nopeasti. Organisaatiossa on oltava riittävä valmius myös vakavissa kriiseissä toimimista varten. Tämä valmius sisältää sekä valmiussuunnitelman, henkilöiden nimeämisen ja tehtävien määrittämisen, resurssien varaamisen että mahdollisen harjoittelun. Vakavassa kriisissä myös henkilöiden turvallisuuteen ja terveyteen saattaa kohdistua uhkia. Tyypillisimpiä tällaisia kriisejä ovat tulipalot.

Voidaan sanoa, että toiminnan jatkuvuuden suunnittelu kuuluu organisaation tietohallinnon ylimmän tason prosesseihin, ja se ohjaakin koko tietoturvatoimintaa suunnittelusta toteutukseen. Toiminnan eriasteinen keskeytyminen tai vahingoittuminen voi johtua teoriassa kaikista niistä erilaisista uhkista ja riskeistä, joihin varaudutaan muun muassa tämän dokumentin mukaisilla toimenpiteillä. Jatkuvuussuunnittelun ansioista riskit ja vahingot voidaan torjua etukäteen hyväksytylle tasolle ja niistä voidaan selviytyä suunnitelmien mukaisesti. On myös tärkeää, että toteutuneet ongelmat analysoidaan, niistä opitaan ja vastaisuudessa niihin voidaan varautua entistä paremmin.

Kriisitilanteista selviytymisen toimenpiteet voidaan jakaa kahteen osaan. Varautumistoimilla varaudutaan riskeihin ja ennakoidaan niitä jo etukäteen. Tarkoituksena on ehkäistä kriisitilanteet, riskien syntyminen tai vaikutukset. Varautumistoimia voivat olla esimerkiksi päivittäiset huoltotoimet sekä erilainen tarkkailu ja hälytykset. Toipumistoimet puolestaan ovat niitä toimenpiteitä ja menettelyitä, joihin ryhdytään toteutuneesta kriisistä toipumiseksi. Tässä luvussa keskitytään erityisesti toipumistoimiin ja niiden suunnitteluun.

Jatkuvuussuunnittelun vaatimat erilaiset tekniset toimet havaittujen ongelmien tai vikojen korjaamiseksi ja tarvittaviin muihin toimiin ryhtymiseksi on tarkemmin kuvattu luvussa *poikkeustilanteet*. Toiminta poikkeustilanteissa on oleellinen osa jatkuvuussuunnittelua ja organisaation tietoturvallisuuden kehittämistä ja ylläpitoa.

## 11.2 Uhkista ja riskeistä

Esimerkkejä toiminnan jatkuvuuteen kohdistuvista yleisistä uhkista on lueteltu alla. Jokainen esimerkki on tarkennettavissa huomattavasti yksityiskohtaisemmaksi tai jaettavaksi useisiin pienempiin osiin, jolloin myös tarkempi analyysi uhkan vaikutuksista on mahdollinen ja riskiltä voidaan tehokkaasti suojautua.

a) Organisaatiossa ei ole käytössä jatkuvuussuunnitelmaa.
b) Jatkuvuussuunnittelu ei toimi yhteystyössä organisaation johdon, liiketoiminnan johdon, tietohallinnon ja tietoturvahallinnon kanssa.
c) Organisaatiossa ei ole valmiuksia vakavassa kriisissä toimimiseen ja kriisistä toipumiseen – henkilöstöä ei ole varattu ja koulutettu, resursseja ei ole varattu tai valmiussuunnitelma puuttuu.
d) Tärkeitä prosesseja ja riskejä ei ole tunnistettu eikä suojausta ole priorisoitu.
e) Jatkuvuussuunnittelua ei kehitetä eikä testata. Muutokset organisaation toimintaympäristössä saavat aikaan jatkuvuussuunnitelmien vanhentumisen.
f) Kriisitilanteita varten ei ole määrätty vastuita eikä varattu resursseja.
g) Ei ole hankittu riittäviä ulkopuolisia vakuutuksia.
h) Jatkuvuussuunnitelmiin ei ole merkitty vastuita, toimenpiteitä ja aikatauluja riittävällä tarkkuudella.

i) Henkilöstöllä ei ole valmiuksia toimia kriisitilanteessa.
j) Kriisitilanteita ei harjoitella tai kaikki tarvittavat henkilöt eivät osallistu harjoituksiin.
k) Kriisitilanteessa jatkuvuussuunnitelmasta ei ole käytettävissä ajantasaista kopiota.
l) Kriisien harjoitusten ja testaamisen tuloksia ei käytetä hyväkseen toiminnan parantamisessa tai suunnitelmien päivittämisessä.

## A9.1 Jatkuvuussuunnittelun prosessi

### kontrolli

Organisaatiossa on oltava jatkuvuuden suunnittelun prosessi. Prosessin omistuksen täytyy olla organisaation johdolla ja sen täytyy kuulua sekä liiketoiminnan johtamisen että tietohallinnon ylimpiin prosesseihin.

### käytännön ohjeita

a) Organisaation jatkuvuussuunnittelua ohjataan prosessilla, jonka organisaation johto omistaa. Jatkuvuussuunnittelu keskittyy organisaation ydintoimintaan ja tärkeimpien prosessien turvaamiseen.
b) Prosessi on saumattomassa vuorovaikutuksessa sekä organisaation ja liiketoiminnan johtamisen, tietohallinnon että tietoturvahallinnon prosessien kanssa.
c) Prosessissa ymmärretään ja arvioidaan uhkat ja riskit, jotka voivat estää tai haitata organisaation toimintaa. Riskien todennäköisyys ja vaikutus on arvioitu.
d) On tunnistettu organisaation ydinprosessit, joiden jatkuminen on turvattava ja joissa tarvittava tieto on suojattava.
e) Turvattaville prosesseille ja organisaation suojattaville tiedoille on määritetty suojauksen tavoitetaso ja prioriteetti. Organisaation päivittäinen toiminta on linjassa tavoitteiden ja prioriteettien kanssa.
f) Jatkuvuussuunnittelua arvioidaan ja kehitetään. Jatkuvuussuunnittelun prosessi ohjaa käytössä olevien jatkuvuussuunnitelmien testaamista ja kehittämistä.
g) Kriisitilanteiden käytännön toteutuksia ja toimenpiteitä varten määritellään vastuut ja varataan resurssit, mukaan lukien tarvittavat kahdennetut tietojärjestelmät, peilatut levyt, RAID-järjestelmät *(redundant array of independent disks*) ja varmistetut tietoliikenneyhteydet.
h) Tarvittaessa toiminta suojataan vakuutuksilla. Vakuutukset voivat suojata niiltä riskeiltä, joilta suojautumiseen ei ole muuten riittävästi resursseja sekä niiltä riskeiltä, joita ei ole tunnistettu. Vakuutus voi myös antaa lisäturvaa tiettyä vahinkoa vastaan, vaikka tältä olisikin suojauduttu.
i) Arvioidaan, voidaanko tietojärjestelmien toimintakyvystä riippuva kriittinen toiminta korvata ei-tietojärjestelmäsidonnaisella toiminnalla.
j) Vakavia kriisejä, esimerkiksi tulipalotilanteita varten, niissä toimimista ja niistä toipumista varten tehdään varautumissuunnitelma, nimetään ja koulutetaan tarpeellinen määrä henkilöitä, varataan muut tarvittavat resurssit ja harjoitellaan kriisitilanteissa toimimista riittävästi. Suunnitelmassa otetaan huomioon kriisitilanteen aikainen tietojen luottamuksellisuuden ja turvallisuuden säilyttäminen siten, että esimerkiksi pelastushenkilökunnalla ei ole asiatonta pääsyä tallennettuihin tietoihin.

## A9.2 Riskien arvioinnin prosessi

### kontrolli

Jatkuvuussuunnittelussa täytyy aluksi tunnistaa sekä organisaation ydinprosessit niissä tarvittavine ja käytettävine tietoineen että tapahtumat, jotka voivat aiheuttaa näiden prosessien keskeytymisen, tuottaa prosesseille vahinkoa, estää prosessien tarvitsemien tietojen käyttöä tai tuhota tietoja. Tuloksena

on riskien arviointi, jossa on arvioitu riskin toteutumisen todennäköisyys ja vaikutus (mihin vaikuttaa ja millä vakavuudella).

### käytännön ohjeita

a) Riskien arvioinnin prosessi on osa jatkuvuussuunnittelun prosessia, ja sitä johdetaan tarkoituksenmukaiselta tasolta. Osana jatkuvuussuunnittelun prosessia myös riskien arvioinnin voidaan suositella olevan suoraan organisaation ylimmän johdon alaisuudessa.
b) Riskien arvioinnissa on mukana riittävä määrä henkilöitä organisaation eri tasoilta. Arviointi sisältää kaikkiin ydinprosesseihin ja niissä käytettäviin kriittisiin tietoihin kohdistuvat riskit eikä siten ole rajoittunut ainoastaan tietoteknisiin riskeihin.
c) Riskiarviota ja sen tuloksia käytetään jatkuvuus- ja tietoturvallisuussuunnittelussa ja niiden riskienhallintaa määritettäessä.
d) Riskien arvioinnissa huomioidaan erityisesti yksittäisten riskien aiheuttamat vahingot (*'single point of failure')*, ja pyritään suojautumaan tällaisilta riskeiltä.

## A9.3 Jatkuvuussuunnittelun käytännön toteutus

### kontrolli

Organisaation toiminnan, liiketoiminnan ja ydinprosessien turvaamiseksi on luotava jatkuvuussuunnitelmat, joiden avulla varaudutaan sekä estämään riskit, minimoimaan niistä aiheutuvat haitat että toipumaan normaalin toiminnan tilaan suunnitelluissa aikatauluissa.

### käytännön ohjeita

a) Tunnistetaan tarvittavat varautumistoimet, toipumistoimet, varasuunnitelmat ja osalliset henkilöt. Sovitaan kaikista vastuista kaikkiin menettelyihin liittyen.
b) Organisaation toiminnan kannalta välttämättömät henkilöt (avainhenkilöt) on tunnistettu.
c) Luetellaan ja ohjeistetaan varautumistoimet yksityiskohtaisesti ja selkeästi.
d) Varautumistoimista pidetään kirjaa. Lokitietoon kirjataan tarpeelliset ja riittävät tiedot, esimerkiksi toimenpide, suorittaja ja aika.
e) Luetellaan ja ohjeistetaan toipumistoimet yksityiskohtaisesti ja selkeästi. Toipumistoimiin liittyvät aikarajat kirjataan.
f) Kriisitilanteen jälkeisistä toipumistoimista pidetään kirjaa. Lokitietoon kirjataan tarpeelliset ja riittävät tiedot, esimerkiksi toimenpide, suorittaja ja aika sekä tieto tapahtumasta, viasta tai ongelmasta.
g) Jos kriisillä voi olla vaikutusta muiden organisaatioiden, esimerkiksi yhteistyökumppanien toimintaan, noudatetaan erityistä tarkkaavaisuutta ja informoidaan muuta organisaatiota suunnitellusti tarpeen mukaan.
h) Huolehditaan, että tarvittavat henkilöt ovat saaneet kriisitilannekoulutuksen ja osaavat toimia oikein.
i) Kriisitilanteita harjoitellaan. Harjoittelusta on mainittu lisää kappaleessa *jatkuvuussuunnitelman testaaminen ja ylläpito*.
j) Jatkuvuussuunnitelmia kehitetään. Muutokset organisaation toiminnassa ja menetelmissä huomioidaan jatkuvuussuunnitelmissa. Varautumis- ja toipumistoimien tehokkuutta testataan määräajoin ja tehdään tarvittavat muutokset suunnitelmiin ja proseduureihin.
k) Jatkuvuussuunnitelmasta säilytetään ajantasaista kopiota organisaation tilojen ulkopuolella riittävän turvallisuuden omaavassa paikassa siten, että organisaatioon, sen tiloihin tai henkilöstöön kohdistunut kriisi ei estä toipumistoimia.

## A9.4 Jatkuvuussuunnitelman testaaminen ja ylläpito

### kontrolli

Jotta jatkuvuussuunnitelmat olisivat ajantasaisia ja tehokkaita, niitä on testattava ja ylläpidettävä määräajoin sekä kriisien harjoittelulla että testaamalla yksittäisten toimenpiteiden tehokkuutta ja onnistumista. Epäonnistuneet testit käynnistävät arvioinnin, jonka perusteella voidaan parantaa toipumismenettelyitä, tilanteen tai olosuhteen väliaikaisesti korjaavia varasuunnitelmia tai päivittää jatkuvuussuunnitelmia vastaamaan muuttuneita olosuhteita ja uusia tilanteita.

### käytännön ohjeita

a) Kaikki tarvittavat henkilöt osallistuvat testaukseen ja harjoituksiin. Kriisien harjoittelu on säännöllistä.
b) Harjoitukset suunnitellaan ja niille laaditaan aikataulu etukäteen. Tarvittaessa kriisitilannetta voidaan harjoitella myös siten, että kaikki mukana olevat eivät tiedä, että kyseessä on harjoitus.
c) Harjoitusten tavoite ja tulos kirjataan. Harjoitusten ja testien kulusta pidetään lokia.
d) Harjoitellaan erilaisia skenaarioita simuloimalla sekä yksittäisiä vikatilanteita että kokonaisten palveluiden tai järjestelmien vikaantumista. Testataan esimerkiksi kahdennettujen varajärjestelmien, varamenetelmien, varalla olevien tilojen ja varavoiman toimivuutta ja varmistusten palautusten toimivuutta. Tilanteissa huomioidaan kokonaisuuden toimiminen: organisaation, henkilöstön, tietojärjestelmien, kommunikaation, toimitilojen ja prosessien toiminta on oltava ongelmatonta.
e) Harjoitusten ja testauksen epäonnistuminen aiheuttaa selvityksen epäonnistumisen syystä. Syy korjataan mahdollisuuksien mukaan (esimerkiksi tekninen, ohjeistukseen tai toimintaan liittyvä syy). Tarpeen mukaan toipumissuunnitelmat päivitetään ajantasaisiksi, kun syy on esimerkiksi muutos organisaatiossa, sen toiminnassa, prosesseissa tai käytetyissä teknologioissa.

## A9.5 Jatkuvuussuunnitelman sisältö

### kontrolli

Jatkuvuussuunnitelman täytyy sisältää riittävät ja tarpeelliset tiedot, jotta kriiseihin voidaan varautua, kriisitilanteista toipua ja jotta kriisejä voidaan testata ja harjoitella onnistuneesti. Suunnitelman täytyy olla ajan tasalla ja saatavissa kaikissa tilanteissa.

### käytännön ohjeita

Jatkuvuussuunnitelmassa on mainittava ainakin,

a) mikä tapahtuma tai olosuhde käynnistää suunnitelman toimenpiteet,
b) mitkä ovat noudatettavat toimenpiteet ja kenellä on niistä vastuu (luetellaan yksittäiset toimenpiteet, henkilöt ja varahenkilöt),
c) millä aikataululla toimiin on ryhdyttävä,
d) millä toipumistoimilla organisaation kriittisin toiminta ja palvelut saadaan jatkumaan esimerkiksi väliaikaisissa toimitiloissa tai väliaikaisilla menetelmillä (varasuunnitelma),
e) millä toimilla koko organisaation toiminta palautuvat normaaleiksi ja toimenpiteet kriisistä raportoimiseen,
f) tarvitaanko paikalla lääkäriä, poliisia, palokuntaa tai muita viranomaisia,
g) tarvitseeko yhteistyökumppaneita, alihankkijoita, asiakkaita, muita organisaatioita tai tiedotusvälineitä informoida, sekä
h) tietoja suunnitelmasta, kuten suunnitelman omistaja ja ylläpitoprosessi, harjoittelu- ja testausmenettely sekä mahdolliset osaamisvaatimukset vastuullisille henkilöille.

# 12 Laillisuus ja sääntöjen mukaisuus

## 12.1 Yleistä

Organisaatioiden toiminnan on oltava lainmukaista ja otettava huomioon tarpeen mukaan erilaiset säännöt ja standardit. Lakien noudattaminen, sen lisäksi että se on eettisesti ja moraalisesti ainoa hyväksyttävä tapa toimia, suojaa organisaatiota mahdollisten oikeustoimien ja korvausten vaikutuksilta.

Tietoturvallisuuteen liittyen säädöksiä löytyy esimerkiksi arkaluonteisten tietojen käsittelyyn, säilytykseen, suojaamiseen ja käytettävään tiedonvälitykseen liittyen. Huomioitavia lakeja on suuri määrä, mutta tässä yhteydessä keskitytään pääasiassa ainoastaan sosiaali- ja terveydenhuollon asiakkaan ja potilaan henkilö- ja potilastietojen suojaamiseen. Kappaleessa *noudatettavat lait* on mainittu henkilötietojen tai potilasasiakirjojen käsittelystä ja säilytyksestä säädetyistä laeista. Muiden lakien osalta ei ole mainittu voimassa olevia säännöksiä, joita tulisi huomioida.

Tietoturvalliselle toiminnalle voi kohdistua uhkia tyypillisesti esimerkiksi erilaisten tekijänoikeuksien ja omistusoikeuksien rikkomuksista. Lisäksi esimerkiksi asiakkaiden, yhteistyökumppaneiden ja alihankkijoiden kanssa solmitut sopimukselliset velvoitteet voivat edellyttää organisaatiolta toimia, joiden laiminlyönneistä se voi joutua oikeudelliseen vastuuseen. Sopimuksista tulevien velvoitteiden lainmukaisuus on luonnollisesti selvitettävä.

Lakien lisäksi erityisesti terveydenhuoltoon kohdistuu erilaisia eettisiä periaatteita, sääntöjä, ohjeita, standardeja ja sopimuksia, jotka on otettava huomioon henkilö- ja potilastietojen käsittelyssä ja säilytyksessä.

Terveydenhuollossa käytettävien tietojärjestelmien on erityisesti ohjattava ja pakotettava käyttäjät lainmukaiseen toimintaan ja estettävä väärinkäytökset. Tietojärjestelmille asetettavia vaatimuksia on lueteltu luvussa *tietojärjestelmien kehitys ja ylläpito*.

## 12.2 Uhkista ja riskeistä

Alla on lueteltu mahdollisia uhkia ja riskejä, joiden toteutuessa organisaatiolle voi kohdistua eriasteisia oikeudellisia vaikutuksia ja vastuita. Näiltä on syytä välttyä analysoimalla riskit tarkemmin ja suojautumalla niiltä.

a) Organisaatiossa ei tunneta voimassa olevia lakeja ja määräyksiä.
b) Organisaation toiminnassa ei välitetä voimassa olevista laeista ja määräyksistä.
c) Organisaatiossa ei ole huomattu, että sen tietojen käsittely tai säilytys ei ole lainmukaista.
d) Organisaatiossa on käytössä luvattomia ohjelmistoja.
e) Organisaation käytössä olevia ohjelmistoja käytetään lisenssien vastaisella tavalla.
f) Organisaatiossa tapahtuvan tietojen käsittelyn yhteydessä henkilöllä on mahdollisuus käsitellä tietoja hänelle kuulumattomin valtuuksin, hänelle kuulumattomilla tavoilla tai tarkoituksessa.
g) Henkilöstöllä ei ole tiedossa ohjelmistojen tai tietojen luvattomasta käytöstä aiheutuvista seuraamuksista.
h) Oikeuksien vastaista toimintaa ei tarkkailla tai ohjelmistojen luvaton käyttö ei aiheuta toimenpiteitä.
i) Organisaatiolla ei ole sovittua menettelyä ohjelmistohankintoja varten tai menettely on puutteellinen.
j) Hankittaessa ohjelmistotuotteita organisaatioon ei ole ennalta määritelty ohjelmistoilta vaadittavia tietosuojan ja tietoturvan toteuttavia ominaisuuksia.
k) Tietojärjestelmien ja tietojen käsittelyn turvallisuutta ei tarkkailla eikä niitä varten ole luotu auditoinnin menettelyitä.
l) Organisaatiossa ei noudateta aiheellisia standardeja.

m) Organisaatiossa käytetään luvattomia kryptografisia menetelmiä.
n) Organisaation asiakirjoja ei ole suojattu asianmukaisesti.
o) Organisaation käyttämien julkisen avaimen infrastruktuurin salaisten avainten tai niiden varmuuskopioiden säilytys ei ole riittävästi suojattu.

## A10.1 Noudatettavat lait

### kontrolli

On noudatettava voimassa olevia lakeja, asetuksia ja määräyksiä. Kaikki aiheelliset lait, asetukset ja muut organisaation toimintaa määrittävät säännöt ja sopimukset on kirjattava ja pidettävä ajan tasalla. Tarpeen mukaan on syytä myös kirjata, mitkä nimenomaiset vaatimukset kohdistuvat organisaatioon. Nämä vaatimukset voidaan kohdistaa myös yksittäiseen tietojärjestelmään ja organisaation osaan. Lakien muuttuessa kaikki muutokset on otettava huomioon organisaation toiminnassa.

Tietojärjestelmien kehityksessä ja hankinnassa on otettava lainmukaisuus huomioon. Tietojärjestelmien on oltava toteutettu siten, että ne ohjaavat käyttäjää oikeanlaiseen toimintaan ja että uusia riskejä lakien tai määräysten vastaisesti toimimiseen ei synny huonosti tai puutteellisesti suunnitelluista tietojärjestelmistä. Tämä on tarkemmin kuvattu luvussa *tietojärjestelmien kehitys ja ylläpito*.

### käytännön ohjeita

Noudatetaan kaikkia – muun muassa alla olevia – lakeja ja määräyksiä, joita on säädetty henkilötietojen tai potilasasiakirjojen käsittelystä ja säilytyksestä sekä toimintaan liittyvistä tietoturvavaatimuksista. Lait eivät ole erityisessä järjestyksessä prioriteetin tai minkään muun seikan mukaan. Alla olevien lakien lisäksi tietojen luovuttamista koskevia säännöksiä on useissa esimerkiksi vakuutuksia ja eläkkeitä koskevissa laeissa. Muutokset laeissa ja uudet lait otetaan huomioon organisaation toiminnassa.

a) Laki viranomaisten toiminnan julkisuudesta (621/1999)
b) Henkilötietolaki (523/1999)
c) Laki potilaan asemasta ja oikeuksista (785/1992)
d) Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
e) Laki terveydenhuollon ammattihenkilöistä (559/1994)
f) Laki yksityisestä terveydenhuollosta (152/1990)
g) Erikoissairaanhoitolaki (1062/1989)
h) Työterveyshuoltolaki (1383/2001)
i) Perustuslaki (731/1999)
j) Rikoslaki (531/2000)
k) Arkistolaki (831/1994)
l) Hallintolaki (434/2003)
m) Hallintomenettelylaki (598/1982)
n) Kuntalaki (365/1995)
o) Väestötietolaki (299/2003)
p) Terveydensuojelulaki (763/1994)
q) Kansanterveyslaki (66/1972)
r) Laki terveydenhuollon valtakunnallisista henkilörekistereistä (556/1989)
s) Laki kuolemansyyn selvittämisestä (459/1973)
t) Potilasvahinkolaki (585/1986)
u) Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
v) Laki sähköisistä allekirjoituksista (14/2003)
w) Sähköisen viestinnän tietosuojalaki (516/2004)
x) Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
y) Laki Kainuun hallintokokeilusta (343/2003)
z) Tartuntatautilaki (583/1986)
å) Mielenterveyslaki (1116/1990)

ä) Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001)
ö) Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen, STM:n oppaita 2001:3, liitteessä säilytysajat
aa) Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta (1225/2003)
bb) Sosiaali- ja terveysministeriön asetus sähköisen lääkemääräyksen kokeilusta (771/2003)
cc) Arkistolaitoksen määräys ja ohje valtionhallinnon asiakirjojen seulonnasta ja hävittämisestä (3/06/87)
dd) Arkistolaitoksen päätös 22.12.2000 pysyvästi säilytettävistä tiedoista/asiakirjoista
ee) Arkistolaitoksen määräys ja ohje arkistolain piiriin kuuluvien sähköisten tietojärjestelmien ja tietoaineistojen käsittelystä (126/40/01)
ff) Valtionarkiston päätös 1.9.1989 kunnallisten asiakirjojen hävittämisestä, osa 5 (sosiaalihuollon ja holhoustoimen asiakirjat)
gg) Valtiovarainministeriön ohje tarpeettomiksi tulleiden tietoaineistojen hävittämisestä (VM 21/01/2000)

## A10.2 Tekijänoikeudet

### kontrolli

Organisaation on turvattava, että tekijänoikeuksiin ja muihin vastaaviin liittyviä rikkomuksia ei organisaatiossa tapahdu. Sen käytössä ei saa olla, mukaan lukien yksittäisten henkilöiden käyttö, luvattomia kopioita ohjelmistoista ja mitään ohjelmistoja ei saa käyttää vääränlaisilla lisensseillä. On myös huolehdittava, että esimerkiksi yhteistyökumppaneille tai asiakkaille toimitettavan materiaalin osalta organisaatiolla on tähän toimitukseen oikeus eikä toiminta riko minkään tahon tekijän- tai omistusoikeuksia.

Kaikkien sellaisten tietojen ja sentyyppisen käytön, johon organisaatiolla ei ole oikeutta, tulee olla kiellettyä ja mahdollisuuksien mukaan estettyä. Tietojen käytön tulee olla sallittua vain niihin tietojen osiin sekä siinä laajuudessa ja tarkoituksessa kuin mihin organisaatiolla tai sen henkilöllä on oikeus.

### käytännön ohjeita

a) Tietoturvakäsikirjassa mainitaan periaatteet ja ohjeet tekijänoikeuksien alaisten ohjelmistojen ja muiden tuotteiden käytölle ja jakelulle.
b) Tietoturvakäsikirjassa mainitaan periaatteet ja ohjeet tietojen käytölle.
c) Tietoturvakäsikirjassa mainitaan periaatteet ja ohjeet lisenssien siirtoon muille käyttäjille tai organisaatioille.
d) Henkilötietojen, potilastietojen ja muiden luottamuksellisten tietojen käyttö kuvataan tietosuojapolitiikassa.
e) Käytetään sellaisia ohjelmistoja, jotka estävät automaattisesti sellaisten tietojen käytön, johon käyttäjällä ei ole oikeutta.
f) Käytetään sellaisia ohjelmistoja, jotka sallivat tietojen käytön vain siinä laajuudessa ja tarkoituksessa kuin mihin käyttäjällä on oikeus.
g) Käytetään sellaisia ohjelmistoja, joissa on mahdollisuus kirjata ja tarkkailla tietojen käyttöä sekä asettaa hälytyksiä valtuudettomasta käytöstä.
h) Jos käyttöoikeudesta ei ole täsmällistä selvyyttä ja käyttäjä voi päästä tietoihin esimerkiksi osana muita tietoja tai käyttää niitä tarpeettomassa laajuudessa (jos edellisten kohtien automatiikkaa ei voida käyttää), ohjelmiston on informoitava ja varoitettava käyttäjää mahdollisesta rikkeestä.
i) Ylläpidetään listaa tekijänoikeuksien alaisista ohjelmistoista ja tuotteista osana luvun *omaisuuden hallinta*, kappaleen *inventaario ja luettelointi* mukaisesti.
j) Todisteet ja todistukset oikeuksista, kuten sopimukset, lisenssit, käyttöavaimet ja vastaavat, säilytetään suojatusti.

k) Ohjelmistojen ja muiden tuotteiden hankinnassa käytetään ennalta sovittuja menettelyitä tekijänoikeuksien tarkastamiseen. Hankittujen tuotteiden käyttö suojataan sopimuksellisesti ja siirretään vastuu tekijänoikeusrikkomuksista mahdollisuuksien mukaan toiselle sopimusosapuolelle.
l) Tietoturvakoulutuksissa mainitaan tekijänoikeuksien alaisten tuotteiden käytön periaatteet ja kerrotaan rankaisumenettelyistä. Tarvittaessa järjestetään erilaisia tietoiskuja tai tiedotteita.
m) Hankitaan riittävät auditointityökalut, joilla voidaan tarkkailla ja varmistua, että luvattomia tuotteita ei ole käytössä.
n) Varmistetaan, että henkilökohtaisille tietokoneille ei asenneta eikä niissä käytetä luvattomia ohjelmistoja.
o) Varmistetaan, että monen käyttäjän tietojärjestelmissä ohjelmistojen käyttö ei ylitä käyttölisenssien määrää.
p) Varmistetaan, että rajoitetuilla ohjelmistolisensseillä olevia tuotteita ei käytetä toiminnoissa, joihin lisenssi ei oikeuta (esimerkiksi käytössä voi olla vain lukuoikeus ilman muokkausta).
q) Varmistetaan, että organisaation henkilöiden käyttäessä erilaisia tietoverkoissa olevia palveluita ja ohjelmistoja heillä on tähän käyttöön tarvittavat valtuudet.
r) Varmistetaan, että tietoverkoissa olevia palveluita ei yritetä käyttää väärillä käyttäjätunnuksilla.
s) Kaikkien tekijänoikeuksien alaisten ohjelmistojen käyttöä tarkkaillaan mahdollisuuksien mukaan ja kaikkiin väärinkäytöksiin puututaan.
t) Kaiken organisaation omaisuuden ja sen hallussa olevan omaisuuden käyttö on luvanvaraista ja väärinkäyttö on kiellettyä. Käyttöä tarkkaillaan ja väärinkäytöstä raportoidaan mahdollisuuksien mukaan. Havaittu väärinkäyttö käynnistää aina asianmukaiset korjaus- ja rankaisutoimenpiteet.

## A10.3 Standardit ja muut säännöt

### kontrolli

On noudatettava organisaation toimintaa ja toimialaa koskevia ja muita aiheellisia standardeja ja muita voimassa olevia sääntöjä ja ohjeita (esimerkiksi viranomaisten hyvän tietojenkäsittelytavan periaatteet).

### käytännön ohjeita

a) Organisaation toimintaa koskevat ja toiminnassa huomioon otettavat standardit listataan ja niiden muutoksia seurataan. Toimitaan vaadittavien standardien mukaisesti.
b) Tietojärjestelmien tekninen standardien mukaisuus arvioidaan säännöllisesti siihen valtuutettujen henkilöiden toimesta. Tarvittaessa toteutetaan tietojärjestelmiin vaadittavat muutokset siitä erikseen määritellyllä tavalla (katso esimerkiksi luku *tietojärjestelmien kehitys ja ylläpito*).
c) Luvanvaraisia tai kiellettyjä kryptografisia menetelmiä ei käytetä ilman asianmukaista lupaa.
d) Jos organisaation käyttämien kryptografisten menetelmien käyttötarkoitukselle on säädetty erillisiä kieltoja (esimerkiksi ohjelmistojen, laitteiden tai algoritmien vienti tai tuonti, salausavainten pituus, salauksen purkumenetelmien käyttö), näitä määräyksiä noudatetaan.

## A10.4 Sopimukset, politiikat ja muut organisaation asiakirjat

### kontrolli

Sopimusten ja muiden organisaation asiakirjojen laadinnassa, ylläpidossa ja säilytyksessä on noudatettava lakien asettamia vaatimuksia. Myös organisaation sopimuksellisista sitoumuksista (myös

esimerkiksi escrow) tai sen itsensä julkaisemista periaatteista ja sertifioidusta toiminnasta koituvia velvoitteita on noudatettava.

Lakeja ja velvoitteita on noudatettava myös esimerkiksi julkisen avaimen infrastruktuurissa tarvittavien organisaation salaisten avainten ja niiden varmuuskopioiden luomisessa, varmuuskopioinnissa ja säilytyksessä. Näissä käytettävät menettelyt julkaistaan tyypillisesti organisaation varmennepolitiikassa.

## käytännön ohjeita

a) Asiakirjat voidaan jakaa asiakirjan tyypin ja siitä koituvien velvoitteiden mukaisesti tarpeellisiin luokkiin, joiden laatimista, käsittelyä ja säilytystä koskevat kutakin omat periaatteet ja säännöt erilaisiin lakeihin, sopimuksiin ja muutoin julkaistuihin velvoitteisiin perustuen.

b) Asiakirjoja ja tietoja säilytetään sellaisessa muodossa ja formaatissa sekä siten, että niiden valtuudeton muuttaminen, käyttö tai tuhoaminen, vääränlainen käyttö tai muu vaarantaminen on estettyä.

c) Sopimusten luomis-, ylläpito- ja säilytyskäytännöt noudattavat säädettyjä lakeja.

d) Toimittaessa kolmansien osapuolten kanssa organisaation ja sen työntekijöiden sopimukselliset vastuut kolmatta osapuolta kohden pyritään minimoimaan.

e) Organisaation asiakirjat, omaisuus ja muut asiat, joiden säilytyksestä on sovittu escrow-sopimuksilla, säilytetään näiden sopimusten mukaisesti.

f) Muiden organisaation asiakirjojen, kuten erilaisten viranomaisten vaatimien organisaation hallintoon, toimintaan ja rahoitukseen liittyvien asiakirjojen luomis-, ylläpito- ja säilytyskäytännöt noudattavat säädettyjä lakeja.

g) Organisaation itsensä julkaisemia periaatteita asiakirjojen käsittelystä ja säilytyksestä esimerkiksi tietosuojapolitiikassa, tietoturvapolitiikassa, varmennepolitiikassa ja muissa julkistetuissa toimintakäytännöissä noudatetaan.

h) Asiakirjojen säilytyksessä ja käsittelyssä toimitaan sertifioinnin mukaisesti ja noudatetaan sertifikaatissa mainittuja käytäntöjä.

i) Julkisen avaimen infrastruktuurissa käytettävät salaiset avaimet ja niiden varmuuskopiot säilytetään turvallisesti ja säilytys kuvataan varmennepolitiikassa.

j) Tietojen suojaamisessa ja turvaamisessa noudatetaan säädettyjen lakien lisäksi organisaation julkaisemia tietosuoja- ja tietoturvapolitiikkoja sekä aiheellisia tietoturvallisuuteen liittyviä standardeja ja määräyksiä.

k) Tietojen ja tietojärjestelmien suojaaminen sekä lakien, standardien ja sääntöjen mukaisuus arvioidaan ja auditoidaan säännöllisesti ja sovitun menetelmän mukaisesti siihen valtuutettujen henkilöiden toimesta. Auditoinnin tulosten perusteella ryhdytään mahdollisiin korjaaviin, organisaation strategioissa, suunnitelmissa ja toimintatavoissa määriteltyihin toimiin.

# 13 Poikkeustilanteet

## 13.1 Yleistä

Tietoturvaloukkausten ja normaalista poikkeavien tilanteiden valvonta ja seuranta, havaitseminen ja raportointi sekä oikeisiin toimenpiteisiin ryhtyminen ongelmien korjaamiseksi ja mahdollisten seuraamusten määrittämiseksi ovat oleellinen osa tietoturvallisuuden ylläpidon prosessia.

Valvonnalla, seurannalla ja erilaisella tarkkailulla on tarkoitus havaita kaikki poikkeamat ja valtuudeton toiminta organisaatiossa, mikä voi vaarantaa tietojenkäsittelyn ja tietojen turvallisuuden. Seuranta sisältää menetelmät kiinteistön ja tilojen valvonnasta (esimerkiksi kulunvalvonta, tunnistimet ja hälyttimet, kameravalvonta) tietojärjestelmien tilan ja niitä käyttävien henkilöiden ja tapahtumien seurantaan ja kirjaamiseen. Tapahtumaseurannassa kirjataan sekä henkilöiden toimenpiteet että järjestelmässä automaattisesti tapahtuvat toiminnat mukaan lukien erilaiset vika- ja häiriötilanteet.

Valvonnasta saatujen tapahtumatietojen, lokitiedostojen, nauhojen ja vastaavien säilytysaika ja säilytystapa on määriteltävä. Joidenkin seurantatietojen osalta säilytysaika voi olla pitkä, kuten lokitietojen luottamuksellisten tietojen käsittelystä. Mahdollisesti todistusaineistona tarvittavien tietojen säilytys takaa sekä organisaation, yksittäisen henkilön että organisaation sidosryhmän oikeusturvan säilymisen.

Poikkeamista ja havaituista loukkauksista raportoidaan välittömästi ja tehdään riittävät hälytykset, joko automaattisesti tai havaitsevan henkilön toimesta. Hälytys käsitellään sekä tietoturvaorganisaatiossa, jotta korjaaviin toimenpiteisiin voidaan ryhtyä mahdollisimman pikaisesti, että johdossa, jotta mahdolliset seuraamukset voidaan määritellä. Henkilöstöllä ja kolmansilla osapuolilla on oltava tieto, miten ja kenelle pitää raportoida havaitsemistaan potentiaalisista tietoturvallisuuteen vaikuttavista tietojärjestelmien haavoittuvuuksista, ongelmista tai epäilyttävistä tilanteista.

Johdon yhtenä velvollisuutena on arvioida tietojen turvaamistoiminnan tehokkuutta, jotta riittävä taso voidaan saavuttaa ja sitä voidaan ylläpitää. Tehokkuuden selvittämiseksi tietoturvatoimintaa täytyy mitata, mihin sisältyy myös poikkeustilanteissa toimimisen mittaaminen ja toiminnan laadun arviointi. Suuri osa mittareista määräytyy luonnollisesti normaalista päivittäisestä toiminnasta ja koko tietoturvallisuusprosessin toimivuudesta. Tällöin mitään loukkauksia ei välttämättä tapahdu, vaan voidaan mitata ainoastaan sitä, onko turvaamistoiminta määritysten mukaista. Poikkeustilanteissa tehtävät havainnot antaa johdolle kuitenkin erityisen hyvää palautetta, jonka avulla turvaamistoimintaa voidaan kehittää. Tarkastelemalla ja mittaamalla hälytysten aiheellisuutta, hälytyksen syntymistä kaikista aiheellisista tapahtumista, hälytyksen syntymiseen kuluvaa aikaa ja toiminta-aikaa ongelmien korjaamiseksi voidaan mahdollisia seuranta- ja hälytysmekanismeja lisätä ja parantaa sekä tarvittaessa organisoida tietoturvatoiminta entistä tehokkaammaksi.

## 13.2 Uhkista ja riskeistä

Tietoturvaloukkausten havaitseminen on erittäin tärkeä osa tietoturvallisuutta ja sen kehittämistä. Jos tätä osa-aluetta ei pystytä hallitsemaan, se vaikuttaa laskevasti koko tietoturvallisuuden tasoon ja siten myös organisaation toimintaan. Alla on mainittu muutamia aiheeseen liittyviä uhkia.

a) Tapahtumien kirjaamisen taso ei vastaa tietojärjestelmien kriittisyyttä tai niihin kohdistuvien riskien vakavuutta.
b) Henkilöiden havaitsemille rikkeille ei ole sovittu käytäntöä.
c) Alihankkijoiden kanssa solmitut ylläpitosopimukset eivät kata vikatilanteen korjaamista riittävän nopeasti.
d) Tapahtumatietoihin pääsee käsiksi ilman tarvittavia valtuuksia tai niitä pystyy muuttamaan ja tuhoamaan.
e) Tapahtumatietojen käyttö ongelmatilanteiden selvittelyssä vaarantaa tapahtumatietojen eheyden tai luottamuksellisuuden.

f) Järjestelmien ja sovellusten tapahtumakirjaus ei ole käytössä tai se ei ole riittävän yksityiskohtainen.
g) Häiriö- tai ylikuormitustilanteita ei havaita.
h) Lokitiedosto kasvaa liian suureksi ja lokitapahtumia menetetään tai järjestelmän toimintaan tulee häiriöitä.
i) Vanhoja tapahtumatietoja ei säilytetä riittävän tietoturvallisesti.
j) Kiinteistön ja toimitilojen valvonta on puutteellista.
k) Valvonnassa syntyviä tietoja ei seurata.
l) Seurannasta ei synny hälytyksiä.
m) Puutteelliset hälytystiedot aikaansaavat vääränlaiset korjaustoimet.
n) Hälytykset eivät käynnistä korjaustoimenpiteitä eikä muita seuraamuksia.
o) Poikkeamia ei mitata ja niiden perusteella ei tarkasteta ja kehitetä organisaation tietoturvallisuustoimintaa.

## A11.1 Toiminnan määrittelyt

### kontrolli

Jotta tarvittavien tapahtumien kirjaaminen, seuranta onnistuu tarpeellisella tavalla ja vaadittaviin toimenpiteisiin voidaan ryhtyä, on tämä toiminta määriteltävä yhteismitallisesti kaikkien aiheellisten tietojärjestelmien osalta. Käytettävistä menettelyistä on yksityiskohtaisempia tietoja seuraavissa kappaleissa.

Poikkeustilanteiden käsittelyä varten on luotava sellaiset menettelyt, että jokainen organisaation henkilö voi helposti toteuttaa omat tietoturvavastuunsa: noudattaa ohjeita ja raportoida havaitsemistaan puutteista tai epäilyksistä asianmukaisesti.

### käytännön ohjeita

a) Tapahtumatietojen kirjaamisesta sovitaan käytäntö. Sekä tietojärjestelmien että kiinteistön ja toimitilojen tapahtumat kirjataan. Kirjattavat tiedot ovat mahdollisuuksien mukaan yhtenevät eri tietojärjestelmien välillä. Esimerkiksi kellonaika välitetään kaikkiin järjestelmiin siten, että järjestelmät ovat keskenään synkronoitu ja tarvittaessa reaaliajassa. Kellonaika esitetään kaikkialla samassa formaatissa. Muiden tietojen osalta (kuten käyttäjätunnukset, verkkotunnukset ja käyttöoikeudet) käytetään mahdollisimman standardia merkitsemistapaa.
b) Tapahtumatietojen seurannasta on sovittu käytäntö.
c) Poikkeustilanteiden käsittelystä on sovittu käytäntö.
d) Määrittelyissä käytetään hyväksi riskianalyysiä ja rakennetaan sen perusteella kullekin tietojärjestelmälle riittävät kirjaamis-, seuranta ja raportointimenettelyt.
e) On sovittu käytäntö ja luotu ohjeet, miten ja kenelle kuka tahansa henkilö voi ilmoittaa tai raportoida havaitsemastaan tietoturvallisuuden mahdollisesti vaarantavasta uhkasta, tietojärjestelmän haavoittuvuudesta tai muusta epäilyttävästä olosuhteesta tai tapahtumasta.
f) On sovittu käytäntö, miten kirjattuja tietoja käytetään, jos joudutaan selvittämään erillisiä tapahtumia tai tilanteita yksityiskohtaisesti esimerkiksi organisaation sisäistä auditointia tai ulkopuolista sertifiointia varten, viranomaisen esittämästä pyynnöstä tai käynnissä olevaa oikeusprosessia varten.
g) Tapahtumien kirjausmenettely on sellainen, että valtuudeton tapahtumatietoihin pääsy tai niiden muuttaminen on estetty.
h) Kirjaustapana voi olla esimerkiksi jokaisen yksittäisen tapahtuman kirjaaminen tai kerättävän tiedon tilastointi, esimerkiksi kuormituksen ja suorituskyvyn sekä pitkäaikaisten tilastollisten poikkeamien seurantaa varten.
i) Alihankkijoiden kanssa on solmittu riittävät ylläpito- ja huoltosopimukset.

## A11.2 Tietojärjestelmien tapahtumien, käytön ja vikojen kirjaaminen

### kontrolli

Tietojärjestelmien on pidettävä automaattista tapahtumalokia, johon on kirjattava tiedot normaalissa toiminnassa (myös automaattisesti suoritettavissa prosesseissa) ja kaikissa käyttäjien toimissa. Kaikki tarpeelliset tiedot sekä epäonnistuneista käyttöyrityksistä että ulkoisista tunkeutumisyrityksistä on kirjattava. Tarvittaessa lokitiedosta voidaan kopioida tietoa erillisesti jotakin tiettyä tarkoitusta varten, esimerkkinä potilastietojen luovutuksesta syntyvien tietojen kopiointi säilytettäväksi erikseen.

Lokitietoa saattaa kertyä huomattava määrä, joten on huolehdittava, että uusi lokitiedosto otetaan käyttöön riittävän usein, jottei tietojärjestelmän toiminta vaarannu tai ylikuormitu. Koska lokitiedot saattavat sisältää arkaluonteisia ja luottamuksellisia tietoja, niiden säilytyspaikka, -aika ja -tapa sekä tuhoaminen on määriteltävä tietoturvavaatimusten mukaisesti.

Jos automaattinen kirjaus ei ole käytössä tai sellaista ei ole mahdollista käyttää, erilaisia lokitietoja on syytä kirjata käsin tarpeen mukaan.

### käytännön ohjeita

a) Tietojärjestelmien automaattinen tapahtumakirjaus aktivoidaan. Käyttöjärjestelmätasolla lokiin kirjataan esimerkiksi
   - järjestelmän ja prosessien käynnistys- ja sammutustiedot (aika, prosessi, oikeudet, onnistumisstatus),
   - käyttäjien sisään- ja uloskirjautumistiedot (aika, käyttäjä, yhteystunniste, oikeudet),
   - tarpeelliset tiedot järjestelmässä tapahtuvista ja tehtävistä muutoksista (esimerkiksi konfiguraatiot ja muut määrittelyt sekä sovellusten ja laitteiden asennukset ja poistot),
   - tiedot sovellusten käytöstä,
   - tiedostojen ja tietokantojen käyttö,
   - verkkoyhteyksien käyttö,
   - järjestelmän resurssien käyttö,
   - tiedot järjestelmän suorituskyky- ja kuormitustilanteesta,
   - tiedot kaikista epäonnistuneista käyttöyrityksistä,
   - kaikista vikatilanteista ja virheellisistä tapahtumista sekä
   - vikojen ja häiriöiden kuittaukset.

b) Tietokanta- ja muiden sovellusohjelmien erillinen tapahtumakirjaus aktivoidaan. Lokiin kirjataan mahdollisuuksien mukaan vastaavat tapahtumat kuin edellä. Erityisesti tietokantojen ylikuormitustilanteet huomioidaan.

c) Tietojärjestelmän verkkoliikenteen tapahtumakirjaus aktivoidaan. Lokiin kirjataan mahdollisuuksien mukaan vastaavat tapahtumat kuin edellä. Verkkoliikenteen ylikuormitustilanteet huomioidaan erityisesti.

d) Uusi lokitiedosto otetaan käyttöön riittävän usein sekä käyttöjärjestelmän että sovellusten osalta.

e) Vanhojen lokitiedostojen säilytyksessä ja käsittelyssä noudatetaan sovittuja tietoturvallisia käytäntöjä.

f) Organisaation normaaleissa prosesseissa tarvittavat tiedot kopioidaan lokitiedostoista erilleen. Käyttöoikeuksia lokitiedostoihin ei myönnetä muille kuin tietojärjestelmistä vastaaville henkilöille.

## A11.3 Muut valvontakeinot

### kontrolli

Luvussa *fyysisen ympäristön turvallisuus* määritellään erilaisia valvontakeinoja esimerkiksi kulunvalvontaan, kameravalvontaan, ikkunoiden ja ovien käytön valvontaan ja olosuhteiden valvontaan (palo, kosteus, ym.) liittyen. Näistä valvontamenetelmistä saatavat tiedot on kirjattava tarvittavaa seurantaa varten.

### käytännön ohjeita

a) Henkilöiden kulunvalvonnassa kirjataan lähtö-, tuloajat sekä kulku kiinteistön sisällä.
b) Ovien, ikkunoiden ja muiden mahdollisten kulkureittien käyttö kirjataan. Erityisesti korkean turvallisuuden tilojen ovien käyttö kirjataan. Esimerkiksi tietojärjestelmiä siirrettäessä ovia saatetaan joutua pitämään auki siten, että automaattiset hälyttimet aktivoituvat.
c) Fyysisiin oloihin liittyvät tapahtumat ja tieto olosuhteista kirjataan. Näitä ovat esimerkiksi lämpötila ja kosteusprosentti. Tieto kirjataan korkean turvallisuuden tilojen osalta seurantaa varten erityisen tarkasti.

## A11.4 Seuranta

### kontrolli

Tietojärjestelmien tapahtumaseurannassa ja muussa valvonnassa kirjattuja tietoja ja tapahtumia on tarkkailtava ja seurattava. Poikkeustilanteita on valvottava ja aina tarvittaessa käynnistettävä hälytys- ja raportointimenettely, jonka perusteella havaitut ongelmat voidaan korjata tai ohittaa ja ryhtyä muihin tarvittaviin toimiin.

Seurannan on oltava säännöllistä ja seurannan taajuuden vastattava seurattavan kohteen kriittisyyttä ja turvatasoa. Mahdollisimman suuri osa seurannasta on automatisoitava ja määritettävä tarkkailulle hälytysrajat, joiden ylittyessä tai alittuessa suoritetaan automaattinen hälytys ja mahdollisuuksien mukaan automaattisesti tehtävät korjaustoimet.

### käytännön ohjeita

a) Seurataan hälytysjärjestelmän ja tapahtumankirjauksen moitteetonta toimintaa.
b) Seurataan järjestelmien moitteetonta toimintaa ja kuormitustilannetta.
c) Seurataan sovellusten ja tietokantojen moitteetonta toimintaa ja kuormitustilannetta.
d) Seurataan tietoliikennettä ja verkkotunkeutumisten yritysten määrää.
e) Seurataan järjestelmissä ja sovelluksissa tehtyjä muutoksia ja niiden vaikutuksia järjestelmien moitteettomaan toimintaan.
f) Seurataan levytilojen käyttöastetta ja täyttymistä.
g) Seurataan käyttäjien kirjautumisia ja toimintaa.
h) Seurataan tietojärjestelmien administraattorien valtuuksien käyttöä.
i) Seurataan viruksia ja muita haittaohjelmia.
j) Seurataan palvelunestohyökkäyksiä.
k) Seurataan valtuudettomia kirjautumisyrityksiä ja niiden määrää.
l) Seurataan automaattisesti syntyviä ja raportoitavia vika-, häiriö-, virhe-, ylikuormitus-, käyttöoikeus- ja väärinkäytöshälytyksiä.
m) Seurataan kulunvalvontatietoja.
n) Seurataan muita kiinteistön ja toimitilojen valvonnasta syntyviä tietoja.

## A11.5 Hälytykset ja raportointi

### kontrolli

Tietoturvaloukkauksista ja poikkeamista on aiheutettava hälytys ja niistä on raportoitava mahdollisimman pikaisesti.

### käytännön ohjeita

a) Hälytys tarvittaville vastuuhenkilöille ja teknisille henkilöille suoritetaan mahdollisimman nopeasti, jotta tarpeellisiin korjaustoimiin voidaan ryhtyä.
b) Hälytyksessä välitetään kaikki tarpeelliset tiedot, jotta korjaustoimet ovat oikeat ja mahdollisimman tehokkaat.
c) Vastaanotettu hälytys kuitataan vastaanotetuksi.
d) Tarvittaessa käytetään 'hiljaista hälytystä', esimerkiksi jotta mahdollinen tietomurron yrittäjä voidaan saada kiinni verekseltään.

## A11.6 Poikkeamien käsittely ja seuraamukset

### kontrolli

Hälytykset on huomioitava ja käsiteltävä mahdollisimman nopeasti. Korjaustoimiin on ryhdyttävä tarpeen mukaan välittömästi ja välitettävä tieto tarpeellisille tahoille. Mahdolliset muut seuraamukset, kuten rikkomuksesta rankaiseminen, on tehtävä asianmukaisesti.

### käytännön ohjeita

a) Hälytys käynnistää välittömän ongelman korjauksen tai, jos ongelmaa ei voida korjata, korvaavan menettelyn rakentamisen.
b) Välitetään hälytyksen tiedot tarpeen ja mahdollisuuksien mukaan automaattisesti viranomaisille, esimerkiksi paloviranomaisille ja poliisille.
c) Tiedot ongelmatilanteesta välitetään tarvittaessa eteenpäin esimerkiksi tiedotusvälineille.
d) Alihankkija tai toimittaja velvoitetaan tarvittaessa osallistumaan korjaustoimiin.
e) Tieto hälytyksestä välitetään johdon, tietoturvaorganisaation ja tietohallinnon arviointia varten, jotta asianmukaisiin seuraamuksiin (mahdollinen käyttöoikeuksien poisto, rikkomuksista rankaiseminen, valvontaprosessin kehittäminen, tietohallinnon kirjanpito) voidaan ryhtyä.
f) Korjaustoimenpiteiden jälkeen ongelma kirjataan korjatuksi.
g) Tiedot hälytyksen aiheuttaneesta tapahtumasta, korjaustoimenpiteet ja korjauksessa havaitut muut seikat tallennetaan poikkeustilanteiden käsittelyn seurantaa ja kehittämistä varten.

## A11.7 Mittaaminen ja kehittäminen

### kontrolli

Poikkeus- ja vikatilanteiden toimintaa ja laatua on mitattava. Raportoiduista ja raportoimattomista ongelmista saatavat tiedot analysoidaan ja toimintaa kehitetään tarpeen mukaan. Yleisesti ottaen toimintaa voidaan erikseen kuvata organisaation muissa dokumenteissa, raporteissa ja tiedotteissa.

### käytännön ohjeita

a) Mitataan hälytysten oikeellisuutta ja laatua (kaikista ja vain aiheellisista tapahtumista tulee hälytys, hälytys tulee määriteltyjen aikarajojen puitteissa, hälytys sisältää kaikki tarvittavat tiedot).

b) Toimintaa poikkeustilanteissa mitataan sopivilla mittareilla (esimerkiksi hälytyksen saapumiseen kuluva aika, korjaukseen kuluva aika, alihankkijan saapumiseen kuluva aika, oikeanlainen tiedottaminen ongelmasta ja korjauksesta).
c) Tietoja käytetään hyväksi arvioitaessa organisaation tietoturvallisuuden tasoa ja yhteensopivuutta tietoturvapolitiikan, tietosuojapolitiikan ja tietohallinnon dokumenttien kanssa.
d) Käynnistetään tarvittaessa alihankkijoille ja muille toimijoille aiheutuvat korvaus-, hyvitys- ja sanktiomenettelyt.

# Standardeja ja kirjallisuutta


[1] ISO/IEC 17799: 2000 "Code of Practice for Information Security Management"

[2] AS/NZS 17799: 2002 "Health Information Security Management"

[3] ISO/IEC 13335 Part 1-5: 1996-2001 "Guidelines for the Management of IT Security"

[4] ISO/IEC 15408:1999 "Evaluation Criteria for IT Security"

[5] ISO/IEC FCD 18045 Methodology for IT Security Evaluation"

[6] ISO/TR 15446 "Guide for the production of Protection Profiles and Security Targets"

[7] ISO/DTS 17090:2001 "Health Informatics – Public Key Infrastructure"

[8] ISO/PDTS 22600 ISO/TC215/WG4 "Health Informatics – Privilege management and access control"

[9] CIHI/ICIS: 2001 Model Digital Signature and Confidentiality Certificate Policies for Health Public Key Infrastructure

[10] ISO/TR 21089 "Health Informatics – Trusted end-to-end information flows"

[11] EESSI European Electronic Signature Standardization Initiative Expert Team Final Report: 1999

[12] HIPAA Privacy Rule and Public Health (*http://www.hhs.gov/ocr/hipaa/*)

[13] Valtiovarainministeriö VAHTI 7/2003 "Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa"

[14] Valtiovarainministeriö VAHTI 4/2003 "Valtionhallinnon tietoturvakäsitteistö"

[15] Valtiovarainministeriö VAHTI 3/2003 "Tietoturvallisuuden hallintajärjestelmän arviointi"

[16] Valtiovarainministeriö VAHTI 4/2001 "Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje"

[17] Valtiovarainministeriö VAHTI 2/2000 "Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje"

[18] Valtiovarainministeriö VAHTI 3/2001 "Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus"

[19] Stakes/Oske: 7/2004 "Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi"

[20] Stakes/Oske: 3/2004 "Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi"

[21] Stakes/Oske: 2/2004 "Tietoturvallinen kommunikaatioalusta: Ohjeita PKI-infrastruktuurin toteuttamiselle"

[22] Stakes/Oske: 5/2004 "Sähköisen potilaskertomuksen yhdenmukaiset rakenteiset ydintiedot"

[23] Stakes/Oske: 3/2003 "Sähköisen asiakas- ja potilasasiakirjojen säilytyksen ja kiistämättömyyden hyvä käytäntö"

[24] Stakes/Oske: 4/2002 "Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi – terveydenhuollon PKI-arkkitehtuuri"

[25] Marja Pajukoski: Sähköinen asiointi sosiaali- ja terveydenhuollossa (Stakes raportteja 283, 2004)

[26] Hannu Sorvari: Oikeudellisia näkökohtia potilastiedosta ja potilaan suostumuksesta tietokoneistuvassa terveydenhuollossa (Stakes raportteja 285, 2004)

[27] Väestörekisterikeskus: Varmennepolitiikka OID 1.2.246.517.1.10.5: 2004

[28] Väestörekisterikeskus: FINEID – S2 CA-model and certificate contents: 2003

[29] Pekka Himanen, Tulevaisuusvaliokunta: Katsaus tietoyhteiskuntamme syviin haasteisiin (Eduskunnan kanslian julkaisu, 2004)

[30] Jukka Jääskeläinen: eWelfare – Tuottava tietotekniikka hyvinvointipalveluissa (SITRA, 2004)

[31] Satakunnan makropilotin tietoteknologian arviointi (2002)

[32] Information Security Forum (ISF) – The Standard of Good Practice for Information Security (2003, 2005)

[33] Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen – STM:n opas terveydenhuollon henkilöstölle (2001)

[34] OECD:n suositus: 2002 "Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet"

[35] Sosiaali- ja terveydenhuoltolainsäädäntö 2004 (toim. Hannu Ranta)

[36] Maarit Outinen: Kirjallisuuskoonnos riskienhallinnasta (Stakes 2004)

[37] Terveydenhuollon tietoturvan ja tietosuojan toteutuksen hyviä käytäntöjä (Suomen Kuntaliitto 1997)

[38] ISO/WD 27799 Health Informatics – Security Management in Health Using ISO/IEC 17799 (ISO/TC 215/WG4) Draft

[39] Leini Sinervo, Noora von Fieandt (toim.): Tietotekniikka sosiaali- ja terveysalan osaamisen kehittämisessä (Stakes aiheita 5/2005)

[40] Pirkko Nykänen (toim.): Terveydenhuollon tietojärjestelmät (Tietojenkäsittelytieteen laitos, Tampereen yliopisto 2003)

[41] Tietoteknologian käytön edistäminen sosiaalihuollossa -hankesuunnitelma (Sosiaali- ja terveysministeriön monisteita 2005:1)

[42] Jakob Nielsen: Usability Engineering (Academic Press 1993)

[43] Tietosuoja-lehti, erityisesti 1/2005 (tietosuojavaltuutetun toimisto, tietosuojalautakunta)

[44] Laadi tietosuojaseloste! Hyvä tietää -sarja 3/2004, http://www.tietosuoja.fi/9122.htm (tietosuojavaltuutetun toimisto)

[45] Tietosuojavaltuutetun toimiston oppaat, http://www.tietosuoja.fi/27212.htm (tietosuojavaltuutetun toimisto)

[46] Turvallisuussuunnitteluopas sosiaali- ja terveydenhuollon toimintayksiköille (Sosiaali- ja terveysministeriön oppaita 2005:13)

# Käytetyt termit

Tässä on listattu dokumentissa käsiteltäviä termejä selityksineen. Lähdesanastona on käytetty pääasiassa Valtiovarainministeriön julkaisua *Valtionhallinnon tietoturvakäsitteistö*. Termien selitykset saattavat sisältää lisäyksiä alkuperäisiin selityksiin.

### aikaleima

en time stamp

tapahtumatietoon tai viestiin liitetty tieto luomis-, lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista

Aikaleimalla saadaan aikaan tapahtuman ajankohdan kiistämättömyys.

### allekirjoitus

en signature

asiakirjaan, viestiin tai muuhun tekstiin liitetty henkilön omakätinen nimikirjoitus tai muu tieto, jonka vain kyseinen henkilö on voinut tuottaa, osoituksena siitä, että teksti vastaa hänen tahtoaan tai aikomustaan

Koska sähköisen asiakirjan allekirjoittaminen omakätisesti ei ole mahdollista, on luotu menetelmä, jota käyttämällä henkilö voi tehdä allekirjoituksen sähköisesti siten, että se vastaa sekä teknisesti että juridisesti käsin tehtyä allekirjoitusta. Sähköinen allekirjoitus on tietoturvallisempi kuin käsin tehty, sillä siihen liittyvä väärinkäyttö, esimerkiksi väärentäminen, on käytännössä mahdotonta.

### biometriset tunnisteet

en biometric identification, biometric authentication

ihmisen tunnistaminen tai todentaminen fyysisten tuntomerkkien perusteella

Biometrisia tunnisteita ovat esimerkiksi henkilön sormenjäljet ja kasvokuva. Tietojärjestelmissä biometrisia tunnisteita käytetään todentamiseen: järjestelmään kirjautunut tai kirjautumassa oleva, toisin sanoen jo tunnistettu henkilö todistaa identiteettinsä biometriatietoon perustuen.

Biometrisia tunnisteita ei käytetä ihmisen tunnistamiseen. Jos näin tehtäisiin, järjestelmän pitäisi saada biometriatiedon perusteella henkilön identiteettitieto suoraan tietojärjestelmästä, joka edellyttäisi rekisterin olemassaoloa henkilöiden biometrisista tunnisteista.

### CA

en certificate authority

katso varmentaja ja TTP

Myös termiä CSP (*cryptographic service provider*) käytetään joissakin yhteyksissä.

### digitaalinen allekirjoitus

en digital signature

sähköinen allekirjoitus, jonka tuottamiseen on käytetty henkilön salaista avainta ja joka voidaan tarkastaa käyttämällä henkilölle myönnetyssä varmenteessa sijaitsevaa henkilön julkista avainta

Viestiin tai asiakirjaan liitetty digitaalinen allekirjoitus yksilöi lähettäjän ja on todiste asiakirjan ja lähettäjän aitoudesta sekä asiakirjan eheydestä. Käytännössä digitaalinen allekirjoitus saadaan aikaan epäsymmetrisellä salauksella, jossa allekirjoitettavan viestin tiiviste salataan käyttäjän salaisella avaimella. Salauksen purku onnistuu vain käyttäjän julkisella avaimella, jolloin myös allekirjoittajan henkilöllisyys todentuu. Tiiviste muodostetaan allekirjoitettavasta asiakirjasta siten, että alkuperäisen asiakirjan muuttaminen on mahdotonta muuttamatta myös tiivistettä. Täten allekirjoitus on matemaattisesti kiistämätön: tiivistefunktio ei salli asiakirjaan tehtäviä muutoksia ja allekirjoituksessa käytettävä salausalgoritmi yhdistää allekirjoittajan vedenpitävästi alkuperäiseen asiakirjaan.

**eheys**

en integrity

tietojen tai tietojärjestelmän aitous, sisäinen ristiriidattomuus ja väärentämättömyys: ominaisuus, että tietoa, viestiä tai asiakirjaa ei ole oikeudettomasti muutettu eikä se ole muuttunut

Tiedon eheyttä kuvatessa käytetään usein myös termejä alkuperäisyys, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus. Tieto voi kuitenkin täyttää eheysvaatimuksen, vaikkei olekaan kattava tai ajantasainen. Tässä mainitut termit kuvaavat pikemminkin tiedon käytettävyyttä ja kelpoisuutta eli tietosisällön laatua.

**epäsymmetrinen salaus**

en asymmetric encryption

salaus, jossa viestin avaaminen tapahtuu eri avaimella kuin sen salakirjoitus

Käyttäjän hallussa olevaa avainta kutsutaan salaiseksi tai yksityiseksi avaimeksi. Varmenteessa oleva avain on julkinen avain, jota käytetään salaisen avaimen haltijan identiteetin todentamisessa tai salaisen avaimen haltijalle lähetettävän viestin salaamisessa.

Vastaavasti symmetrinen salaus tarkoittaa salausta, jossa viestin salakirjoitus ja avaaminen ja tehdään käyttämällä samaa avainta.

**fyysisen ympäristön turvallisuus**

en physical and environmental security

henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen, varastojen ja vastaavien suojaaminen tuhoja ja vahinkoja vastaan turvaamalla muun muassa kulun- ja tilojen valvonnan, vartioinnin sekä torjumalla palo-, vesi-, sähkö-, ilmastointi- ja murtovahingot

Fyysinen turvallisuus sisältää myös esimerkiksi työntekijöiden hyvinvoinnin sekä käytössä olevien työ- ja toimitilojen turvaamisen. Tähän voidaan lukea mukaan työhuoneissa näkyvillä oleva turvattava materiaali. Myös kuriirit ja tietoaineistoja sisältävät lähetykset on turvattu.

**haavoittuvuus**

en vulnerability

alttius tietoturvallisuutta uhkaaville tekijöille

Haavoittuvuus on joku tietty (esimerkiksi) tietojärjestelmän ominaisuus, joka aiheuttaa tai johon voi kohdistua uhka tietojärjestelmälle tai sen toiminnalle. Esimerkiksi käyttöjärjestelmissä on usein ohjelmointi- ja suunnitteluvirheiden johdosta erilaisia haavoittuvuuksia, joita löydettäessä ohjelmistotoimittaja julkaisee korjauspaketin, jonka asentaminen poistaa tai korjaa haavoittuvuuden.

Uhkia kartoitettaessa ja riskejä analysoitaessa on hyvä, mitä enemmän haavoittuvuuksia on tiedossa, jotta ainakin tunnettujen haavoittuvuuksien osalta voidaan varautua niistä mahdollisesti aiheutuviin riskeihin.

**hakemistopalvelu**

en directory service

julkisen avaimen infrastruktuurin palvelu, joka hallitsee varmenteita ja sulkulistoja sisältäviä hakemistoja

Hakemistopalvelun ominaisuuksista on luotu standardit X.500 ja LDAP (kevytversio, *lightweight directory access protocol)*, joissa määritellään esimerkiksi hakemistojen ja niissä sijaitsevien objektien ja tietojen rakenteet ja ominaisuudet, tietojen hakumenetelmät ja hakuprotokollat.

**hallinnollinen tietoturvallisuus**

en administrative information security, organizational information security

tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta

Hallinnollisen tietoturvallisuuden toteuttamisessa ovat avainasemassa seuranta, valvonta, palautteen antaminen ja poikkeustilanteiden hallinta.

### henkilöstöturvallisuus

en personnel security

henkilöstöön liittyvien tietoturvariskien hallinta esimerkiksi henkilöiden soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta

### henkilövarmenne

en personal certificate, identity certificate

varmenne, jota käytetään henkilön tunnistamiseen tai todentamiseen sähköisessä asioinnissa ja sähköisten allekirjoitusten tarkastamisessa

Jos varmenteen kohteena ei ole henkilön identiteetti vaan esimerkiksi rooli, puhutaan roolivarmenteesta. Tällöin on huomattava, että varmenteesta ei käy ilmi henkilön identiteetti. Tällaista varmennetta voidaan käyttää esimerkiksi sovellukseen kirjautumisen yhteydessä, kun käyttäjän identiteetillä ei ole merkitystä vaan ainoastaan sillä, onko käyttäjällä tehtävään tai rooliin perustuva käyttövaltuus järjestelmään. Sähköisen allekirjoituksen yhteydessä varmennetta ei ole syytä käyttää, sillä varmenteesta ei käy ilmi allekirjoittaja.

Kansalaisvarmenne on Väestörekisterikeskuksen myöntämä ja ylläpitämä varmenne. Laatuvarmenne on sähköisestä allekirjoituksesta säädettyyn lakiin perustuvat ominaisuudet omaava varmenne, jota käytetään sähköiseen allekirjoitukseen. Laki koskee nimenomaan julkisesti myönnettäviä varmenteita, joten esimerkiksi organisaation työntekijöilleen myöntämät varmenteet eivät ole laatuvarmenteita. Organisaation myöntämien varmenteiden oletetaan yleensä noudattavan vähintään niitä laadullisia ominaisuuksia kuin mitä laatuvarmenteista on säädetty. Laatuvarmenteet sellaisenaan eivät usein kelpaa organisaatiokäyttöön tiettyjen ominaisuuksien takia, esimerkiksi laissa mainittu allekirjoittajan nimi on mahdollista olla myös salanimi.

### ISO 17799

tietoturvallisuuden eri alat kattava kansainvälinen standardi

Pohjautuu Britannian standardointi-instituutin julkaisemaan suositukseen (BS7799) yrityksen tietoturvallisista toimintaperiaatteista ja turvallisuustodistusten myöntämisperusteista.

### julkisen avaimen infrastruktuuri

en public key infrastructure, PKI

julkisen avaimen menetelmään perustuvaa infrastruktuuri, jossa nimetyt varmentajat tuottavat käyttäjille avainparit, varmentavat ne digitaalisella allekirjoituksellaan ja jakavat ne käyttäjille, ylläpitävät tarvittaessa julkisten avainten hakemistoja ja sulkulistoja sekä mahdollisia muita infrastruktuuriin kuuluvia palveluita, kuten aikaleimapalvelu

Infrastruktuuri on kokonaisuus ja koostuu kaikista sitä hyödyntävistä laitteista, ohjelmistoista, sovelluksista ja palveluista mukaan lukien käyttäjien toimikortit ja palveluiden käyttöliittymät. Infrastruktuuri perustuu epäsymmetriseen salausmenetelmään, jossa kaksi matemaattisesti toisiinsa liitettyä avainta muodostavat perustan käyttäjien tunnistukseen ja todentamiseen, tiedon salaukseen ja eheyteen, sähköiseen allekirjoitukseen ja tapahtumien kiistämättömyyteen.

### kiistämättömyys

en non-repudiation

tietoverkoissa eri menetelmin saatava varmuus siitä, että tietty henkilö on allekirjoittanut tai lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys) tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi

Tapahtumaan, viestiin tai allekirjoitukseen voidaan liittää myös aikaleima, jolloin myös tapahtuman ajankohta on kiistämätön.

**kontrolli**

en control

(tässä yhteydessä) riskien hallinnan tavoite, keino tai menetelmä: suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan tietoturvaloukkauksia vastaan

**kryptografia, kryptaus**

en cryptography

salakirjoitus tai salaustekniikka; menetelmät ja välineet tiedon salaamiseen ja kätkemiseen

Salakirjoittamisessa alkuperäinen tieto muutetaan eli salataan (*encryption*) siten, että salauksen purku (*decryption*) ja siten tiedon alkuperäinen sisältö on mahdollista selvittää vain tietämällä salauksen purkuun tarvittava menetelmä (*encryption algorithm*) ja mahdollinen salauksen purkuun käytettävä avain.

**käytettävyys**

en usability, usein myös availability

tieto on tallennettu siten ja sellaisessa muodossa, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein

Käytettävyyteen liittyy myös, että saatavilla olevat tiedot ovat kattavia, ajantasaisia, oikeellisia ja muuten käyttökelpoisia vaadittavalla tavalla ja helppokäyttöisesti ilman tulkinta- ja väärinkäyttömahdollisuutta. Usein käytettävyydellä tarkoitetaan myös sitä, että tiedot ovat saatavilla, siis saavutettavissa ja käytettävissä. Tätä vaatimusta kuvaa kuitenkin paremmin termi saatavuus.

**käyttöoikeus**

en access right

käyttäjälle annettava tiettyyn tietoon, ohjelmistoon tai järjestelmään annettava oikeus

Käyttöoikeuksia ovat esimerkiksi lukuoikeus, kirjoitusoikeus, muutosoikeus, tuhoamisoikeus ja hallintaoikeus eli muiden käyttäjien oikeuksien määrittely.

**käyttöturvallisuus**

en operations security

tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi

**käyttövaltuus**

en user right, authorization, privilege

tietojärjestelmän käyttäjälle myönnetyt yksilöidyt oikeudet nimettyjen tietojen, järjestelmien, ohjelmistojen tai niiden osien käyttöön

**laitteistoturvallisuus**

en computer security

tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen toimivuuteen ja tietoturvallisuuteen liittyvät toimet

**loki**

en log

tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista

Loki kerätään yleensä automaattisesti *(automatic logging, audit trail*) ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki ja laskutusloki. Lokitiedosto voi olla järjestelmän sähköisesti allekirjoittama ja lokitapahtumat sovelluksen sähköisesti allekirjoittamia, jolloin lokitiedoston eheys ja kiistämättömyys voidaan taata. Lokitietoja käytetään tyypillisesti tapahtumien ja käyttäjien toimien seurannassa ja raportoinnissa (*auditing, reporting*), valvonnassa (*monitoring*), tarkastuksissa ja laskutuksessa (*accounting*).

**(tietojen) luokitus, luokittelu**

en (information) classification

tietojen ryhmittely jollakin tietyllä perusteella

Tietojen luokittelun perusteena voi olla esimerkiksi tärkeys ja kriittisyys, merkitys organisaation toiminnalle, salassa pidettävyys ja luottamuksellisuus, suojaustarve ja haavoittuvuus asiattomalle käsittelylle tai omistajuus.

**luottamuksellisuus**

en confidentiality

vain tietyn tai tiettyjen henkilöiden tietoon tarkoitettujen tietojen säilyminen heidän hallussaan ja tiedossaan sekä näiden tietojen suojaaminen paljastumiselta esimerkiksi tietojen käsittelyn yhteydessä myös tietoliikenteen osalta

**notaaripalvelu**

en notary service

verkkonotaarin palvelu, esimerkiksi aikaleimojen antaminen

**ohjelmistoturvallisuus**

en software security

käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi

**PKI**

en public key infrastructure

katso julkisen avaimen infrastruktuuri

**politiikka**

en policy

(tässä yhteydessä) asiakirja, joka kuvaa pääpiirteissään jonkin tietyn kokonaisuuden: päämäärät, määritellyt ja sovitut toimintaperiaatteet, päätökset, ratkaisut ja niiden käytännön toteutuksen

Ratkaisujen ja käytännön toteutuksen kuvaaminen ei ole yksityiskohtaista, vaan kuvataan vain tarvittaessa ja ainoastaan riittävällä tasolla. Tietoturvallisuuden kehittämisessä ja hallinnassa tarvittavia asiakirjoja ovat esimerkiksi tietoturva-, tietosuoja- ja varmennepolitiikka.

**pääsynhallinta**

en access control

toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille

Pääsynhallinnassa tietojärjestelmien, tietoverkkojen ja tietojen käyttäjät tunnistetaan ja todennetaan sovitulla tavalla. Todennetuille käyttäjille myönnetään valtuudet – käyttäjien tehtävien ja roolien mukaisesti etukäteen sovitut käyttöoikeudet – järjestelmiin ja tietoihin.

**riski**

en risk

(tässä yhteydessä) tietoturvallisuuden ja sen vaarantumisen uhka: todennäköisyys, että uhka toteutuu ja aiheuttaa tietyn suuruisen menetyksen tai vahingon

Riskin odotusarvo voidaan mitata kertomalla uhkan todennäköisyys mahdollisen vahingon arvolla. Organisaation riskien hallinta perustuu riskianalyysiin. Tällöin uhkat ja riskit arvioidaan systemaattisin menetelmin, ja arvioinnin perusteella organisaatio varautuu valittuihin riskeihin valituilla toimenpiteillä.

**saatavuus, saavutettavuus**

en availability, accessibility

tiedon tai tietojärjestelmän ominaisuus, että siihen on riittävän esteetön, vaivaton ja nopea pääsy

**sähköinen allekirjoitus**

en electronic signature

katso digitaalinen allekirjoitus

**sähköinen identiteetti**

en electronic identity

henkilön identiteetti ja henkilöllisyys tietojärjestelmän kannalta

Tyypillisesti tietojärjestelmässä henkilön identiteettiä vastaa käyttäjätunnus. Henkilö valtuutetaan tietojärjestelmän käyttöön ja hänelle myönnetään järjestelmässä olevien tietojen käyttöoikeudet sähköisen identiteettinsä, käyttäjätunnuksensa perusteella. Julkisen avaimen infrastruktuurissa rekisteröijä tunnistaa ja todentaa henkilön ja luo tälle rekisteröitymisen yhteydessä sähköisen identiteetin, varmenteen. Käytännössä tämä varmenne vastaa fyysisen maailman henkilöllisyystodistusta.

**tarkastettavuus**

en auditability

järjestelmän ominaisuus, että järjestelmän tapahtumat kirjataan ja järjestelmän toiminta ja siinä esiintyvät virheet, epäsäännöllisyydet ja väärinkäytökset tuodaan esiin

**tietoliikenneturvallisuus**

en telecommunications security

tietoturvallisuuden toteuttaminen tietoliikenteen osien (laitteiden, järjestelmien ja ohjelmistojen) ja niissä kulkevien tietojen osalta

**tietosuoja**

en privacy protection, data protection

tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen, henkilötietojen suojaaminen valtuudettomalta ja henkilöä vahingoittavalta käytöltä

Tietosuoja tarkoittaa yksilön suojaa – ihmisten yksityiselämän ja yksityisyyden suojaa – ja näitä turvaavia oikeuksia esimerkiksi henkilö- tai potilastietoja käsiteltäessä. Tietosuoja-termi on nimenomaan juridinen, ja sen toteuttamisesta ja vaatimuksista on säädetty useassa eri laissa.

**tietosuojapolitiikka**

en privacy policy, privacy protection policy, data protection policy

tietosuojasäädökset ja niiden toimeenpanoa koskevat päätökset

Jos organisaatio käsittelee yksityishenkilöiden henkilötietoja, se laatii asiakirjan tietosuojapolitiikka tai henkilötietojen käyttö, jossa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja käytäntö organisaatiossa. Asiakirja voidaan jakaa myös niille, joiden henkilötietoja organisaatio käsittelee, jolloin voidaan edesauttaa luotettavan kuvan syntymistä organisaation toiminnasta.

## tietoturva, tietoturvallisuus

en information security

tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu

Asiantila, jossa tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä.

Tietoturvan toteutuminen edellyttää tietojen asianmukaista luokittelua, tietoja uhkaavien uhkien ja riskien kartoittamista sekä sopiviin suojaustoimenpiteisiin ryhtymistä. Täytyy olla tiedossa, mitä tietoja suojataan, miksi näitä tietoja suojataan ja miltä tietoja ollaan suojaamassa. Suojaaminen sisältää erilaisia hallinnollisia ja teknisiä päätöksiä, periaatteita, menettelytapoja ja toimenpiteitä, joilla varaudutaan tietoihin kohdistuviin uhkiin ja estetään riskien toteutuminen tai vähennetään niiden vaikutuksia.

## tietoturvapolitiikka

en security policy, information security policy, data security policy

organisaation tasolla johdon hyväksymä näkemys ja julkaistu kannanotto tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta

Tietoturvapolitiikka annetaan tyypillisesti esimerkiksi asiakkaiden, yhteistyökumppaneiden tai toimittajien luettavaksi. Se on osoitus organisaation tahdosta ja kyvystä käsitellä tietoja turvallisesti ja luotettavasti. Tietoturvapolitiikka ei yksilöi periaatteita eikä käytäntöä niin tarkasti, että dokumentin jaolla organisaation ulkopuolelle olisi vaikutusta tietoturvallisuuteen.

Jotta organisaatiossa toimitaan tietoturva- ja tietosuojapolitiikkojen mukaisesti, on noudatettavat käytännöt, ohjeet ja periaatteet hyvä koota yhteen, *"tietoturvakäsikirjaksi"*.

## tiiviste

en hash, digest

(Tässä yhteydessä) tiedosta, viestistä tai asiakirjasta jonkin säännön mukaan muodostettu lyhyempi uusi tieto, eräänlainen tarkistussumma, varmisteen luomiseksi alkuperäisestä tiedosta.

Tiivisteestä ei ole mahdollista päätellä alkuperäistä tietoa tai jotakin muuta tietoa, joka tuottaisi alkuperäisen tiedon kanssa identtisen tiivisteen. Alkuperäisestä tiedosta laskettu tiiviste on samaa funktiota käyttämällä aina identtinen. Täten tiivistettä voidaan käyttää sähköisen allekirjoituksen yhteydessä todisteena, että allekirjoitus koskee nimenomaisesti alkuperäistä ja muuttumatonta asiakirjaa. Tiivistettä kutsutaan joskus myös sormenjäljeksi (*fingerprint*).

## todennus

en authentication, verification

tietojärjestelmän käyttäjän (kuten henkilö, laite tai ohjelmisto) tai viestinnän toisen osapuolen aitouden ja oikeellisuuden varmistaminen

Käyttäjän todennuksen yhteydessä käyttäjä todistaa olevansa se, joka hän väittää olevansa. Esimerkiksi salasanan tietämällä käyttäjä todistaa olevansa henkilö, joka on oikeutettu käyttäjätunnuksen käyttöön, vastaavasti pankkiasioinnissa PIN-koodin tietämällä henkilö todistaa olevansa oikeutettu pankkikortin käyttöön. Vastaavaa toimikorttiin perustuvaa menetelmää käytetään vahvan tunnistamisen omaavassa sähköisessä asioinnissa: henkilö tunnistautuu tietojärjestelmään toimikortilla ja todentautuu PIN-koodin tai sormenjäljen käytöllä.

**toimikortti**

en smart card

suorittimen ja mikropiirejä sisältävä luottokortin kokoinen muovikortti

Toimikortti toimii erityisen lukulaitteen yhteydessä. Lukulaite voi olla joko kontaktillinen tai langaton toimikortinlukija esimerkiksi kulunvalvontaa tai tietojärjestelmän käyttöä varten. Kortille voi olla tallennettuna tietoja ja erilaisia sovelluksia. Usein toimikortilla käytettävien sähköisten palveluiden ja tietojärjestelmien käyttö on mahdollista myös vastaavat ominaisuudet omaavalla USB-avaimella (USB token).

**TTP**

en trusted third party

luotettu kolmas osapuoli; luotettu taho, joka tuottaa esimerkiksi varmennepalveluita (varmentaja) tai verkkonotaarin palveluita

Katso myös varmentaja.

**tunnistus**

en identification

menettely, jolla yksilöidään esimerkiksi tietojärjestelmän käyttäjä

Tyypillisesti tunnistus tapahtuu tarkistamalla, onko käyttäjän esittämä käyttäjätunnus hyväksyttävien tunnusten joukossa. Tunnistuksen jälkeen käyttäjä tyypillisesti todennetaan eli hän todistaa olevansa kyseinen henkilö esimerkiksi salasanan avulla.

**turvallisuustietoisuus**

en security awareness

organisaation henkilöstön tiedot ja asenteet, jotka koskevat turvallisuuden tavoitteita ja keinoja

Turvallisuustietoisuus on organisaation tietoturvallisuuteen mahdollisesti eniten vaikuttava kokonaisuus. Ilman hyvää turvallisuustietouden tasoa tekniset turvaamiskeinot saattavat olla turhia; suurimmat riskit koituvat tyypillisesti aina ihmisten toiminnan tai toimimattomuuden seurauksena.

**turvaluokitus**

en security classification

tietojen ja asiakirjojen jakaminen luokkiin niiden salassa pidettävyyden perusteella

Turvaluokkia voivat olla esimerkiksi julkinen, luottamuksellinen, salainen ja erittäin salainen. Terveydenhuollon asiakirjojen turvaluokittelussa voidaan noudattaa eri periaatteita kuin valtionhallinnon vastaavassa luokittelussa (katso VAHTI-ohjeistus). Esimerkiksi luottamuksellinen tieto voidaan tarvittaessa jakaa alaluokkiin "luottamuksellinen, hoitotieto" ja "luottamuksellinen, muu tieto".

**uhka**

en threat

(esimerkiksi) organisaatioon, tietoihin tai tietojärjestelmään tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus

**vaarantaa**

en compromise

asettaa alttiiksi uhkalle tai riskille

Julkisen avaimen infrastruktuurissa salaisen avaimen vaarantuessa (compromised private key) esimerkiksi PIN-koodin paljastumisesta tai toimikortin hukkumisesta johtuen henkilölle myönnetty varmenne mitätöidään ja merkitään varmentajan ylläpitämälle sulkulistalle. Tällöin tarkastettuaan sulkulistan mikä tahansa sähköisen asioinnin osapuoli voi estää palvelun, jos joku yrittää käyttää asiointiin kyseistä identiteettiä. Henkilölle myönnetään uusi avainpari ja uusi varmenne mitätöidyn tilalle.

**vahva tunnistus**

en strong authentication

käyttäjän tunnistus ja todennus, joka käyttää ainakin kahta kolmesta menetelmästä: jotakin, mitä käyttäjä on (sormenjälki); jotakin, mitä käyttäjä tietää (salasana, PIN-koodi) tai jotakin, mikä käyttäjällä on hallussaan (avain, toimikortti)

**varmenne**

en certificate

aitoustodistus, sähköinen identiteettitodistus, jonka ulkopuolinen luotettu taho (varmentaja) on myöntänyt julkisen avaimen infrastruktuurin mukaisessa palveluverkossa toimivalle taholle

Varmenne voidaan myöntää esimerkiksi henkilölle, laitteelle tai sovellukselle. Varmenteiden ominaisuuksista on määrittelyitä ITU:n standardissa X.509.

Varmenne sisältää tietoja esimerkiksi varmenteen voimassaolosta, myöntäjästä (varmentaja), käyttötarkoituksesta ja varmenteen kohteesta (kuten henkilö tai palvelin) sekä tämän julkisen avaimen. Laajennusosaan voi olla merkittynä muita tarpeelliseksi katsottuja tietoja, kuten henkilön sähköpostiosoite, valokuva tai muu biometrinen tunniste tai linkki julkiseen hakemistoon muita, mahdollisesti muuttuvia tietoja varten. Varmenne on varmentajan sähköisesti allekirjoittama, joten varmenteen aitous on varmistettavissa.

Katso myös henkilövarmenne.

Laitteistolle tai ohjelmistolle myönnettyä varmennetta kutsutaan tapauskohtaisesti laitevarmenteeksi, palvelinvarmenteeksi tai ohjelmistovarmenteeksi. Koska tällainen varmenne identifioi tyypillisesti sen organisaation, jonka palveluita kyseisellä laitteistolla ja ohjelmistolla tuotetaan, käytetään tässä yhteydessä joskus myös termiä organisaatiovarmenne.

**varmentaja**

en certificate authority

julkisen avaimen infrastruktuurissa luotettu taho, joka tuottaa käyttäjille avainparin, myöntää ja jakelee varmenteet ja ylläpitää varmenteet ja sulkulistat sisältävää hakemistoa

Varmenteen myöntöön ja mitätöintiin liittyviä prosesseja hallinnoi varmentajan valtuuttamana rekisteröijä. Käyttäjän salainen avain annetaan ainoastaan käyttäjälle esimerkiksi toimikortille tallennettuna. Avaimen käyttöön oikeuttava PIN-koodi voidaan toimittaa käyttäjälle avaimen toimituksesta erillisellä menetelmällä, mikä lisää toimitusprosessin turvallisuutta. Varmentajaa kutsutaan usein myös varmenneviranomaiseksi.

Väestörekisterikeskus (VRK) toimii varmentajana, joka myöntää kansalaisille sähköistä asiointia varten sähköisiä henkilöllisyystodistuksia, kansalaisvarmenteita. Tällöin salainen avain talletetaan henkilölle annettavaan toimikorttiin, HST-korttiin. Kortti toimii myös virallisena henkilötodistuksena ja matkustusasiakirjana.

**viranomaiskortti**

en civil service card

sähköinen henkilökortti, jota henkilö käyttää toimiessaan viranomaisena

**X**

X.509, katso varmenne.

X.500 on hakemistostandardi, jossa on määrittelyitä muun muassa hakemiston rakenteeseen, talletus- ja hakukäytäntöihin sekä hakemistoon talletettavien tietojen, objektien ja niiden ominaisuuksien (attribuuttien) osalta.

**älykortti**

katso toimikortti

# Liite 1 Sähköisen viestinnän tietoturvallisuuden järjestämistä ja tietosuojaa koskevia säädöksiä

Suomen perustuslaki (731/1999); 10 pykälä

Sähköisen viestinnän tietosuojalaki (516/2004)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

Arkistolaki (831/1994)

Henkilötietolaki (523/1999)

Laki yksityisyyden suojasta työelämässä (759/2004)

Viestintämarkkinalaki (393/2003)

Radiolaki (1015/2001)

Rikoslaki 38 luku ja 34 luku 9a pykälä

Laki eräiden suojausten purkujärjestelmien kieltämisestä (1117/2001)

Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

Laki sähköisistä allekirjoituksista (14/2003)

Laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003)

(Lähde www.ficora.fi/suomi/tietoturva/saadokset.htm)

# Liite 2 Julkisen avaimen arkkitehtuuri

Seuraavassa on kuvattu lyhyesti, mitä julkisen avaimen arkkitehtuuri, PKI (public key infrastructure), tarkoittaa ja millaisia termejä usein käytetään puhuttaessa sen avulla rakennetusta tietoturvasta. PKI on kokonaisuus, jolla voidaan toteuttaa verkkosovellusten ja -palveluiden tietoturvallisuus etukäteen määritellyllä ja sovitulla tavalla. Kokonaisuus muodostuu käytettävistä ohjelmistoista, laitteistoista, tietoliikenteestä ja palveluista.

Käyttäjä rekisteröityy verkkopalveluiden ja sovellusten käyttöä varten henkilökohtaisesti rekisteröijällä (RA, registration authority), joka todentaa käyttäjän henkilöllisyyden ennalta sovitun käytännön mukaisesti, esimerkiksi käyttäjän henkilöllisyystodistuksesta. Rekisteröijä edustaa varmentajaa (CA, certificate authority), joka on luotettava organisaatio tehtävänään myöntää sähköistä asiointia ja palveluita varten sähköisiä henkilötunnisteita, varmenteita (certificate). Henkilölle myönnettävää varmennetta, jossa varmentamisen kohteena on henkilön identiteetti, kutsutaan henkilövarmenteeksi. Varmentajaa kutsutaan usein luotetuksi kolmanneksi osapuoleksi (TTP, trusted third party). Varmenteiden ominaisuudet, luotettavuus ja käytettävyys kuvataan varmentajan julkaisemassa varmennepolitiikassa (CP, certificate policy).

Rekisteröijä luo käyttäjälle sähköistä asiointia varten avainparin. Avaimista toinen on julkinen ja toinen salainen, vain käyttäjän itsensä hallussa. Käytännössä avain on esimerkiksi 1024-bittinen luku. Avaimet ovat toisistaan riippuvaiset perustuen matemaattiseen algoritmiin. Avainpari on uniikki ja kutakin avainta vastaa vain yksi toinen avain. Tällaista kahteen avaimeen perustuvaa salausmenetelmää kutsutaan epäsymmetriseksi. Avaimina käytettyjen lukujen suuruus ja matemaattisen algoritmin ominaisuudet takaavat, että salaisen avaimen päättely tai selvittäminen julkisen avaimen perusteella on käytännössä mahdotonta. Juuri tähän arkkitehtuurin tietoturvallisuus perustuukin. Koska henkilö itse on salaisen avaimensa ainoa haltija, voidaan sähköisessä asioinnissa kiistämättömästi luottaa, että asioiva osapuoli on juuri kyseinen henkilö itse.

Salainen avain talletetaan esimerkiksi toimikortille, joka on suojattu siten, että avain ei ole poistettavissa kortilta. Julkinen avain julkaistaan varmenteessa, jossa on mainittu myös käyttäjän nimi ja tarvittaessa muita käyttäjän identifioivia tietoja. Varmenne siis yhdistää julkisen avaimen (ja siten myös salaisen avaimen) nimenomaisesti kyseiseen käyttäjään. Varmenne voidaan julkaista myös julkiseen hakemistoon, mutta se ei ole välttämätöntä. Tyypillisesti toimikortilla on salaisen avaimen lisäksi myös varmenne, joten asiointitapahtuman yhteydessä sovellusta käyttäessään henkilö voi toimittaa myös todisteen henkilöllisyydestään. Palvelun tuottaja tarkastaa varmenteen voimassaolon varmentajan julkaisemalta sulkulistalta varmenteen sarjanumeron perusteella. Täten esimerkiksi ammattiin liittyvien varmenteiden ei tarvitse sijaita julkisessa hakemistossa, vaikka puhutaankin julkisen avaimen arkkitehtuurista.

Salaisen avaimen käyttö eri sovelluksissa oikeutetaan esimerkiksi PIN-koodin kyselyllä tai sormenjäljen tunnistamisella. Kortinlukijaan asetettu toimikortti kytketään mukaan osaksi sovelluksen käyttöä esimerkiksi todentautumisen tai sähköisen allekirjoittamisen ajaksi. Sovellukset ja palvelut edellyttävät käyttäjältä toimikortin (ja siten avaimen) käyttöä aina, kun tietoturvallisuus sitä vaatii. Kortin käyttö mahdollistaa sen, että sovellus tunnistaa käyttäjän kiistattomasti (henkilöllä on kortti hallussaan ja PIN-koodi tiedossaan). Kortilla olevan salaisen avaimen avulla käyttäjä voi myös sähköisesti allekirjoittaa asiakirjat ja viestit, jolloin myöhemmin voidaan todeta allekirjoittaja ja varmistua myös siitä, että asiakirjaa tai viestiä ei ole muutettu jälkikäteen. Asioitaessa sähköisesti kaikki asiakirjat ja viestit voidaan myös salata käyttämällä toisen asiointiosapuolen julkista avainta. Tällaisen salauksen voi purkaa ainoastaan käyttämällä kyseisen julkisen avaimen vastinparia, salaista avainta, joka on ainoastaan toisen osapuolen hallussa.

Edellä mainitun mukaisesti PKI edesauttaa oleellisesti tietoturvallisuuden kehitystä ja lisäämistä sähköisissä palveluissa. Sitä hyödyntämällä saadaan aikaan käyttäjien luotettava todentaminen, luottamuksellisuuden säilyminen, asiakirjojen ja tietojen eheyden takaaminen ja tarvittaessa tapahtumien kiistämättömyys. Sähköiseen asiointiin, palveluihin ja allekirjoituksiin liittyen onkin jo voimassa olevaa lainsäädäntöä. Tämä antaa mahdollisuuden tuottaa sähköisessä muodossa myös niitä palveluita, jotka

ovat aiemmin esimerkiksi allekirjoitusvaatimusten takia olleet ainoastaan paperidokumentteihin perustuvia.

# Liite 3 Tarkastuslista

Seuraava tarkastuslista sisältää yksittäisiä toimenpiteitä, joiden avulla voidaan toteuttaa ja ylläpitää organisaation tietoturvallisuutta. Tarkastuslista on yksilöity ja numeroitu luettelo aiemmissa luvuissa mainittuihin kontrolleihin liittyvistä suositustoimenpiteistä. Listalla on toimenpiteen ja sen tunnisteen lisäksi varattu kohdat valmiutta, relevanssia, vastuuta ja aikataulua koskeville merkinnöille. Aikatauluun voidaan merkitä esimerkiksi säännöllisen katselmuksen ajankohta tai aikaväli. Lisäksi on varattu kohta lisätiedoille, johon voidaan mainita esimerkiksi havaitut puutteet ja niiden korjausaikataulu.

Esimerkin mukainen taulukko voidaan täyttää määrävälein, esimerkiksi kerran vuodessa, hyväksyä tietoturvallisuusjohdon toimesta ja liittää tietoturvallisuuslokina osaksi organisaation toiminnallista kuvausta. Sertifioinnin yhteydessä tapahtumien seurannan kirjaaminen ja dokumentointi on välttämätöntä.

Jos tarkastuksen kohteena on jatkuva toiminta, on olemassa oltava sekä ohjeistus että prosessi kuvattuna niin, että prosessin mukaan myös toimitaan. Toiminnasta saattaa myös löytyä loki, käsin kirjattu tai sähköinen. Esimerkiksi "kaikki tiedot, tietojärjestelmät ja tietovälineet on merkitty sovitun käytännön mukaisesti" tarkoittaa, että tiedot on sekä merkitty että niiden merkitsemisestä on olemassa ohjeistus ja toimiva prosessi.

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A1.1 Tietoturvapolitiikan luominen*** | | | | | |
| ***A1.1.1*** | Tietoturvapolitiikassa on mainittu johdon sitoutuminen | ☐ ok ☐ ei ok ☐ ei merkitystä | TT | 1.1.2005 | |
| ***A1.1.2*** | Tietoturvapolitiikassa on kuvattu vastuut tietoturvallisuudesta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.3*** | Tietoturvapolitiikassa on kuvattu menettely tietoturvadokumenttien ylläpidosta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.4*** | Tietoturvapolitiikassa on kuvattu, mitä ja minkä tyyppisiä tietoja suojataan (sekä organisaation tietojen että potilas- ja muiden henkilötietojen osalta) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.5*** | Tietoturvapolitiikassa on kuvattu, millä perusteella tiedot on luokiteltu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.6*** | Tietoturvapolitiikassa on kuvattu, mitä vaatimuksia liiketoiminta tai organisaation toiminta asettaa tietoturvallisuudelle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.7*** | Tietoturvapolitiikassa on mainittu riskit yleisellä tasolla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.8*** | Tietoturvapolitiikassa on mainittu lakien vaatimukset | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.9*** | Tietoturvapolitiikassa on mainittu noudatettavat standardit | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.10*** | Tietoturvapolitiikassa on kuvattu tietoturvatoiminnan päämäärä ja tavoitteet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.11*** | Tietoturvapolitiikassa on kuvattu hyväksytyt ja käytössä olevat periaatteet tarpeellisilta osin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A1.1.12*** | Tietoturvapolitiikassa on kuvattu organisaation koulutus, ymmärrys ja asiantuntemus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.13*** | Tietoturvapolitiikassa on kuvattu tietoturvallisuus-organisaatio | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.14*** | Tietoturvapolitiikassa on kuvattu seuranta ja raportointi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.15*** | Tietoturvapolitiikassa on kuvattu toiminta turvaloukkaustilanteissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.1.16*** | Tietoturvapolitiikassa on kuvattu sopimukset ja muut asiakirjat, jotka siihen vaikuttavat tai joihin se vaikuttaa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.2 Tietoturvapolitiikan julkaisu ja jakelu*** | | | | | |
| ***A1.2.1*** | Tietoturvapolitiikka on julkaistu siten, että se on helposti saatavissa ja ymmärrettävissä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.2.2*** | Tietoturvapolitiikka on jaettu koko organisaatiolle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.2.3*** | Organisaatiolla on ymmärrys tietoturvapolitiikan merkityksestä ja sisällöstä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.2.4*** | Kolmansien osapuolten käyttöön jaetusta versiosta on poistettu niiden tietoon kuulumattomat asiat | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.3 Tietoturvapolitiikan ylläpito*** | | | | | |
| ***A1.3.1*** | Tietoturvapolitiikalle on määritelty vastuuhenkilö | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.3.2*** | Tietoturvapolitiikan ylläpito ja päivitykset sisältyvät organisaation tietoturvallisuuden johtamisen prosesseihin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4 Tietosuojapolitiikan luominen*** | | | | | |
| ***A1.4.1*** | Tietosuojapolitiikassa on mainittu henkilön tietojen, kuten potilastietojen ja muiden henkilötietojen, käsittelystä säädetyt lait ja olemassa olevat standardit ja hyvä tietojenkäsittelytapa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4.2*** | Tietosuojapolitiikassa on kuvattu tarvittavalla tasolla tietojen säilytyksen, käsittelyn ja luovutuksen periaatteet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4.3*** | Tietosuojapolitiikassa on kuvattu henkilöstön toiminta ja osaaminen henkilön tietojen käsittelyyn liittyen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4.5*** | Tietosuojapolitiikassa on mainittu toiminta mahdollisissa väärinkäytöstilanteissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4.6*** | Tietosuojapolitiikassa on mainittu tietojärjestelmät ja tietojenvälitystekniikat, joilla henkilön tietoja käsitellään | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.4.7*** | Tietosuojapolitiikassa on kuvattu säännöt ja menetelmät henkilön oikeudesta omiin tietoihinsa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A1.4.8*** | Tietosuojapolitiikassa on kuvattu henkilön valitusmenettely | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.5 Tietosuojapolitiikan julkaisu ja jakelu*** | | | | | |
| ***A1.5.1*** | Tietosuojapolitiikka on julkaistu helposti saatavassa ja ymmärrettävässä muodossa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.5.2*** | Tietosuojapolitiikka annetaan potilaalle tai asiakkaalle pyydettäessä, ajanvarauksen tai ilmoittautumisen yhteydessä tai esimerkiksi vastaanottotiloista | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.5.3*** | Tietosuojapolitiikasta on tiedotettu riittävästi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.6 Tietosuojapolitiikan ylläpito*** | | | | | |
| ***A1.6.1*** | Tietosuojapolitiikalle on määritelty vastuuhenkilö | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A1.6.2*** | Tietosuojapolitiikan ylläpito ja päivitykset sisältyvät organisaation tietoturvallisuuden johtamisen prosesseihin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A2.1 Johdon sitoutuminen ja toiminta*** | | | | | |
| ***A2.1.1*** | Johdon tietoturvatoiminta on esimerkillistä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.2*** | Johto motivoi tietoturvatoimintaa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.3*** | Tietoturvallisuustavoitteet on määritelty kattavasti ja selkeästi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.4*** | Organisaation tietoturvallisuuden johtamiseen on määritelty prosessit | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.5*** | Riskienarviointi ja -hallinta sisältyy organisaation tietoturvallisuuden johtamiseen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.6*** | Tietoturvallisuusorganisaation on nimetty ja sen roolit ja vastuut ovat selkeät | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.7*** | Tarvittavat resurssit tietoturvallisuuden ylläpitoon ja kehittämiseen on varattu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.8*** | Tietoturvallisuusorganisaatio raportoi johdolle ja yhteistyö on saumatonta ja säännöllistä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.9*** | Henkilöstön turvallisuustietouden ylläpito ja hallinta, mukaan lukien palaute ja kurinpito, on mukana tietoturvallisuuden johtamisen prosesseissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.10*** | Organisaation toiminnan tietoturvallisuutta mitataan, seurataan ja valvotaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.1.11*** | Turvatoiminnasta annetaan säännöllistä palautetta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A2.1.12*** | Mahdollisesta turvatoiminnan sertifioinnista tiedotetaan henkilöstölle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2 Turvaorganisaation toiminta*** | | | | | |
| ***A2.2.1*** | Tietoturvatyössä noudatetaan tietoturvapolitiikkaa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.2*** | Suojattavat tiedot on määritelty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.3*** | Tietoihin kohdistuvat riskit on tunnistettu, kuvattu, luokiteltu ja analysoitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.4*** | Riskien hallinnalle on olemassa menetelmät, toimintamallit ja ohjeet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.5*** | Tietojärjestelmille ja tiedoille on määritelty yksilölliset omistajat ja vastuut | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.6*** | Uusien tietojärjestelmien käyttöönotolle on olemassa sovittu toimintatapa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.7*** | Uudet tietojärjestelmät on lisätty voimassa oleviin toimintaohjeisiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.8*** | Havaituista turvaloukkauksista on raportoitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.9*** | Turvaorganisaation oma tekninen osaamistaso on ajan tasalla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.10*** | Organisaatiolle on järjestetty tuki, neuvonta ja mahdollisuus turvallisuushavaintojen ja -rikkeiden raportointiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.2.11*** | Kolmansien osapuolten toiminnalle on määritelty auditointi- ja seurantaprosessi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.3 Lakien, standardien ja sopimusten huomioiminen*** | | | | | |
| ***A2.3.1*** | Tietoturvallisuusprosesseissa seurataan muutoksia laeissa, standardeissa ja viranomaisten suosituksissa ja otetaan muutokset huomioon | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.3.2*** | Tietoturvahallinto on mukana tarvittavissa yhteistyö- ja standardointielimissä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A2.3.3*** | Kolmansien osapuolten välisten sopimusten katselmointi on mukana tietoturvallisuusprosesseissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A3.1 Omaisuuden muoto*** | | | | | |
| ***A3.1.1*** | Tiedot säilytetään muodossa, joka vastaa niiden kriittisyyttä ja sen asettamia vaatimuksia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A3.1.2*** | Tietojenkäsittelyyn käytetään sellaisia laitteistoja, ohjelmistoja ja tietovälineitä, jotka takaavat tietojen saatavuuden ja käytettävyyden pitkänkin ajan kuluttua | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.1.3*** | Tiedot säilytetään sellaisessa formaatissa ja käytetään sellaisia tietorakenteita, jotka takaavat tietojen käytettävyyden pitkänkin ajan kuluttua | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.2 Inventaario ja luettelointi*** | | | | | |
| ***A3.2.1*** | Kaikki tärkeät tiedot on luetteloitu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.2.2*** | Kunkin tiedon osalta on kuvattu arvo, tärkeys, omistaja, sijainti ja turvaluokitus | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.2.3*** | Yksittäisten henkilöiden henkilökohtaisessa hallussa olevasta omaisuudesta (esimerkiksi kannettavat tietokoneet) on tehty erillinen luettelo | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.2.4*** | Merkittäville muutoksille alttiit ja uudenlaisia teknologioita toteuttavat tietojärjestelmät on tunnistettu, ja tieto on välitetty esimerkiksi muutoksenhallinnan prosesseille | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3 Tietojen omistus*** | | | | | |
| ***A3.3.1*** | Tietojen omistaja on nimetty tavalla, joka parhaiten tukee organisaation prosesseja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.2*** | Omistaja on huolehtinut tietojen asianmukaisesta kuvaamisesta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.3*** | Omistaja on huolehtinut tarvittavien pääsyoikeuksien jakamisesta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.4*** | Omistaja on huolehtinut, että tarvittavat käyttöohjeet on olemassa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.5*** | Omistaja on huolehtinut, että riittävät palvelutasosopimukset on käytössä tietojärjestelmien hoitoa ja ylläpitoa varten | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.6*** | Omistaja on huolehtinut oman osaamisensa ylläpidosta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.3.7*** | Omistajan ja päivittäistä hoitoa tekevä tapaavat säännöllisesti käydäkseen läpi järjestelmien hoitoon ja tietoturvaan liittyvät tapahtumat ja tarpeet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.4 Luokittelun periaatteet*** | | | | | |
| ***A3.4.1*** | Kaikkien tietojen tärkeyden luokittelussa noudatetaan sovittuja periaatteita | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.4.2*** | Kaikki tiedot on turvaluokiteltu sovittuja periaatteita noudattaen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.4.3*** | Kaikki pääsyoikeudet noudattavat sovittuja periaatteita eikä tarpeettomia oikeuksia ole valtuutettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A3.4.4*** | Tärkeys- ja turvaluokituksen ajoittainen arviointi kuuluu organisaation tietoturvaprosesseihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A3.4.5*** | Suojaustaso on määritelty ja tiedot on nimetty ja merkitty siten, että sekaannuksilta ja väärinymmärryksiltä vältytään | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.4.6*** | Tietoja ei ole ylisuojattu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5 Merkitseminen*** | | | | | |
| ***A3.5.1*** | Kaikki tiedot, tietojärjestelmät ja tietovälineet on merkitty sovitun käytännön mukaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5.2*** | Tietojärjestelmät ja käyttöliittymät osoittavat aina tarvittaessa suojaustason väärinkäytösten ja sekaannusten välttämiseksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5.3*** | Kaikissa paperimuotoisissa tulosteissa ja muussa materiaalissa (esimerkiksi röntgen- ja muut kuvat sekä laboratorio- ja muut mittaustulokset) on mainittu suojaustaso aina tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5.4*** | Eri suojaustasojen mukaiset käsittelysäännöt on asetettu näkyville ja ne ovat henkilöstön tiedossa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5.5*** | Kolmansille osapuolille toimitettavissa tiedoissa ja tietovälineissä on asianmukaiset suojaustason osoittavat merkinnät | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A3.5.6*** | Kolmansille osapuolille on tiedotettu käsittelysäännöt kunkin suojaustason mukaisille tiedoille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A4.1 Tarkastukset työsuhteen solmimisen yhteydessä*** | | | | | |
| ***A4.1.1*** | Organisaatioon palkattavien henkilöiden taustojen tarkastuksen menettelytavat on määritelty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.1.2*** | Kaikkien palkattavien henkilöiden taustat on selvitetty määrittelyiden mukaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.1.3*** | Tarkastuksia tekevät ja ilmeneviin tietoihin ovat oikeutettuja vain siihen valtuutetut henkilöt | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.1.4*** | Suoritettujen tarkastusten tulokset on arkistoitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.1.5*** | Strategisesti tärkeisiin ja tietoturvallisesti arkaluonteisiin tehtäviin palkattujen osalta on noudatettu tiukennettuja tarkastusmenettelyitä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.1.6*** | Kolmansien osapuolten palveluksessa olevien henkilöiden osalta tarkastukset on edellytetty tehtäväksi kolmansien osapuolten toimesta ja ne on tarvittaessa todistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2 Sopimukselliset velvoitteet*** | | | | | |
| ***A4.2.1*** | Kaikkien henkilöiden työsopimuksissa on mainittu tietoturvalliseen toimintaan liittyvät ehdot, vastuut ja velvollisuudet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.2*** | Kaikki työsopimukset sisältävät maininnat noudatettavista työsopimuslaeista ja sitoumuksen salassapidosta ja vaitiolosta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A4.2.3*** | Voimassa oleva tietoturvapolitiikka ja tietoturvallisuusohjeet koskevat kaikkia henkilöitä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.4*** | Jos henkilö ei ole työsopimussuhteessa organisaatioon, häneltä edellytetään salassapitosopimuksen allekirjoittaminen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.5*** | Salassapitosopimuksessa on tarvittaessa sovittu henkilötietojen suojaamisesta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.6*** | Henkilöitä on velvoitettu tietoturvallisesta toiminnasta myös organisaation ulkopuolisissa tiloissa, kuten työmatkoilla, etätöissä tai kolmansien osapuolten tiloissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.7*** | Henkilöitä on velvoitettu huolehtimaan kannettavien päätelaitteiden tietoturvasta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.8*** | Työ- ja muissa sopimuksissa on mainittu seuraamukset sopimuksenvastaisesta ja tietoturvallisuuden vaarantavasta toiminnasta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.9*** | Sopimuksissa on mainittu, kuinka pitkään salassapito on voimassa vielä työsuhteen loppumisen jälkeen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.10*** | Niiden henkilöiden kanssa, jotka ovat jo työsuhteessa ja joiden sopimuksissa ei ole mainittu tietoturvallisuutta ja salassapitoa asianmukaisesti, solmitaan erillinen salassapitosopimus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.11*** | Niille henkilöille, jotka joutuvat työtehtäviensä puolesta sitoutumaan kolmansien osapuolten laatimiin salassapito- tai vaitioloehtoihin ja allekirjoittamaan vastaavia sitoumuksia, on laadittu ohjeistus tällaisissa tilanteissa toimimista ja allekirjoitettavan sopimuksen arviointia varten. | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.2.12*** | On estetty tilanteet, joissa työntekijä voi joutua henkilökohtaiseen oikeudelliseen vastuuseen tai suorittamaan henkilökohtaisia sanktioita tai korvauksia kolmannelle osapuolelle. | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.3 Tietoturvavastuiden määrittäminen*** | | | | | |
| ***A4.3.1*** | Kaikille organisaation henkilöille on määritelty osaamistaso, joka henkilön täytyy vähintäänkin hallita | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.3.2*** | Kaikille organisaation henkilöille on määritelty tietoturvavastuut ja velvollisuudet, joita jokaisen henkilön on noudatettava | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.3.3*** | Kaikki erityisvastuut on kuvattu, sovittu ja dokumentoitu erikseen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.4 Tietoturvavastuista tiedottaminen*** | | | | | |
| ***A4.4.1*** | Kaikki henkilöt on tutustutettu voimassa oleviin ohjeisiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.4.2*** | Kaikki henkilöt on vastuutettu huolehtimaan turvallisuudesta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.4.3*** | Kaikki henkilöt ovat allekirjoittaneet ymmärtävänsä heihin kohdistuvat turvallisuusvaatimukset | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A4.4.4*** | Kaikki henkilöt ovat allekirjoittaneet vastaanottaneensa tietoturvapolitiikan, tietosuojapolitiikan ja tietoturvakäsikirjan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.4.5*** | Yhdellekään henkilölle ei ole myönnetty pääsyoikeuksia tietoihin ennen kuin hän on allekirjoittanut ymmärtävänsä tietoturvavaatimukset ja vastaanottaneensa sovitut asiakirjat | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5 Tietoturvatietoisuus, -osaaminen ja -koulutus*** | | | | | |
| ***A4.5.1*** | Tietoturvakoulutusta järjestetään säännöllisesti ja se on osa organisaation tietoturvallisuusprosesseja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.2*** | Jokainen henkilö osallistuu tietoturvakoulutukseen ja osallistuminen kirjataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.3*** | Koulutustilaisuudet sisältävät riittävästi tietoa kaikkiin kohdistuvista edellytyksistä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.4*** | Koulutustilaisuuksissa käsitellään seuranta, mittaaminen, palkitseminen ja väärinkäytöksistä rankaiseminen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.5*** | Koulutus kattaa tunnetut uhkat ja niiden havaitsemisen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.6*** | Koulutuksissa annetaan toimintaohje turvaloukkaushavainnoissa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.7*** | Koulutuksissa kerrotaan yhteyshenkilö tietoturvaasioihin ja lisätietoihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.8*** | Yhdellekään henkilölle ei ole myönnetty pääsyoikeuksia tietoihin ennen kuin hän on osallistunut tarvittaviin koulutustilaisuuksiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.5.9*** | Tietoturvavaatimuksiin tulleista muutoksista on tiedotettu ja järjestetty koulutus aina tarvittaessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6 Toiminta tietoturvaloukkauksissa*** | | | | | |
| ***A4.6.1*** | Tietoturvaloukkausten havainnointiin ja käsittelyyn on määritelty prosessi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6.2*** | Tietoturvaloukkaukset käynnistävät aina käsittelyprosessin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6.3*** | Tiedossa olevat uhkat on liitetty tarkkailun piiriin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6.4*** | Uusien uhkien, joista ei ole aiemmin havaintoja tai joita ei ole tunnustettu, käsittelyn liittäminen tarkkailtavaksi on olemassa prosessi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6.5*** | Ennen mahdollisia kurinpitotoimia on varmistuttu loukkauksen aitoudesta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A4.6.6*** | Kurinpitotoimet kohdistuvat yhtäläisesti kaikkiin henkilöihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A4.6.7*** | Kurinpitotoimissa on otettu huomioon rikkeen vakavuus ja vaikutukset sekä muut asiaan kuuluvat seikat | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.6.8*** | Kurinpitotoimista on tiedotettu tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7 Toimenpiteet työsuhteen loppuessa*** | | | | | |
| ***A4.7.1*** | Toimintatavat ja vastuut on määritelty henkilön työsuhteen loppuessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.2*** | Kaikki henkilöt ovat tietoisia itseensä kohdistuvista velvollisuuksista työsuhteen loppuessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.3*** | Henkilö on palauttanut kaiken hallussaan olevan organisaation omaisuuden ja tämä on kirjattu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.4*** | Henkilön kaikki kulku- ja pääsyoikeudet sekä kortit ja avaimet on lakkautettu ja palautettu asianmukaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.5*** | Henkilön tiedot on poistettu kaikista niistä asiakirjoista, joissa hänen on todettu kuuluvaksi organisaatioon | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.6*** | Henkilön työsuhteen loppumisesta on tiedotettu kaikille tarpeellisille tahoille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.7*** | On varmistettu, että henkilö ei kopioi mukaansa organisaation tietoja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A4.7.8*** | On varmistettu, että henkilö on siirtänyt osaamisensa riittävällä tasolla jollekin toiselle henkilölle organisaatiossa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.1 Tilojen rakenteet ja työskentelytilojen ympäristö*** | | | | | |
| ***A5.1.1*** | Tietojärjestelmät on sijoitettu tiloihin, joiden fyysinen suojaus vastaa säilytettävien tietojen turvatasoa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.2*** | Turva-alueet on selkeästi merkitty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.3*** | Turvarakenteissa ei ole murtautumisen mahdollistavia aukkoja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.4*** | Turvarakenteet suojaavat tulvilta ja maanjäristyksiltä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.5*** | Tilat on rakennettu siten, että niissä työskentely ei vaaranna terveyttä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.6*** | Tiloissa on saatavilla pelastusvälineet ja tarvittavat ohjeet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.7*** | Käytössä on tarvittavat kassakaapit, laitteistokassakaapit ja lukittavat laitetelineet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.1.8*** | Korkean turvallisuuden tiloissa ei säilytetä ylimääräistä paperia tai tyhjiä varmistusnauhoja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.9*** | Korkean turvallisuuden tilat eivät sijaitse julkisessa käytössä olevien tilojen välittömässä läheisyydessä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.10*** | Korkean turvallisuuden tiloista ei käy ulkopuoliselle ilmi, että ne ovat turvatiloja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.11*** | Kaikkia vierailijoita – potilaita, asiakkaita ja muita organisaation ulkopuolisia henkilöitä – varten on vastaanotto | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.12*** | Vastaanottotiski on miehitetty kaikkina aikoina, kun vierailijoita kulkee tiloissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.13*** | Kaikki vierailijat tunnistetaan, rekisteröidään ja heille myönnetään tarvittavat kulkuoikeudet vastaanottotiskillä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.14*** | Kulkuoikeuksien myöntämisestä sovitaan etukäteen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.15*** | Käytetyt rakenteet suojaavat murtautumiselta ja sekä kiinteistön sisällä että ulkopuolella tapahtuvilta vahingoilta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.16*** | Käytetään tarvittavaa automatiikkaa vahinkojen ja tunkeutujien havaitsemiseksi, hälyttämiseksi ja vahinkojen korjaamiseksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.17*** | Käytetään korotettuja lattioita tarpeen mukaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.18*** | Huolehditaan, että tiloihin joutuva vesi ei pääse kaapeleihin eikä tietojärjestelmiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.19*** | Palo-ovet pidetään suljettuina ja niissä on hälyttimet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.20*** | Huolehditaan, että varauloskäynneistä on ulospääsy, mutta ei ole sisäänpääsyä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.21*** | Kiinteistössä olevien eri organisaatioiden pääsy omiin tiloihin on estetty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.1.22*** | Erilaisilla turvatasoilla varustettujen tilojen välillä kulkemista kontrolloidaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.2 Kulunvalvonta*** | | | | | |
| ***A5.2.1*** | Tiloihin ei ole pääsyä ilman kulkuoikeuksia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.2.2*** | Tarvittaessa ulkopuolisilla on aina mukanaan saattaja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.2.3*** | Kaikki tiloissa asioivat henkilöt tunnistetaan ennen kulkuoikeuksien myöntämistä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.2.4*** | Kulkuoikeuksien myöntämisen yhteydessä kirjataan tarvittavat henkilön tiedot, myönnetyt oikeudet sekä tulo- ja lähtöaika | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.5*** | Ulkopuoliset henkilöt valokuvataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.6*** | Ulkopuolisilta henkilöiltä otetaan pantti, joka luovutetaan poistumisen yhteydessä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.7*** | Vierailijoille jaetaan ohjeet tiloissa liikkumiseen ja käyttäytymiseen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.8*** | Korkean turvallisuuden tiloihin ei myönnetä turhia kulkuoikeuksia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.9*** | Kulkua korkean turvallisuuden tiloissa kontrolloidaan tarvittaessa esimerkiksi sähköisin tunnistein ja PIN-koodein | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.10*** | Korkean turvallisuuden tiloissa liikkuminen kirjataan lokiin ja videoidaan tarvittaessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.11*** | Kaikilla henkilöillä on organisaation tiloissa liikuttaessa näkyvä tunniste: henkilöstöllä oma tunniste ja vierailijoilla omansa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.12*** | Organisaation henkilöstö on vastuutettu ja ohjeistettu saattamaan kaikki ilman tunnistetta liikkuvat vastaanottotiskille | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.13*** | Huoltotoimien yhteydessä ulkopuoliselle voidaan myöntää kulku turvatiloihin, jolloin hänellä on mukanaan saattaja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.2.14*** | Korkean turvallisuuden tiloihin jaetut kulkuoikeudet tarkastetaan ja päivitetään säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3 Toimistotilojen ja työhuoneiden suojaus*** | | | | | |
| ***A5.3.1*** | Työhuoneet ovat lukittavia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.2*** | Työhuoneita pidetään lukittuina aina työajan ulkopuolella | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.3*** | Työhuone lukitaan aina sieltä poistuttaessa tarpeen mukaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.4*** | Sisäiseen käyttöön tarkoitetut puhelinluettelot, organisaatiokaaviot ja muut tiedot säilytetään asianmukaisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.5*** | Arkaluonteisia tietoja sisältävät paperit, röntgen- ja muut kuvat ja muut tietovälineet säilytetään asianmukaisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.6*** | Papereiden ja tietovälineiden säilytystä varten on tarvittaessa olemassa lukittava säilytystila | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.3.7*** | Kriittisen tiedon säilytystä varten on tarvittaessa olemassa kassakaappi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.3.8*** | Arkistoidun arkaluonteisen tiedon säilytys ja arkistointitiloihin pääsy on erityisen kontrolloinnin piirissä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.9*** | Työpöydillä ei säilytetä arkaluonteista tietoja turhaan eikä asiattomalla tavalla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.10*** | Näyttöpäätteillä ei pidetä arkaluonteisia tietoja näkyvillä tarpeettomasti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.11*** | Huolehditaan, että asiaankuulumattomat henkilöt eivät kuule keskusteluja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.12*** | Puhuttaessa puhelimessa ja jätettäessä viestejä puhelinvastaajaan noudatetaan varovaisuutta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.13*** | Neuvottelutilat ovat näkö- ja äänieristettyjä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.14*** | Neuvottelutiloihin ei jätetä arkaluonteista materiaalia, kuten piirroksia tai papereita | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.15*** | Henkilökohtainen tietokone lukitaan poistuttaessa huoneesta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.16*** | Käytetään työaseman automaattista lukitusta ja näytönsäästäjää | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.17*** | Tietokoneessa käytettävää toimikorttia ei jätetä kortinlukijaan poistuttaessa työpisteestä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.18*** | Työasema, erityisesti kannettava tietokone, kiinnitetään tarvittaessa työpöytään | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.19*** | Kovalevyn sisältö salataan tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.20*** | Työasemissa käytetään virustorjuntaa ja palomuuriohjelmistoa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.21*** | Työasemiin ei asenneta ulkopuolisia ohjelmistoja ilman lupaa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.22*** | Sähköpostin käytöstä, liitetiedostojen avaamisesta, Internet-selailusta ja kielletyistä tai sallituista verkkosivustoista on olemassa säännöt | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.23*** | Tulostukset jaettuihin tulostimiin noudetaan välittömästi tulostuksen jälkeen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.24*** | Saapuvat telefaxit toimitetaan välittömästi niiden vastaanottajalle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.25*** | On olemassa ohjeistus, jota noudatetaan löydettäessä arkaluonteiseksi merkittyjä papereita tai muuta materiaalia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.3.26*** | Organisaatioon saapuva posti toimitetaan välittömästi vastaanottajalle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.27*** | Kopiokoneiden käyttö on valvottua ja tarvittaessa estetty työajan ulkopuolella | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.28*** | Tuhottavaa arkaluonteista materiaalia varten on olemassa oma lukittava asianmukaisin merkinnöin varustettu roskasäiliö, joka tyhjennetään sovitun prosessin mukaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.29*** | Tietojen käsittelyyn käytetään vain siihen tarkoitettuja tietojärjestelmiä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.30*** | Tietojärjestelmiä käytetään vain niiden suunnitellussa käyttötarkoituksessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.31*** | Potilastietoja käsitellään vain tarkoitukseen varatuilla työasemilla, joita ei käytetä esimerkiksi Internet-selailussa tai sähköpostikäytössä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.3.32*** | Työasemista voidaan poistaa levyke- ja cd-asemat sekä estää muut keinot, joilla saadaan helposti ja huomaamattomasti kopioitua tietoja organisaation ulkopuolelle | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.4 Työskentely korkean turvallisuuden tiloissa*** | | | | | |
| ***A5.4.1*** | Tieto korkean turvallisuuden tiloista, niissä työskentelystä ja siellä säilytettävistä tiedoista on vain tietoa tarvitsevilla henkilöillä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.4.2*** | Kaikkea tiloissa työskentelyä valvotaan ja tapahtumat kirjataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.4.3*** | Miehittämättömät tilat ovat lukittuja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.4.4*** | Tilat ovat jatkuvassa tai säännöllisessä valvonnassa ja tarkkailussa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.4.5*** | Erilainen kuvan tai äänen taltiointi tiloissa on kiellettyä, ellei sitä nimenomaisesti tapauskohtaisesti ole sallittu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.5 Lastaus- ja purkualueet*** | | | | | |
| ***A5.5.1*** | Pääsyä lastaus- ja purkualueelle on valvottua ja kulkuluvat tarkastetaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.5.2*** | Kaikki kulku alueella on luvanvaraista ja se rekisteröidään | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.5.3*** | Alueelta ei ole suoraa kulkua organisaation muihin tiloihin ilman kontrollipistettä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.5.4*** | Alueelle ja alueelta tehtävät kuljetukset kirjataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.5.5*** | Toimitukset noudetaan organisaation tiloihin mahdollisimman pian toimituksen jälkeen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.5.6*** | Kaikki toimitettavat tietojärjestelmät tarkastetaan, esimerkiksi ulkoisesti lastausalueella ja yksityiskohtaisesti myöhemmin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.5.7*** | Lastausalueen uloin portti tai ovi on suljettuna, kun alueelta siirretään materiaalia organisaation tiloihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6 Laitteistojen huolto*** | | | | | |
| ***A5.6.1*** | Laitteistoja hoidetaan ja puhdistetaan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6.2*** | Laitehuollossa sekä toimenpiteiden, huollon suorittajan että huoltovälin osalta noudatetaan valmistajien suosituksia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6.3*** | Laitteet huolletaan vain valtuutettujen henkilöiden toimesta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6.4*** | Lähetettäessä laitteita huollettavaksi tai korjattavaksi organisaation ulkopuolelle kiinnitetään huomiota kuljetuksenaikaiseen suojaan ja valtuudettomaan tietoihin pääsyyn | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6.5*** | Ulkopuoliseen huoltoon valtuutetaan vain riittävästä osaamisesta, luotettavuudesta ja maineesta nauttiva taho | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.6.6*** | Huollon suorittaja vastuutetaan sopimuksellisesti sekä laatuun että salassapitoon huollossa saamistaan tiedoista | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7 Laitteistojen sijoitus ja suojaus organisaation tiloissa*** | | | | | |
| ***A5.7.1*** | Laitteistot on sijoitettu niiden suojaustasoa ja tietojen kriittisyyttä vastaaviin tiloihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.2*** | Laitteistokomponentit on kahdennettu tarpeen mukaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.3*** | Palvelinlaitteistot sijaitsevat tiloissa, joissa on mahdollisimman vähän päivittäistä työskentelyä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.4*** | Varmistusnauhoja säilytetään eri tiloissa kuin tietojärjestelmiä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.5*** | Varmistusnauhoja ja varmistus- ja palautusprosessia testataan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.6*** | Erityistä suojaa vaativat laitteistot, esimerkiksi potilastietoja sisältävät arkistot, on erotettu muista järjestelmistä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.7*** | Erityissuojauksessa olevien laitteiden käytöstä ja käynnistä kirjataan merkintä tarvittaessa allekirjoituksella varustettuna | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.8*** | Laitteistoissa ja laitetelineissä on tarvittavat varkauksienestokiinnikkeet ja hälyttimet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.7.9*** | Laitteistot on sijoitettu tiloihin, joissa voidaan suojautua sekä ulkopuolisia että sisäisiä uhkia vastaan (esimerkiksi tulipalo, räjähdysvaara, ukonilmat, haitalliset kaasut ja savu, kosteus, vesi ja jäähdytinnesteet, pöly, tärinä, erilaiset kemialliset aineet ja sammutusaineet, sähkövirtakatkokset ja virtapiikit, oikosulut, säteily, EMP sekä tahallinen vahingoittaminen, ilkivalta ja terrorismi) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.10*** | Kuumissa, kylmissä, pölyisissä ja kosteissa tiloissa käytetään erillisiä suojalaitteita | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.11*** | Ruokailu, juominen, tupakointi ja muut vastaavat toimet on kielletty aina tarvittaessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.7.12*** | Ongelmat ja havainnot kirjataan tapahtumalokiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8 Suojaus organisaation tilojen ulkopuolella*** | | | | | |
| ***A5.8.1*** | Tietojen ja tietojärjestelmien vientiin organisaation ulkopuolelle tarvitaan lupa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.2*** | Henkilöt, joilla on oikeus viedä tietojärjestelmiä organisaation ulkopuolelle, on selkeästi tunnistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.3*** | Organisaation ulkopuolelle vietävä järjestelmien vienti ja tuonti kirjataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.4*** | Ulkopuolelle vietyjen laitteiden osalta tehdään pistotarkastuksia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.5*** | Kun tietoja tai tietojärjestelmiä on siirretty tiloihin, jotka eivät vastaa tietojen turvatasoa, niitä ei jätetä yksin vartioimattomaan tilaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.6*** | Henkilöstön käytössä on opas työskentelystä organisaation tilojen ulkopuolella, matkustettaessa ja etätöissä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.7*** | Organisaation tilojen ulkopuolella olevia tietoja säilytetään ja siirretään salattuna | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.8*** | Kannettavan tietokoneen käyttö on aina suojattu vähintään salasanalla | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.9*** | Matkustettaessa kannettava tietokone kuuluu käsimatkatavaroihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.10*** | Tietokoneiden säilytys hotelleissa, autossa, muussa kulkuvälineessä tai kongressitiloissa tehdään erityistä varovaisuutta noudattaen ja koneet naamioidaan tarvittaessa huomion ja kiinnostuksen välttämiseksi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.11*** | Etätyöskentelytiloissa on tarvittavat lukitut tilat ja noudatetaan muuta varovaisuutta ("*clean desk policy*", "*clear screen policy*") | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A5.8.12*** | Vältetään sellaisen koneen käyttöä etätyöhön, jota käytetään Internet-selailussa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.8.13*** | Noudatetaan varovaisuutta keskusteltaessa arkaluonteisista asioista organisaation tilojen ulkopuolella | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.8.14*** | Neuvotteluissa syntyvää materiaalia ei jätetä neuvottelutiloihin vaan otetaan mukaan tuhottavaksi myöhemmin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.8.15*** | Organisaation ulkopuolella sijaitsevat tietojärjestelmät vakuutetaan tarvittaessa erikseen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9 LVIS ja ympäristö*** | | | | | |
| ***A5.9.1*** | Tilojen virransyöttö on suunniteltu sekä kapasiteetin että jatkuvuuden osalta riittäväksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9.2*** | Katkeamattoman virransyötön (akut, varavoimageneraattori) toimintakyky ja kesto testataan säännöllisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9.3*** | Tärkeät toimisto- ja työhuoneet on liitetty katkeamattoman virransyötön piiriin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9.4*** | Virransyöttö on suojattu ylivirtapiikkejä ja oikosulkuja vastaan ja laitteet on maadoitettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9.5*** | Laitetilat on jäähdytetty ja ilmastoitu ylikuumenemisen estämiseksi ja erityisesti ikkunalliset tilat on tarvittaessa lämmitetty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.9.6*** | Tiloissa on automaattinen ja käsitoiminen palontorjuntalaitteisto | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10 Kaapelointi*** | | | | | |
| ***A5.10.1*** | Tietoliikenne salataan mahdollisuuksien mukaan aina | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.2*** | Kaapelit ja johdot on sijoitettu niille varattuihin kouruihin korotetun lattian alle, seinäkouruun, kattoon tai muualle näkymättömiin ja suojatuksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.3*** | Kaapelit on varustettu tarvittavilla merkinnöillä, esimerkiksi lähtö- ja päätepiste | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.4*** | Suositaan valokaapelin käyttöä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.5*** | Tietoliikenne- ja puhelinkaapelit on fyysisesti erotettu virtakaapeleista | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.6*** | Kaapelit on suojattu sähkömagneettisesti ja mahdollisia oikosulkuja vastaan ja niiden kunto tarkastetaan säännöllisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.10.7*** | Kaapelit ja tietoliikennelaitteet ja -yhteydet kahdennetaan tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A5.11 Puhelinverkot*** | | | | | |
| ***A5.11.1*** | Sekä sisäinen puhelinverkko että ulkoiset yhteydet laitteineen ja kaapeleineen on suojattu asianmukaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A5.11.2*** | Julkiset telepalvelut on hankittu luotettavilta toimijoilta ja niiden tietoturvallisuusmääräysten noudattaminen ja tietoturvapolitiikka on evaluoitu | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.3*** | Puhelinverkosta ja sen käyttäjistä on laadittu riittävä dokumentaatio | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.4*** | Puhelinten ja muiden kommunikointivälineiden käytöstä on laadittu ohjeistus | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.5*** | Hätätilanteiden hoitoa ja puhelinpalveluita varten on varattu riittävästi puhelinyhteyksiä | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.6*** | Puhelinliikenteen ja puhelinvaihteiden kuormitusta on seurannassa | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.7*** | Kuormitustilanteita varten on varattu riittävä kapasiteetti | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.8*** | Puhelinvaihteet ovat riittäviltä osiltaan kahdennettu | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.9*** | Avainhenkilöillä on käytössään vähintään kaksi puhelinliittymää (kannettava ja kiinteä) | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.11.10*** | Salakuuntelun estämiseksi pääsy puhelinvaihteisiin ja keskustiloihin on sallittu ainoastaan valtuutetuille henkilöille | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12 Tietojen, tietovälineiden ja laitteiden poisto*** | | | | | |
| ***A5.12.1*** | Tiedot tuhotaan sekä sähköisesti että fyysisesti mahdollisuuksien mukaan | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12.2*** | Jos sähköisen tuhoamisen lopputuloksesta ei voida olla täysin varmoja, tiedot tuhotaan aina fyysisesti (myös kovalevyt ja vastaavat) | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12.3*** | Arkaluonteista tietoa, esimerkiksi potilastietoja, sisältävät paperit tuhotaan aina fyysisesti esimerkiksi silppurissa tai laittamalla ne lukolliseen roskasäiliöön, jonka sisältö tuhotaan säännöllisesti | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12.4*** | Muu arkaluonteista tietoa sisältävä materiaali, esimerkiksi levykkeet, cd-levyt, kuvat ja filmit, tuhotaan aina fyysisesti tarpeellista keinoa käyttäen | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12.5*** | Normaali tietojen poisto (delete) ei riitä, vaan kovalevyllä oleva tieto aina ylikirjoitetaan | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A5.12.6*** | Vahingoittuneiden laitteiden poistossa noudatetaan aina erityistä varovaisuutta | ☐ok ☐ei ok ☐ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.1 Prosessikuvaukset, toimintaohjeet ja käyttöohjeet*** | | | | | |
| ***A6.1.1*** | Organisaation ydinprosessit ja muut tärkeät prosessit sekä henkilöiden toiminta on kuvattu | ☐ok ☐ei ok ☐ei merkitystä | | | |
| ***A6.1.2*** | Tehtävien ja vastuiden kuvaus on riittävän yksityiskohtainen ja kattava | ☐ok ☐ei ok ☐ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.1.3*** | Tärkeisiin tehtäviin on määritelty varahenkilöt, joilla on valmius tehtävien hoitoon | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.4*** | Tehtävät ja vastuut on tarpeen mukaan ositettu ja jaettu eri henkilöille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.5*** | Tehtäväkuvaukset ovat yksityiskohtaisia ja sisältävät riittävästi yksityiskohtia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.6*** | Tehtäväkuvaukset ja ohjeet ovat kaikkia niitä tarvitsevien saatavilla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.7*** | Arkaluonteisten tietojen käsittelystä ja noudatettavista menettelyistä on laadittu erilliset ohjeet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.8*** | Tietojärjestelmien kuvaukset ovat kattavat | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.9*** | Järjestelmien vastuuhenkilöiden ohjeistus on kattava | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.1.10*** | Ohjeiden, kuvauksien ja manuaalien ylläpidosta on sovittu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2 Muutoksen hallinta*** | | | | | |
| ***A6.2.1*** | Kaikista tietojärjestelmiin ja verkkoihin tehtävistä muutoksista pidetään kirjaa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.2*** | Oleellisista muutoksista (sellaisista, joilla on vaikutus esimerkiksi tietoturvallisuuteen, arkkitehtuuriin ja palveluihin) kirjataan riittävät yksityiskohdat kaikkiin tarvittaviin asiakirjoihin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.3*** | Muutoksista aiheutuvat riskit on analysoitu ennen muutostoimiin ryhtymistä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.4*** | Muutosten hyväksymiseen on menettely, jota noudatetaan kaikkien muutosten yhteydessä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.5*** | Muutoksista tiedotetaan riittävällä laajuudella | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.6*** | Muutosprosessi on suunniteltu siten, että muutostoimet voidaan keskeyttää ja palata alkuperäiseen tilanteeseen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.7*** | Muutosprosessista vastaavat henkilöt ja eri tehtävistä vastuulliset on tiedossa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.8*** | Muutosten jälkeen vanhentuneet tiedot poistetaan käytöstä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.9*** | Muutosten jälkeistä tilannetta seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.2.10*** | Kolmansista osapuolista johtuvat ja kolmansiin osapuoliin vaikuttavat muutokset sovitaan näiden osapuolien kanssa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.2.11*** | Jos järjestelmiin tehtävät muutokset aiheuttavat muutoksia palveluissa, kaikkien palveluita käyttävien tai niitä tuottavien osapuolten tiedotuksesta on huolehdittu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3 Kehitysjärjestelmät*** | | | | | |
| ***A6.3.1*** | Kehitysjärjestelmät ovat tuotantojärjestelmistä ja tarvittaessa tuotannollisesta tietoverkosta erillään | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.2*** | Testijärjestelmät ovat tuotantojärjestelmistä ja tarvittaessa tuotannollisesta tietoverkosta erillään | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.3*** | Eriyttäminen on toteutettu järjestelmien ja niillä käsiteltävien tietojen kriittisyyden perusteella ja vaatimusten mukaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.4*** | Kehityshenkilöillä ei ole pääsyä tuotannollisiin tietojärjestelmiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.5*** | Tuotannollisesta tietoverkosta ei ole pääsyä kehitysjärjestelmiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.6*** | Hyväksyntätestauksessa tuotannollista ympäristöä emuloidaan mahdollisimman tarkasti ja käytetään tarvittaessa tuotannollisen datan kopioita tai tuotantotietoa vastaavaa tietoa (dummy) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.3.7*** | Testi- ja koekäyttötilanteessa ilmenee, että kyseessä on testikäyttö | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4 Kolmansien osapuolten palvelut*** | | | | | |
| ***A6.4.1*** | Kolmansien osapuolten kanssa on solmittu sopimukset, joissa määritellään palvelutaso ja laatu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.2*** | Sopimuksissa on riittävät määräykset sanktioille, korvauksille ja rangaistuksille, jos vaadittua palvelutasoa tai laatua ei pystytä toteuttamaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.3*** | Yhteistyötä kolmannen osapuolen kanssa ohjataan ohjausryhmässä, joka hallinnoi yhteistyötä ja puuttuu mahdollisiin väärinkäytöksiin ja poikkeamiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.4*** | Ulkoistettaessa palveluita (esimerkiksi tietoverkkojen tai järjestelmien hoito) noudatetaan riittävää tietoturvallisuuden valvontaa sekä palveluiden käyttöönoton että käytön aikana | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.5*** | Kolmannelta osapuolelta edellytetään riittävä toimintakyky ja varmuus (vakavaraisuus, henkilömäärä, maine, luotetut ja standardien mukaiset tuotteet, sertifioitu toiminta), kun hankitaan tuotteita tai palveluita kriittiseen käyttöön | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.6*** | Kolmannelta osapuolelta edellytetään riittävää raportointia (tapahtumat, laatu, vasteajat, suorituskyky, vikatilanteet, muut palveluun vaikuttavat tekijät) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.7*** | Kolmannen osapuolen toimintaa seurataan, ja se tarkastetaan tai auditoidaan määräajoin tarpeen mukaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.4.8*** | Kolmannen osapuolen kanssa pidetään säännöllisiä ylläpitokokouksia, joissa arvioidaan toiminnan taso | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.5 Tietojärjestelmien ja tietoverkkojen hoito*** | | | | | |
| ***A6.5.1*** | Tietojärjestelmien ja -verkkojen hallintatoimet on määritelty, vastuutettu ja ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.2*** | Uudet tietojärjestelmät testataan ja vastuut määritellään ennen käyttöönottoa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.3*** | Järjestelmien toimintakykyä seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.4*** | Seurantaan on käytettävissä tarvittavat työkalut ja apuvälineet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.5*** | Seurannan kohteina ovat vähintään prosessorien kuormitus, toiminta- ja vasteajat, levytilan ja muistin täyttöasteet sekä verkkoliikenteen, tapahtumien ja käyttäjien määrä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.6*** | Vikoja ja tietoturvaloukkauksia seurataan vastaavalla menetelmällä kuin järjestelmien toimintakykyä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.7*** | Seurannan tuloksena seurannassa havaituista asioista vastuuhenkilö hälytetään tai häntä tiedotetaan aina tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.8*** | Seurantatietoja käytetään hyväksi määritettäessä järjestelmien ja verkkojen pullonkaulat ja kehitettäessä järjestelmiä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.9*** | Tietoliikennearkkitehtuuri on suunniteltu tietoturvalliseksi ja käytössä on esimerkiksi puolueettomat vyöhykkeet *(neutral zone, dmz*) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.10*** | Järjestelmät on suojattu viruksilta, ja virustorjunta ja sen päivitykset on mahdollisuuksien mukaan automatisoitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.11*** | Organisaation tietoverkko on eristetty ulkoisista verkoista palomuurein | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.12*** | Organisaation tietoverkko on eristetty ulkoisista verkoista tunkeutumisen havainnointi- ja estoohjelmin (IDS, IPS) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.13*** | Verkkoliikenteen määrää seurataan, ja palvelunestohyökkäykset tunnistetaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.14*** | Käyttäjien ja käyttöoikeuksien hallinta on vastuutettu ja ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.15*** | Järjestelmien käyttöä seurataan ja siihen puututaan tarvittaessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.16*** | Käyttäjien työasemissa on estetty tarvittaessa ulkoisten tietolähteiden (levyke- ja cd-asemat, modeemit, USB-muistit) käyttö | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.17*** | Käyttäjien työasemissa olevat modeemit toimivat takaisinsoittoperiaatteella | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.5.18*** | Käyttäjät eivät voi tehdä työasemiinsa oikeudettomia muutoksia (esimerkiksi ohjelmistojen asennukset) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.6 Käyttäjien velvollisuudet: tietoturvaohjeistuksen laadinta käyttäjille*** | | | | | |
| ***A6.6.1*** | Salassa pidettävistä asioista ja tiedoista on laadittu luettelo ja niiden käsittely on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.2*** | Turvallinen tapa käyttää tietokonetta ja tietojärjestelmiä on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.3*** | Virustorjunnan käyttö on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.4*** | Näytönsäästäjän ja sen salasanan käyttö on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.5*** | Etäyhteyksien käyttö on ohjeistettu (organisaatiossa oleviin tietoihin pääsy organisaation ulkopuolelta ja organisaatioon kuulumattomilta tietokoneilta) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.6*** | Kannettavien tietokoneiden kytkeminen organisaation ulkopuolisiin verkkoihin on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.7*** | Kotitietokoneen käyttö on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.8*** | Matkapuhelimen ja henkilökohtaisten PDA-laitteiden käyttö on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.9*** | Tietoturvallinen käyttäytyminen esimerkiksi matkustettaessa, julkisissa tiloissa ja puhuttaessa puhelimessa on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.10*** | Tietojen, erityisesti luottamuksellisten tietojen tallentaminen on ohjeistettu (mukaan lukien tietokoneen kovalevyn, verkkolevyjen, cd-levyjen, levykkeiden, USB-muistien ja paperitulosteiden käyttö tallennukseen) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.11*** | Internet-käyttö on ohjeistettu, ja kielletyt sivustot ja aihealueet on mainittu ohjeessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.12*** | Salasanamenettely on ohjeistettu, ja salasanojen laadusta (pituus, merkistö) on ohjeet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.13*** | Käyttäjät eivät anna salasanojaan toisille, eikä yhteiskäyttöisiä tunnuksia ole käytössä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.14*** | Organisaatiotunnusten kanssa identtisten käyttäjätunnusten ja salasanojen käyttö organisaation ulkopuolella on kielletty | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.15*** | Henkilökohtaisten työasemien käyttö muiden kuin työasioiden hoitoon on määritelty ja ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.16*** | Sähköpostin ja liitetiedostojen käyttö on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.17*** | Sähköpostien salaus- ja allekirjoituskäytännöt on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.6.18*** | Sähköpostia ei käytetä potilastietojen lähettämiseen Internetissä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.6.19*** | Työntekijöiltä edellytettävät toimet esimerkiksi avainten ja kulkukorttien säilytyksessä, havaitessaan väärinkäytöstilanteen tai vastaanottaessaan vieraita on ohjeistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7 Haittaohjelmilta suojautuminen*** | | | | | |
| ***A6.7.1*** | Ennen tietojärjestelmien hankkimista ja kehittämistä otetaan haittaohjelmien mahdollisuus huomioon | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.2*** | Käyttäjille annettava tietoturvakoulutus ottaa huomioon haittaohjelmat ja niiltä suojautumisen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.3*** | Käyttäjien työasemissa on aktivoitu ajantasainen virustorjunta, joka tarkastaa säännöllisesti uusien haittaohjelmien olemassaolon | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.4*** | Käyttäjiltä estetään tarvittaessa pääsy haitallisille sivustoille tai haitallisiin verkkoyhteyksiin (esimerkiksi aikuisviihde, uhkapeli tai tekijänoikeuksia rikkovat viihde- tai vertaisverkkopalvelut) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.5*** | Käyttäjät tietävät, että ainoastaan nimenomaisesti sallittujen ohjelmistojen (ja joihin on olemassa voimassaoleva lisenssi) käyttö on sallittua | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.6*** | Työasemissa säilytettävät tiedot liitetään varmistusmenettelyjen piiriin, mutta on suositeltavaa, ettei kriittisiä tietoja säilytetä työasemissa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.7*** | Haittaohjelmien esiintymistä seurataan, niistä raportoidaan ja ohjelmilta suojautumiseksi on varauduttu toimintasuunnitelmalla | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.8*** | Organisaation verkkoon ei sallita organisaatioon kuulumattomien työasemien kytkemistä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.7.9*** | Neuvottelutiloissa ja muissa tiloissa, joihin päästetään vierailijoita, on erilliset Internet-yhteydet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8 Kryptografia ja PKI*** | | | | | |
| ***A6.8.1*** | Kaikille verkkopalvelimille on hankittu palvelinvarmenne tarpeen mukaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.2*** | Verkkopalveluiden käytön tietoliikenne on tarpeen mukaan salattua | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.3*** | Palveluita tai järjestelmiä käyttäville henkilöille on myönnetty tarvittaessa varmenteet, joilla henkilöt todennetaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.4*** | Kriittisiä tietoja sisältävien tietojärjestelmien käyttäjien todennuksessa käytetään vahvaa tunnistusta ja varmenteellista toimikorttia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.5*** | Sähköistä allekirjoitusta käytetään tarpeen mukaan, jotta sekä lakien vaatimus allekirjoituksen käytöstä täytetään että tiedon eheys voidaan taata | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.6*** | Käytettävät ohjelmistot ja ohjelmistokoodi on sähköisesti allekirjoitettua (*signed code*) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.8.7*** | Organisaatiolla on menettely, jolla arvioidaan ulkoisten varmentajien myöntämien varmenteiden hyväksyminen organisaation järjestelmien ja palveluiden käytössä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.8.8*** | Myöntäessään itse varmenteita organisaation varmennepolitiikka ottaa huomioon varmenteiden käyttötarpeen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.8.9*** | On luotu säännöt, joilla organisaation myöntämiä varmenteita voidaan käyttää muiden organisaatioiden palveluissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9 Varmistukset ja palautukset*** | | | | | |
| ***A6.9.1*** | Kaikkien organisaatiossa käsiteltävien ja säilytettävien tietojen varmistustarve on määritelty siten, että tietojen tärkeys ja turvaluokitus on huomioitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.2*** | Kunkin tietojärjestelmän osalta olevassa varmistusmenettelyssä on määritelty aikataulut, vastuut, testaus, varmuuskopioiden säilytys ja toiminta palautustilanteessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.3*** | Varmistusten otosta pidetään pöytäkirjaa tai lokia, johon merkitään oleelliset tiedot varmistustapahtumasta ja sen onnistumisesta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.4*** | Varmuuskopiointiohjelmistoina, -laitteistoina ja -menettelyinä käytetään vain sellaisia, jotka tiedetään turvallisiksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.5*** | Käytettävistä ohjelmistoista on olemassa toimivat varmuuskopiot | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.6*** | Tietokantojen varmuuskopioinnissa huomioidaan tietokantojen varmuuskopioinnin työkalut | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.7*** | Tiedostojen nimeämisessä käytetään mahdollisuuksien ja tarpeiden mukaan versionumerointia, jotta vahingolliselta ylikirjoittamiselta vältytään | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.8*** | Kaikista tiedoista on olemassa riittävän tuore varmuuskopio riittävän etäällä tietojärjestelmistä, jotta fyysinen vahinko ei tuhoa sekä tuotannollista tietoa että varmuuskopioita | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.9*** | Varmuuskopioiden suojaus noudattaa vastaavaa turvatasoa kuin tuotannollisten tietojen suojaus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.10*** | Kryptografian käyttö tietojen varmistamisessa ja varmuuskopioiden salaus on selvitetty ja mahdolliset menetelmät on arvioitu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.11*** | Varmistusten salausperiaatteiden toteuttamiseksi on käytetty tarvittavia teknisiä ja hallinnollisia toimia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.12*** | Varmistusten toimivuus (varmistusten otto, varmistusmediat, tietojen eheys ja kattavuus, varmistusten palautus) testataan säännöllisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.13*** | Varmistusten palautuksessa on varauduttu mahdolliseen palautusprosessin pitkään kestoon | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.9.14*** | Automaattisten varmistusten onnistumista seurataan ja prosessi integroidaan hälytysjärjestelmiin seurantaa varten | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10 Tietovälineiden hallinta*** | | | | | |
| ***A6.10.1*** | Tietovälineiden käytöstä ja käsittelystä on sovittu toimintatavat ja käytöstä on laadittu ohjeistus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.10.2*** | Tietovälineiden käytöstä pidetään kirjaa ja tietovälineiden kiertoa seurataan mahdollisuuksien mukaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.3*** | Tietovälineiden tuhoamisessa noudatetaan sovittuja prosesseja ja tuhotut tietovälineet merkitään poistettuiksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.4*** | Arkaluonteisten tietojen tallentaminen eri tietovälineille ohjeistetaan tarkasti, ja niiden säilytyksestä ja tuhoamisesta annetaan kattavat ohjeet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.5*** | Siirrettäessä tietoja (esimerkiksi manuaalisesti) kertakäyttöiseltä tai siirrettävältä tietovälineeltä tietojärjestelmään, huolehditaan siirrettävien tietojen oikeellisuudesta, kattavuudesta ja eheydestä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.6*** | Pyritään välttämään arkaluonteisten tietojen tallentamista sellaisille tietovälineille, joille tallentaminen luo uhkan tietoturvallisuuden vaarantumiselle (levykkeet, cd-levyt, USB-muistit, tietyissä tapauksissa jopa paperitulosteet) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.7*** | Kaikkia tietovälineitä käytetään vain valmistajan ohjeiden ja suositusten mukaisesti (käyttötarkoitus, käyttöolosuhteet) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.10.8*** | Järjestelmädokumentaatio, prosessi- ja muut kuvaukset ja muut asiakirjat säilytetään siten, että oikeudettomilla henkilöillä ei ole pääsyä asiakirjoihin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11 Tiedonvälitys*** | | | | | |
| ***A6.11.1*** | Kaikki tiedonvälityksessä käytettävät menetelmät on otettu huomioon säännöissä ja ohjeissa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.2*** | Välitettäessä tietoja toiseen organisaatioon otetaan huomioon tarvittavat tietoturvavaatimukset, kuten osapuolten todentaminen, tietojen vastaanottajan oikeus tietoihin ja tietoliikenteen salaus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.3*** | Tietojen siirrosta ja sitä koskevista säännöistä sovitaan kirjallisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.4*** | Käytettävien tiedonsiirtotapojen uhkat on analysoitu ja riskit tietoturvarikkeisiin kartoitettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.5*** | Organisaation tietojärjestelmät on suojattu asianmukaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.6*** | Ohjelmallinen siirto, siinä käytettävät menettelyt ja rajapinnat tietojärjestelmästä toisen organisaation tietojärjestelmään on määritelty ja dokumentoitu yksityiskohtaisesti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.7*** | Vain sellaisten alihankkijoiden ohjelmistoja käytetään, joissa on toteutettuna vaatimusten ja standardien mukaiset tiedonsiirron ja käyttöliittymien rajapinnat | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.8*** | Lähetettäessä tietoja fyysisesti (esimerkiksi paperikopioiden tai cd-levyjen lähetys), suojataan sekä pakkaus että tiedot asianmukaisesti (lukitut pakkauslaatikot, sinetit, tiedon salaus cd-levyllä) sekä kuljetuksenaikaiselta vahingoittumiselta, lähetyksen katoamiselta tai varastamiselta että salaa lukemiselta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A6.11.9*** | Sähköinen tiedonvälitys suojataan haittaohjelmilta ja piilotetuilta kanavilta siten, että muodostettua tietoliikenneyhteyttä pitkin ei voida lähettää ylimääräistä tietoa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A6.11.10*** | Organisaatiosta lähetettävien tai vastaanotettavien sähköisten tietojen eheys, alkuperäisyys ja muuttumattomuus varmistetaan tarvittaessa käyttämällä sähköistä allekirjoitusta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.11.11*** | On laadittu menettelytapa niiden viestien analysoimiseksi, joiden alkuperää ei pystytä varmistamaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.11.12*** | Lähetysosoitteen kirjauksessa noudatetaan erityistä huolellisuutta ja tarvittaessa automaattista varmistusta (kuten sähköpostin tai telefaxin kohdeosoite tai numero) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.11.13*** | Huolehditaan, että luottamukselliset viestit eivät jää sähköpostiohjelmiston, erilaisten välimuistien (*cache*) tai telefax-laitteen muistiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.11.14*** | Tietojen julkaisemisesta yleisiin tai julkisiin medioihin on olemassa selkeät käytännöt ja ohjeistus, joka huomioi myös julkaistujen, mutta vanhentuneiden tietojen poiston | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A6.11.15*** | Yleisiin medioihin (myös organisaation omat Internet-sivut) julkaisu on vastuutettu, ja henkilöiden todennus tehdään sovituilla menettelyillä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A7.1 Pääsyn hallinnointi*** | | | | | |
| ***A7.1.1*** | Käyttäjien tunnistamisen menetelmistä ja käytettävistä tunnisteista on olemassa politiikka | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.1.2*** | Pääsyoikeuksista ja valtuuksien myöntämisestä on olemassa politiikka | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.1.3*** | Valtuuksien myöntöprosessissa on määritetty yksityiskohtaisesti käytettävät menettelyt | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.1.4*** | Verkkopalveluiden käytöstä, verkkoyhteyksistä ja tietojärjestelmäresurssien käytöstä on olemassa politiikka | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.1.5*** | Tietojärjestelmien ja sovellusten oletusprofiileita ja oletuskäyttäjiä ei ole käytössä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.1.6*** | Myönnettyjä valtuuksia katselmoidaan ja tarvittaessa puututaan virheellisiin valtuutuksiin tai epäkohtiin myöntöprosessissa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.2 Käyttäjänhallinta*** | | | | | |
| ***A7.2.1*** | Käyttäjän rekisteröinti ja valtuuksien määrittely noudattaa prosessia, jota noudatetaan myös valtuuksien muutoksissa ja poistoissa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.2.2*** | Käyttäjien rekisteröinti tehdään henkilökohtaisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.2.3*** | Rekisteröinnin yhteydessä käyttäjälle kerrotaan tietojen käsittelyn säännöt ja henkilö kuittaa vastuunsa tietojen suojaamisesta allekirjoituksellaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.2.4*** | Valtuuksien myönnössä käytetään allekirjoitettuja lomakkeita tai sähköistä hyväksyntämenettelyä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A7.2.5*** | Käyttäjätunnukset, salasanat ja fyysiset välineet (toimikortit ym.) toimitetaan turvallisella menetelmällä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.6*** | Fyysisiä välineitä ja niiden käyttöön oikeuttavia PIN-koodeja ei säilytetä samassa paikassa eikä kuljeteta samassa lähetyksessä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.7*** | Laajojen valtuuksien myöntöä ja käyttöä seurataan ja valvotaan tehostetusti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.8*** | Henkilöiden käyttäjätunnisteet ovat yksiselitteisiä ja uniikkeja, ja niistä käy ilmi henkilön tiedot riittävällä tasolla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.9*** | Käyttäjätunnisteista ei käy ilmi käyttäjän asema tai valtuudet | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.10*** | Käyttäjätunnuksista ja valtuuksista ylläpidetään ajantasaista luetteloa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.11*** | Yhteiskäyttöisiä tunnisteita (esimerkiksi ryhmätunnukset) ei ole käytössä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.12*** | Tunnukseton käyttö (esimerkiksi Internet-palveluissa) oikeuttaa pääsyn ainoastaan julkisiin tietoihin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.13*** | Käytettäessä varmennetta käyttäjän tunnisteena siihen kirjataan ainoastaan käytön kannalta välttämättömät tiedot | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.14*** | Käyttäjätunnusten käyttöä seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.15*** | Aktivoidut käyttäjätunnukset, joita ei käytetä, poistetaan tai lukitaan siten, että niiden käyttö estyy | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.16*** | Käyttäjällä on pääsy vain niihin tietoihin ja niillä oikeuksilla, jotka hänelle on myönnetty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.17*** | Käyttöoikeuksien rajoittaminen ei estä sellaista tietojen käyttöä, johon käyttäjällä on oikeus roolinsa tai tehtäväkuvansa perusteella esimerkiksi hätä- tai kriisitilanteessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.2.18*** | Vastuut on eriytetty asianmukaiselle tasolle ja riittävälle määrälle eri käyttäjiä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.3 Käyttäjien todentaminen*** | | | | | |
| ***A7.3.1*** | Tietojärjestelmiin kirjaudutaan riittävän turvallisella menetelmällä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.3.2*** | Kirjautumismenetelmä varoittaa ulkopuolisia vääristä kirjautumisyrityksistä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.3.3*** | Kirjautumisprosessissa näytetään järjestelmästä ainoastaan ne tiedot, joita käyttäjä tarvitsee kirjautuessaan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A7.3.4*** | Virhetilanteessa kirjautumisen yhteydessä järjestelmä ei kerro, missä vaiheessa kirjautumisprosessia virhe sattui | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A7.3.5*** | Kirjautumisyritysten määrä on sopivasti rajoitettu ja uusia kirjautumisyrityksiä säädetään sopivalla aikarajoittimella | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.6*** | Käyttäjätunnuksia tai salasanoja ei siirretä verkossa salaamattomina | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.7*** | Onnistuneen kirjautumisen yhteydessä käyttäjälle ilmoitetaan edellinen sisäänkirjautuminen ja virheelliset yritykset | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.8*** | Verkkoyhteyksien takaa kirjautuvat käyttäjät todennetaan riittävän turvallisilla menetelmillä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.9*** | Salasanojen hallintamenetelmä on turvallinen, ja sillä voidaan säätää laatutaso käyttäjien salasanoille | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.10*** | Korkean turvatason järjestelmiin ja kriittisen tiedon käsittelyyn on käytössä vahva käyttäjien tunnistusmenetelmä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.11*** | Toimikorttien käyttö oikeutetaan PIN-koodilla tai biometrisella tunnisteella, kuten sormenjäljellä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.12*** | Sähköisen allekirjoituksen luonnissa jokainen allekirjoitus vahvistetaan omalla PIN-koodin tai sormenjäljen syötöllä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.13*** | Kertakirjautumisessa käytetään vahvaa todennusta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A7.3.14*** | Tietoverkon laitteet, palvelut ja sovellukset on tunnistettavissa esimerkiksi palvelinvarmenteiden tai ohjelmistovarmenteiden avulla | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A8.1 Vaatimukset tietojärjestelmien turvallisuudelle*** | | | | | |
| ***A8.1.1*** | Riskianalyysiä ja organisaation toiminnan dokumentteja on käytetty määritettäessä tietojärjestelmien turvallisuustaso | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.2*** | Lakien vaatimukset on toteutettavissa ja otettavissa huomioon tietojärjestelmätasolla riittävän helpoilla tietojärjestelmien määrittelytoimenpiteillä siten, että järjestelmät noudattavat lakien vaatimuksia ja että ne ohjaavat ja tarvittaessa pakottavat käyttäjät oikeanlaisiin toimenpiteisiin niin, ettei käyttäjälle aiheetta anneta mahdollisuuksia laittomaan, virheelliseen tai väärään toimintaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.3*** | Tarvittavat tietoturvaominaisuudet (loki-, seuranta- ja hälytysmenetelmät, käyttöoikeuksien hallinta, salakirjoitus- ja allekirjoitusmenetelmät ja muut toiminnot) on määritelty | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.4*** | Kaupallisten valmisohjelmistojen turvaominaisuuksien arviointiin on menettely | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.5*** | Tietojärjestelmien sertifioimiseen on menettely | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.6*** | Vaatimukset on toteutettu tietojärjestelmiin riittävän aikaisessa vaiheessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A8.1.7*** | Testaussuunnitelma ja hyväksymiskäytäntö on kuvattu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.8*** | On varmistettu, että alihankkijoiden (tietojärjestelmien ja ohjelmistojen toimittajat ja kehittäjät) toiminta ja hankitut tuotteet vastaavat asetettuja laatuvaatimuksia. | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.9*** | On varmistuttu alihankkijan maineesta, taloudellisesti vakaasta asemasta ja tulevaisuudennäkymistä, kyvystä tuottaa tarvittavia ylläpito- ja huoltopalveluita sekä toiminnan laadusta, joka on sertifioitu. | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.1.10*** | Kriittisessä käytössä olevat tietojärjestelmät ja ohjelmistot on turvaluokiteltu ja niistä on laadittu asianmukainen turvaprofiili | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2 Tietojärjestelmien ja sovellusten sisäinen tietoturva*** | | | | | |
| ***A8.2.1*** | Tietojärjestelmissä käytettäville tiedoille tehdään tarvittaessa manuaalinen tarkastus ja siihen on valtuutettu tarvittavat henkilöt | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.2*** | Tietojärjestelmien kello käy reaaliaikaa ja järjestelmät on synkronoitu keskenään | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.3*** | Kryptografiset menetelmät noudattavat lakeja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.4*** | Tietojärjestelmä tarkastaa syötetietojen eheyden | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.5*** | Tietojärjestelmä tarkastaa syötetietojen kattavuuden ja käyttökelpoisuuden | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.6*** | Tietojärjestelmä tarkastaa syötetietojen sisäisen oikeellisuuden (merkistöt, oikeat päivämäärät ym.) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.7*** | Suurille tietomäärille on varattu ylivuotopuskuri ja liian suurien tietomäärien vastaanotto on estetty | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.8*** | Tietojärjestelmä tarkastaa syötetietojen alkuperän ja lähettäjän valtuudet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.9*** | Tietojärjestelmä huolehtii, että käsittelyprosessin aikana tietoa ei muuteta tai poisteta aiheettomasti ja että vain valtuutetuilla on pääsy tietoon | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.10*** | Käytössä on riittävät käyttäjien varoitusmenettelyt *('haluatko poistaa tiedon'*) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.11*** | Käytössä on tarvittavat varmistus- ja palautusmenettelyt | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.12*** | Käytössä on tarvittavat sähköisen allekirjoituksen tarkastus- ja uusimismenettelyt | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.13*** | Tiedonsiirto on turvattu riittävillä menetelmillä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.2.14*** | Eräajosovellukset käynnistetään oikeaan aikaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A8.2.15*** | Tietojärjestelmä varmistaa tulostustiedon eheyden, kattavuuden ja oikeellisuuden sopivalla menetelmällä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.2.16*** | Lähetettäessä tietoa tietojärjestelmä varmistuu vastaanottavan kohteen aitoudesta ja valtuuksista | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.2.17*** | Salausavainten varmuuskopioinnille on olemassa käytäntö | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3 Lähdekoodi*** | | | | | |
| ***A8.3.1*** | Ohjelmistokehityksessä noudatetaan siihen soveltuvia standardeja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.2*** | Oikeudettomilla henkilöillä ei ole pääsyä lähdekoodiin kehitysvaiheessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.3*** | Oikeudettomilla henkilöillä ei ole pääsyä tuotannollisessa käytössä olevan ohjelmiston lähdekoodiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.4*** | Kehitysjärjestelmä on erillinen, ei-tuotannollinen järjestelmä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.5*** | Lähdekoodi on säilytetty asianmukaisesti ja siitä on olemassa riittävät varmuuskopiot | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.6*** | Käytetään tarvittavia escrow-sopimuksia | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.7*** | Alihankkijoiden toimittamien ohjelmistojen osalta on solmittu tarvittavat huolto- ja ylläpitosopimukset | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.3.8*** | Tietojen siirtyminen piilotettuja kanavia pitkin on estetty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4 Muutoksen hallinta*** | | | | | |
| ***A8.4.1*** | Muutoksenhallintatoimet ja -menetelmät on dokumentoitu ja toimiin on oikeutettu ainoastaan valtuutetut henkilöt | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4.2*** | Muutosten suunnittelussa noudatetaan sopivaa muutospyyntö- ja hyväksymismenettelyä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4.3*** | Käytettävien ohjelmistojen käyttöön on hankittu tarvittavat lisenssit | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4.4*** | Tarpeettomia muutoksia ei toteuteta | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4.5*** | Muutoksista on kuvattu niiden piirteet, toiminnot, vaikutus muihin järjestelmiin ja organisaation toimintaan, käytännön menettely, testaus, laaduntarkastus ja dokumentointi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A8.4.6*** | Käytössä on sopiva versionhallintamenettely | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A8.4.7*** | On olemassa muutosten tiedotusmenettely | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.8*** | On olemassa muutosten testausmenettely | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.9*** | Muutokset ja käyttöön otettavat järjestelmät on testattu riittävällä laajuudella ja riittävän yksityiskohtaisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.10*** | Testitulokset ja katselmointitulokset on kirjattu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.11*** | Testaukseen käytetään siihen varattua testijärjestelmää | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.12*** | Muutosten vaikutus hälytysjärjestelmiin on huomioitu ja uusi konfiguraatio on dokumentoitu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.13*** | Järjestelmään tehtävistä muutoksista pidetään lokia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A8.4.14*** | Vanhat ohjelmistoversiot on tallennettu ja on varmistuttu, että uusilla versioilla luotua tietoa voidaan käyttää vanhoilla ohjelmistoversioilla | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A9.1 Jatkuvuussuunnittelun prosessi*** | | | | | |
| ***A9.1.1*** | Organisaatiossa on prosessia jatkuvuussuunnittelua varten | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.2*** | Organisaation johto on omistautunut jatkuvuussuunnittelulle | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.3*** | Jatkuvuussuunnittelu tehdään yhteistyössä liiketoiminnan, tietohallinnon ja turvahallinnon kanssa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.4*** | Organisaation toimintaan vaikuttavat riskit on tunnistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.5*** | Organisaation ydinprosessit ja toiminnan jatkumiseen vaikuttavat seikat on tunnistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.6*** | Jatkuvuussuunnittelua arvioidaan ja kehitetään säännöllisesti vastaamaan organisaation toimintaa ja toimintaympäristöä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.7*** | Kriisitilanteita varten on nimetty vastuut ja varattu resurssit | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.8*** | Ylimääräisiä vakuutuksia käytetään aina tarvittaessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.1.9*** | Tarvittaessa tietojärjestelmäriippuva toiminta voidaan korvata esimerkiksi paperien käsittelyllä, esimerkiksi potilasasiakirjojen käyttö paperimuodossa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A9.1.10*** | Vakaviin kriiseihin on varauduttu erillisellä varautumissuunnitelmalla, nimeämällä henkilöt, varaamalla resurssit ja harjoittelemalla kriisitilanteessa toimimista | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.2 Riskien arvioinnin prosessi*** | | | | | |
| ***A9.2.1*** | Riskien arvioinnille on prosessi ja niiden vaikutukset organisaation toimintaan tiedetään | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.2.2*** | Riskien arviointiin osallistuu riittävä määrä henkilöitä riittävällä asiantuntemuksella | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.2.3*** | Riskien arviointia käytetään jatkuvuussuunnittelussa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3 Jatkuvuussuunnittelun käytännön toteutus*** | | | | | |
| ***A9.3.1*** | Tarvittavat varautumistoimet, toipumistoimet ja osalliset henkilöt on tunnistettu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.2*** | Kaikista vastuista on sovittu ja ne on kirjattu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.3*** | Varautumistoimet on kuvattu yksityiskohtaisesti ja selkeästi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.4*** | Varautumistoimista pidetään lokia, johon kirjataan toimenpiteet, suorittaja ja aika | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.5*** | Toipumistoimet on kuvattu yksityiskohtaisesti ja selkeästi aikarajoineen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.6*** | Kriisien toipumisesta pidetään lokia, johon kirjataan tiedot tapahtumasta tai ongelmasta, toimenpiteistä, suorittajasta ja ajasta | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.7*** | Muita organisaatioita informoidaan tarvittaessa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.8*** | Organisaatio on saanut koulutuksen kriisitilanteita varten tarvittavilta osiltaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.9*** | Kriisitilanteita harjoitellaan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.3.10*** | Varautumis- ja toipumistoimien tehokkuutta testataan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4 Jatkuvuussuunnitelman testaaminen ja ylläpito*** | | | | | |
| ***A9.4.1*** | Kaikki tarvittavat henkilöt osallistuvat testeihin ja harjoituksiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.2*** | Harjoitukset ja testaus suunnitellaan etukäteen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.3*** | Tarvittaessa harjoitellaan siten, että kaikki osalliset eivät tiedä, että kyseessä on harjoitus | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A9.4.4*** | Tarvittaessa tehdään yllätystestejä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.5*** | Harjoitusten ja testien tavoite ja tulos kirjataan ja kulusta pidetään lokia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.6*** | Varmistusten ottoa ja palautusta testataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.7*** | Vikatilanteisiin on varauduttu riittävillä hälytysmenettelyillä ja käytössä on riittävä määrä kahdennettuja laitteita ja varaosia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.8*** | Kahdennettujen laitteiden, järjestelmien ja tietoliikenteen toimivuutta testataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.9*** | Varakonesalien ja varavoiman toimintaa testataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.10*** | Varahenkilöiden osaamista testataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.4.11*** | Epäonnistuneet testit aiheuttavat korjauksen menettelyissä, tekniikassa, ohjeissa, toiminnassa ja tarvittaessa muutoksia jatkuvuussuunnitelmissa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5 Jatkuvuussuunnitelman sisältö*** | | | | | |
| ***A9.5.1*** | Jatkuvuussuunnitelmassa on mainittu toiminnan käynnistävä tapahtuma tai olosuhde | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.2*** | Jatkuvuussuunnitelmassa on mainittu vastuulliset henkilöt | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.3*** | Jatkuvuussuunnitelmassa on mainittu tarvittavat aikataulut | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.4*** | Jatkuvuussuunnitelmassa on mainittu toimenpiteet yksilöidysti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.5*** | Jatkuvuussuunnitelmassa on mainittu tiedotusvelvollisuudet viranomaisiin, tiedotusvälineisiin ja muihin tahoihin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.6*** | Jatkuvuussuunnitelmassa on mainittu omistaja ja ylläpitoprosessi, testausmenettelyt ja osaamisvaatimukset | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A9.5.7*** | Jatkuvuussuunnitelmassa on mainittu toiminta kriisistä toipumisen jälkeen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A10.1 Noudatettavat lait*** | | | | | |
| ***A10.1.1*** | Organisaation toiminnassa noudatetaan voimassa olevia lakeja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.1.2*** | Muutoksia laeissa tarkkaillaan ja ne otetaan huomioon organisaation toiminnassa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A10.1.3*** | Organisaation käyttämissä strategioissa, suunnitelmissa ja ohjeissa on huomioitu ja mainittu riittävällä tarkkuudella aiheelliset lait | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.1.4*** | Tietoturvapolitiikassa on huomioitu ja mainittu aiheelliset lait | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.1.5*** | Tietosuojapolitiikassa on mainittu riittävällä tarkkuudella aiheelliset lait | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2 Tekijänoikeudet*** | | | | | |
| ***A10.2.1*** | Tekijänoikeuksien alaisten tuotteiden käyttö on ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.2*** | Organisaatiossa käsiteltävien tietojen käyttö on ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.3*** | Ohjelmistolisenssien siirto muille käyttäjille on ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.4*** | Luvanvaraisten lisenssien luovutus organisaation ulkopuolelle on ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.5*** | Käytössä olevat ohjelmistot estävät tietojen näkymisen ja saatavuuden oikeudettomille käyttäjille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.6*** | Käytössä olevat ohjelmistot estävät tietojen käytön niiden käyttötarkoituksen vastaisessa laajuudessa tai väärässä tarkoituksessa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.7*** | Käytettävät ohjelmistot kirjaavat tietojen käytön | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.8*** | Käytettävät ohjelmistot hälyttävät tietojen väärästä käytöstä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.9*** | Lisenssit ja sopimukset säilytetään asianmukaisesti ja riittävästi suojattuina | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.10*** | Ohjelmistojen hankintaa varten on laadittu ohjeistus | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.11*** | Ohjelmistojen hankinnan yhteydessä tarkastetaan oikeuksien siirtyminen ja suojataan oma organisaatio sopimuksin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.12*** | Tietoturvakoulutuksissa varmistetaan henkilöstön tietoisuus ohjelmistojen luvattoman käytön seurauksista | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.13*** | Käyttäjien työasemissa ei käytetä luvattomia ohjelmistoja | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.14*** | Käytettävien ohjelmistojen käyttäjämäärä tai käyttötarkoitus ei ylitä lisenssiä | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A10.2.15*** | Tietomurtoja ei yritetä esimerkiksi kirjautumalla tietoverkkojen palveluihin väärillä käyttäjätunnuksilla | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A10.2.16*** | Luvattomien ja sallittujen ohjelmistojen käyttöä tarkkaillaan ja käytetään tarvittavia auditointityökaluja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.2.17*** | Tarkkaillaan organisaation omaisuuden käyttöä ja estetään väärinkäyttö | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.2.18*** | Omaisuuden ja ohjelmistojen väärästä tai luvattomasta käytöstä aiheutuu tarvittavat seuraamukset | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.3 Standardit ja muut säännöt*** | | | | | |
| ***A10.3.1*** | Noudatetaan aiheellisia standardeja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.3.2*** | Toiminnan ja tietojärjestelmien standardien mukaisuus arvioidaan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.3.3*** | Luvattomia kryptografisia menetelmiä ei käytetä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.3.4*** | Luvanvaraisia kryptografisia menetelmiä ei käytetä ilman lupaa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4 Sopimukset, politiikat ja muut organisaation asiakirjat*** | | | | | |
| ***A10.4.1*** | Asiakirjat on jaettu asiakirjan tyypin ja käyttötarkoituksen mukaisiin luokkiin | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.2*** | Asiakirjoja säilytetään sellaisessa muodossa, että niiden oikeudeton muuttaminen, käyttö tai tuhoaminen on estettyä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.3*** | Asiakirjoja säilytetään sellaisessa muodossa, että niiden vääränlainen käyttö tai muu vaarantaminen on estettyä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.4*** | Noudatetaan solmittuja escrow-sopimuksia | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.5*** | Organisaation asiakirjojen luomis-, ylläpito-, käsittely- ja säilytyskäytännöt noudattavat lakeja | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.6*** | Noudatetaan organisaation itse julkaisemia politiikkoja ja periaatteita | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.7*** | Toimitaan sertifioidulla tavalla ja noudatetaan sertifikaatissa mainittuja käytäntöjä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.8*** | Julkisen avaimen infrastruktuurin salaiset avaimet ja niiden varmuuskopiot säilytetään asianmukaisesti ja varmennepolitiikassa kuvatulla tavalla | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.9*** | Tietojen ja tietojärjestelmien suojaaminen sekä lakien, standardien, sääntöjen ja sopimusten mukaisuus arvioidaan ja auditoidaan säännöllisesti | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A10.4.10*** | Poikkeamat sovitusta toiminnasta raportoidaan ja ne aiheuttavat tarvittavat toimenpiteet | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A11.1 Toiminnan määrittelyt*** | | | | | |
| ***A11.1.1*** | Tietojärjestelmien tapahtumatiedot kirjataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.2*** | Kiinteistön ja toimitilojen tapahtumatiedot kirjataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.3*** | Kirjattavat tiedot ovat keskenään yhteneväisessä ja mahdollisimman standardissa muodossa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.4*** | Järjestelmien tapahtumakirjauksen kellonajat on synkronoitu keskenään ja toimivat reaaliajassa | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.5*** | Kirjattuja tapahtumatietoja seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.6*** | Havaittujen poikkeustilanteiden käsittelystä on sovittu käytäntö ja se on ohjeistettu | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.7*** | Tietojärjestelmien riskianalyysi on otettu huomioon poikkeustilanteiden käsittelyssä rakentamalla seurantaan ja käsittelyyn oikeantasoiset menettelyt | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.8*** | Henkilöiden havaitsemille poikkeamille, haavoittuvuuksille ja uhkille on luotu ja ohjeistettu käytäntö | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.9*** | Muita tarkoituksia varten tarvittavien lokitietojen toimittamisesta kyseiselle taholle on sovittu käytäntö (esimerkiksi potilastietojen luovutusloki tai viranomaispyynnöt) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.10*** | Tapahtumatietojen kirjaus- ja käsittelyprosessi on tietoturvallinen eikä tietojen oikeudeton saanti, muuttaminen tai poisto ole mahdollista | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.11*** | Käytetään sekä yksittäisten tapahtumien kirjausta että tilaston keruuta esimerkiksi kuormituksen ja pitkäaikaisten trendien seurantaa varten | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.1.12*** | Alihankkijoiden kanssa on solmittu riittävän tasoiset ja kattavat ylläpito- ja huoltosopimukset | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.2 Tietojärjestelmien tapahtumien, käytön ja vikojen kirjaaminen*** | | | | | |
| ***A11.2.1*** | Tietojärjestelmien tapahtumakirjaus on aktivoitu ja automaattinen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.2.2*** | Lokiin kirjataan järjestelmän, prosessien ja sovellusten käynnistys- ja sammutustiedot (aika, prosessin nimi, oikeudet, statuskoodit) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.2.3*** | Lokiin kirjataan käyttäjien kirjautumistiedot (aika, käyttäjä, yhteystunniste, oikeudet) ja virheelliset tai väärät käyttöyritykset | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.2.4*** | Lokiin kirjataan järjestelmässä tehdyt ja tapahtuneet muutokset (konfiguroinnit, sovellusten ja laitteiden asennukset ja poistot) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.2.5*** | Lokiin kirjataan tiedostojen, tietokantojen, verkkoyhteyksien ja järjestelmän resurssien käyttö suorituskyky- ja kuormitustietoineen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A11.2.6*** | Lokiin kirjataan vikatilanteet, virheelliset tapahtumat sekä vikojen kuittaukset | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.2.7*** | Tietokanta-, tietoliikenne- ja muiden sovellusohjelmien erilliset tapahtumakirjausominaisuudet aktivoidaan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.2.8*** | Uusi lokitiedosto otetaan käyttöön riittävän usein kuormituksen välttämiseksi | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.2.9*** | Vanhojen lokitiedostojen käsittelyssä sovelletaan tietoturvallisia käytäntöjä | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.2.10*** | Käyttöoikeuksia lokitiedostoihin myönnetään ainoastaan järjestelmistä vastaaville henkilöille | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.3 Muut valvontakeinot*** | | | | | |
| ***A11.3.1*** | Kulunvalvontatiedot kirjataan (lähtö- ja tuloajat sekä liikkuminen tiloissa) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.3.2*** | Ovien, ikkunoiden ja muiden mahdollisten kulkureittien käyttö kirjataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.3.3*** | Korkean turvallisuuden tilojen sisäänkäyntien käyttö kirjataan erikseen | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.3.4*** | Fyysisiin olosuhteisiin liittyvät tiedot kirjataan (lämpötila, kosteusprosentti) | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4 Seuranta*** | | | | | |
| ***A11.4.1*** | Tapahtumakirjauksen ja hälytysjärjestelmän moitteetonta toimintaa seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.2*** | Tietojärjestelmien moitteetonta toimintaa ja kuormitustilannetta seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.3*** | Sovellusten ja tietokantojen moitteetonta toimintaa ja kuormitustilannetta seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.4*** | Tietoliikenteen määrää ja kuormitustilannetta seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.5*** | Käyttäjien kirjautumista ja toimintaa seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.6*** | Levytilojen käyttöastetta ja täyttymistä seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.7*** | Järjestelmiin ja sovelluksiin tehtäviä muutoksia ja niiden vaikutuksia seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.8*** | Viruksia, muita haittaohjelmia, verkosta tapahtuvia tunkeutumisyrityksiä, oikeudettomia kirjautumisyrityksiä ja palvelunestohyökkäyksiä seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.4.9*** | Administraattorin valtuuksien käyttöä seurataan | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A11.4.10*** | Automaattisia ja ilmoitettuja vika-, häiriö-, virhe-, ylikuormitus- ja väärinkäytöshälytyksiä seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.4.11*** | Kulunvalvontatietoja ja toimitilojen valvonnasta saatuja tietoja seurataan | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.5 Hälytykset ja raportointi*** | | | | | |
| ***A11.5.1*** | Toimitetaan hälytys vastuuhenkilöille ja tekniselle henkilöstölle mahdollisimman nopeasti | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.5.2*** | Hälytyksessä välitetään kaikki mahdollisimman tehokkaassa ongelman ratkaisemisessa tarvittavat tiedot | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.5.3*** | Vastaanotettu hälytys kuitataan vastaanotetuksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.5.4*** | On olemassa käytäntö ja ohjeet 'hiljaisen hälytyksen' toimittamista varten | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6 Poikkeamien käsittely ja seuraamukset*** | | | | | |
| ***A11.6.1*** | Hälytys käynnistää välittömän ongelman korjauksen tai ongelman ohittavan menetelmän rakentamisen | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.2*** | On olemassa käytäntö ja ohjeet välittää hälytystiedot palo-, poliisi- ja muille viranomaisille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.3*** | On olemassa käytäntö ja ohjeet välittää hälytystiedot tiedotusvälineille | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.4*** | On olemassa käytäntö ja ohjeet välittää hälytystiedot alihankkijoille, joiden edellytetään osallistuvan korjaustoimiin | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.5*** | Hälytystieto toimitetaan organisaation tai liiketoiminnan johdolle, tietoturvajohdolle tai tietohallintojohdolle arviointia ja jatkotoimenpiteitä varten | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.6*** | Seuraamusmenettelyt (rangaistukset, käyttöoikeuksien poistot, valvontaprosessin kehittäminen, tietohallinnon kirjanpito) on määritelty | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.7*** | Korjaustoimenpiteiden jälkeen hälytys kuitataan korjatuksi | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.6.8*** | Tiedot hälytyksen aiheuttaneesta tapahtumasta, korjaustoimenpiteet ja korjauksessa havaitut muut seikat tallennetaan poikkeustilannekäsittelyn kehittämistä varten | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.7 Mittaaminen ja kehittäminen*** | | | | | |
| ***A11.7.1*** | Hälytysten oikeellisuutta ja laatua mitataan (kaikista ja vain aiheellisista tapahtumista tulee hälytys sovittujen aikarajojen puitteissa sisältäen kaikki tarvittavat tiedot) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |
| ***A11.7.2*** | Toimintaa poikkeustilanteissa mitataan sopivilla mittareilla (hälytyksen saapumiseen kuluva aika, korjaukseen kuluva aika, alihankkijan saapumiseen kuluva aika, oikeanlainen tiedottaminen ongelmasta ja korjauksesta) | ☐ ok ☐ ei ok ☐ ei merkitystä | | | |

| Tunniste | Selitys | Valmius | Vastuu | Aikataulu | Lisätietoja |
|---|---|---|---|---|---|
| ***A11.7.3*** | Kerättyä hälytystietoa käytetään hyväksi organisaation tietoturvatoiminnan tason, riskianalyysin toimivuuden ja yhteensopivuuden tietoturva-, tietosuoja- ja muiden politiikkojen sekä tietohallinnon dokumenttien kanssa | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |
| ***A11.7.4*** | Alihankkijoiden suorittamat korvaus- ja hyvitys- ja sanktiokäytännöt on sovittu | ☐ ok ☐ ei ok<br>☐ ei merkitystä | | | |

# Liite 4 Malli tietoturvapolitiikaksi

Seuraavassa on esitettynä malli tietoturvapolitiikaksi, joka on käytettävissä sellaisenaan. Organisaatio voi tehdä malliin muutoksia ja lisäyksiä tarpeen mukaan, vähintäänkin lisätä omat tietonsa niille varattuihin kohtiin.

Tietosuojapolitiikka osoittaa organisaation sitoutumisen tietoturvalliseen toimintaan. Se on tarkoitus jakaa organisaation kanssa toimiville osapuolille – muille yrityksille ja organisaatioille, kuten yhteistyökumppaneille, alihankkijoille ja asiakkaille, sekä yksityishenkilöille tarpeen mukaan. Asiakirja on julkinen.

## Johdanto

<Organisaation nimi, esimerkiksi 'Keskussairaala Abc:n'> toiminta, palveluiden tuottaminen ja niiden tehokkuus on riippuvainen tietojenkäsittelystä ja sen toimintakyvystä, turvallisuudesta ja virheettömyydestä. Tietojenkäsittelyn turvallisuus on toiminnan jatkuvuuden ja palveluiden laadun kannalta erittäin tärkeää, siksi juuri näiden turvaaminen ohjaa <organisaation nimi> kaikkea tietoturvatoimintaa.
Tämä dokumentti on <organisaation nimi> tietoturvapolitiikka. Dokumentissa kuvataan ne periaatteet, joita <organisaation nimi> kaikessa toiminnassa noudatetaan <organisaation toimialue, esimerkiksi 'Keskussairaala Abc:n kaikilla toimialueilla Uudellamaalla'> tietoturvallisuuden toteuttamiseksi ja kehittämiseksi. Tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säädöksiä, standardeja ja suosituksia.

<Organisaation nimi> johto on vahvistanut tietoturvapolitiikan ja se on otettu käyttöön <päivämäärä>. Organisaation johto ja koko henkilöstö on sitoutunut tietoturvalliseen toimintaan ja toimii tässä dokumentissa julkaistujen periaatteiden mukaisesti. Tietoturvapolitiikka on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota. Tietoturvapolitiikasta voidaan tarvittaessa julkaista uusi versio, joka korvaa tämän dokumentin julkaisuhetkellä.

<Organisaation nimi> johto vastaa tietoturvapolitiikan julkaisusta. Dokumentti on saatavissa <paikka, esimerkiksi 'pyydettäessä vastaanotosta'> tai verkkosivuilta <verkkosivujen osoite, esimerkiksi 'http://www.abc.fi/tietoturvapoli-tiikka'>.

## Käsitteet

**tietoturva**

Tietoturvalla ja tietoturvallisuudella tarkoitetaan tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Suojaaminen sisältää erilaisia hallinnollisia ja teknisiä päätöksiä, periaatteita, menettelytapoja ja toimenpiteitä, joilla varaudutaan tietoihin kohdistuviin uhkiin ja estetään riskien toteutuminen tai vähennetään niiden vaikutuksia. Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien tietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton, esimerkiksi järjestelmän vikaantuminen, tapaturma tai luonnonkatastrofi.

**tietosuoja**

Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Tietosuojalainsäädännössä säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa liittyen.

**käytettävyys ja saatavuus**

Tiedon tai tietojärjestelmän käytettävyydellä ja saatavuudella tarkoitetaan, että tieto on tallennettu siten ja sellaisessa muodossa, että se on luettavissa, ymmärrettävissä, tulkittavissa oikein, kattava, ajantasainen, oikeellinen ja muuten käyttökelpoinen vaadittavalla tavalla ja helppokäyttöisesti ilman tulkinta- ja väärinkäyttömahdollisuutta. Tiedon, tietojärjestelmän ja palvelun on oltava saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti vaaditulla tavalla ja vaadittuna aikana.

**eheys**

Eheydellä tarkoitetaan, että tieto tai tietojärjestelmä on aito, sisäisesti ristiriidaton ja väärentämätön. Eheää tietoa, viestiä tai asiakirjaa ei ole oikeudettomasti muutettu eikä se ole muuttunut tai vahingoittunut.

**luottamuksellisuus**

Luottamuksellisuudella tarkoitetaan, että vain tietyn tai tiettyjen henkilöiden tietoon tarkoitetut tiedot säilyvät heidän hallussaan ja tiedossaan. Näiden tietojen suojaaminen vaarantumiselta tai paljastumiselta on suojattu kaikessa tietojen käsittelyssä, säilytyksessä ja tietoliikenteessä.

**pääsynhallinta**

Pääsynhallinta kattaa ne toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille. Pääsynhallinnassa tietojärjestelmien, tietoverkkojen ja tietojen käyttäjät tunnistetaan ja todennetaan sovitulla tavalla. Todennetuille käyttäjille myönnetään valtuudet – käyttäjien tehtävien ja roolien mukaisesti etukäteen sovitut käyttöoikeudet – järjestelmiin ja tietoihin. Käyttöoikeuksia ovat esimerkiksi lukuoikeus, kirjoitusoikeus, muutosoikeus, tuhoamisoikeus ja hallintaoikeus eli muiden käyttäjien oikeuksien määrittely.

**kiistämättömyys**

Kiistämättömyydellä tarkoitetaan teknisin menetelmin saatavaa varmuutta siitä, että tietty henkilö on allekirjoittanut tai lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys) tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi. Tapahtumaan, viestiin tai allekirjoitukseen voidaan liittää myös aikaleima, jolloin myös tapahtuman ajankohta on kiistämätön.

## Tietoturvan päämäärä ja tavoitteet

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jonka päämääränä on turvata <organisaation nimi> toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen oikeanlainen ja keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille, estää niiden valtuudeton käyttö, tahaton tai tahallinen tietojen tuhoutuminen tai vääristyminen sekä vähentää tietoturvariskejä ja minimoida niistä aiheutuvat vahingot. <Organisaation nimi> tiedot, tietojärjestelmät ja palvelut suojataan asianmukaisesti sekä normaali- että poikkeusoloissa riittävien hallinnollisten ja teknisten toimenpiteiden avulla.

Tietoturvallisuustyöhön kuuluu oleellisena osana turvattavien tietojen ja tietojärjestelmien määrittely ja luokittelu, näihin kohdistuvien uhkien ja riskien kartoitus sekä niiltä suojautuminen. Suojautuminen kattaa sekä riskien toteutumista ehkäisevät toimet, toiminnan jatkuvuutta suojaavat toimet että poikkeustilanteita varten laadittujen valmiussuunnitelmien mukaiset toimet. <Organisaation nimi> tietoturvallisuustyössä noudatettavat periaatteet on määritelty asiakirjassa <asiakirjan nimi, esimerkiksi 'tietoturvalliset toimintaperiaatteet'>, joka on saatavilla verkkosivuilta <verkkosivujen osoite>. Henkilö- ja potilastietojen suojaaminen on kuvattu erillisessä dokumentissa <tietosuojadokumentin nimi, esimerkiksi 'tietosuojapolitiikka'>, joka on saatavissa verkkosivuilta <verkkosivujen osoite, esimerkiksi 'http://www.abc.fi/tietosuojapolitiikka'>.

Jokaisen organisaation on noudatettava toiminnassaan voimassa olevia lakeja. Tietoturvallisuustyössä on otettava huomioon säädetyt lait ja se, mitä laeissa edellytetään organisaation toiminnan ja tietojenkäsittelyn turvallisuudelta. Tietoturvallisuudesta, arkaluonteisten tietojen käsittelystä ja erityisesti potilastiedoista on säädetty useassa eri laissa, joista tässä yhteydessä oleellisimmiksi voidaan katsoa laki viranomaisen toiminnan julkisuudesta (621/1999), henkilötietolaki (523/1999) ja laki potilaan asemasta ja oikeuksista (785/1992). Lisäksi tietoturvallisuudesta on olemassa erilaisia standardeja, joista mainittakoon *ISO/IEC 17799*.

## Organisointi ja vastuut

Tietoturvallisuustyötä johtaa ja valvoo `<toimintaa johtava elin, esimerkiksi 'keskussairaalan johtaja'>`, joka päättää turvallisuustoiminnan ja sen kehittämisen tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista.

Tietoturvallisuudesta huolehtiminen on koko `<organisaation nimi>` henkilöstön yhteinen asia. **Jokaisella työntekijällä** on henkilökohtainen vastuu huolehtia oman toimintansa turvallisuudesta ja noudattaa tehtäviensä hoidossa annettuja ohjeita ja määräyksiä. Jokainen on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuteen liittyvistä uhkista ja poikkeamista esimiehelleen tai tietoturvasta vastaavalle, erikseen nimetylle henkilölle. Tietoturva-asioista ja ohjeiden noudattamisesta omassa yksikössään vastaa **yksikön esimies**.

Käytännön tietoturvatoimia hallinnoidaan ja hoidetaan nimetyn tietoturvaorganisaation toimesta. Toimintaan kuuluvat päivittäisten toimien ohella tietojen turvaamismenetelmien määrittely ja ylläpito, työhön osoitettujen riittävien resurssien turvaaminen sekä välineistön ja toimenpiteiden turvallisuudesta ja tietoturvaominaisuuksista huolehtiminen. Tietoturvaorganisaatioon kuuluu

a) tietoturvavastaava, joka vastaa tietoturvallisten toimintaperiaatteiden toteutuksesta ja valvoo toimintaa, huolehtii turvatietoisuuden ylläpidosta, edistämisestä ja koulutuksesta sekä raportoi johdolle. Tietoturvavastaavalla on johdon antama valtuutus tietoturvallisuuskartoitusten tekemiseen ja havaittujen heikkouksien parantamiseen. Tietoturvavastaava vastuulla on ohjata tietoturvaryhmän toimintaa.
b) tietoturvaryhmä, joka toimii tietoturvavastaavan ohjauksessa ja vastaa organisaation keskeisten toimintojen turvanäkemyksiä. Ryhmään kuuluu edustaja keskeisistä toimintayksiköistä, tietohallintojohtaja, tekninen johtaja ja valmiusjohtaja. Tietohallintojohtaja edustaa ryhmässä tietojärjestelmä- ja tietoverkkoympäristöjen turvallisuusnäkemyksiä. Tekninen johtaja edustaa kiinteistö- ja toimitilaturvallisuutta ja valmiusjohtaja poikkeusoloihin varautumista.
c) tietosuojavastaava, joka on erikseen nimetty henkilö vastuunaan henkilötietojen ja potilastietojen suojaaminen.
d) Jokaisella tietojärjestelmällä on erikseen nimetty omistaja, joka vastaa tietojärjestelmän toiminnasta, turvallisuudesta, tietojärjestelmän hoidosta ja riittävistä toiminnoista, joilla turvallisuus toteutetaan. Näitä ovat esimerkiksi kriittisyyden määrittely, konfiguraatiotietojen ylläpito, seuranta- ja valvontamenettelyt, varmuuskopiointi ja käyttöoikeuksien hallinta.

Kaikki tietoturvaloukkaukset, väärinkäytökset ja poikkeustilanteet raportoidaan johdolle ja jokaiseen tilanteeseen reagoidaan sen vaatimalla tavalla.

## Koulutus ja ohjeistus

Jokaisesta tietojärjestelmästä ja käytettävästä ohjelmistosta on olemassa käyttöohjeet, joista käyttäjä saa tarvitsemansa tiedon järjestelmien ja ohjelmistojen sekä niissä olevien tietojen oikeanlaisesta käytöstä. Kaikille käyttäjille järjestetään riittävä määrä tietojärjestelmien käyttökoulutusta.

Tietoturvakoulutusta järjestetään sekä yksittäisinä koulutustapahtumina tietyille käyttäjäryhmille että tietoiskutyyppisinä tilaisuuksina. Koulutuksen tarkoitus on sekä ylläpitää riittävä tietoturva-asioiden

osaamistaso että muistuttaa säännöllisesti tietoturvan tärkeydestä. Koulutus on pakollinen koko henkilöstölle ja on osana jokaisen työntekijän henkilökohtaisia vaatimuksia ja osaamisen kehittämissuunnitelmaa.

Tietoturvallisuuden ohjeistus, tietoturvakäsikirja, sisältää kaiken oleellisen tiedon tietoturvan ylläpitämisessä. Se on jaettu jokaiselle työntekijälle, ja on myös saatavissa sisäisessä tietoverkossa. Jokaisella on velvollisuus noudattaa tietoturvakäsikirjassa mainittuja ohjeita ja määräyksiä, jotka sisältävät ohjeet esimerkiksi tietojen turvallisesta käsittelystä, henkilökohtaisen tietokoneen käytöstä, sähköposti- ja nettikäytöstä sekä salasanaohjeen.

## Tietoturvallisuuden toteutus

Tietoturvallisuuden toteuttamiseksi <organisaation nimi> on määritelty tietoturvalliset toimintaperiaatteet, jotka koostuvat yhdestätoista osakokonaisuudesta. Tietoturvatoiminta perustuu näihin periaatteisiin. Niissä määritellään hyväksytyt ja suositeltavat hallinnolliset ja käytännön toimet, tekniset vaatimukset ja rakenteet koko organisaatiolle ja käytettäville tietojärjestelmille. Tietoturvalliset periaatteet noudattavat säädettyjä lakeja ja ottavat huomioon eettiset toimintasäännöt sekä tietoturvallisuudesta laaditut standardit. Periaatteet on jaettu standardin ISO/IEC 17799 mukaisiin osakokonaisuuksiin, joista alla on esitetty lyhyt kuvaus.

Periaatteet huomioidaan kaikissa erilaisissa toiminta- ja käyttöohjeissa, säännöissä ja määräyksissä, joita organisaation päivittäisessä toiminnassa käytetään ja joiden mukaan organisaatiossa toimitaan. Jokainen työntekijä on tietoinen omaan työhönsä liittyvistä turvallisuusasioista ja on sitoutunut tietoturvalliseen toimintaan.

**tietoturvapolitiikka ja tietosuojapolitiikka**

Tietoturvapolitiikka on johdon kannanotto ja julkilausuma organisaation tietoturvallisuuden toteuttamiseen. Sen olemassaolo on vakuutus organisaation kanssa asioiville, että tietojenkäsittely organisaatiossa on luotettavaa ja että tietoturvallisuuteen on paneuduttu. <Tietosuojadokumentin nimi> puolestaan on osoitus organisaatiossa käsiteltävien henkilö- ja potilastietojen käsittelyn ja säilytyksen luotettavuudesta, lainmukaisuudesta ja tietojen luottamuksellisuuden säilymisestä. <Tietosuojadokumentin nimi> ohella henkilölle annetaan pyydettäessä rekisteriseloste, josta ilmenee henkilöstä säilytettävät henkilötiedot lain edellyttämällä tavalla.

**tietoturvallisuuden hallinnointi ja organisaatio**

Tietoturvallisuuden toteuttamiseen nimetty turvaorganisaatio vastaa koko organisaation tietoturvallisuuden määrittelystä, toteuttamisesta ja turvallisuustason ylläpidosta. Osakokonaisuus määrittelee tietoturvatoiminnan yleiseen hallinnointiin ja organisointiin liittyvät toimet aina johdon toimista ja turvaorganisaation nimeämisestä turvaorganisaation käytännön toimintaan.

**omaisuuden hallinta**

Tässä osakokonaisuudessa kuvataan ne vaatimukset ja määritellään ne toimet, jotka liittyvät organisaation omaisuuden – myös tietojen ja tietojärjestelmien – hallintaan. Omaisuus luetteloidaan ja merkitään, omistus ja omistaja määritellään, arvioidaan tietojen tärkeys sekä tietoihin kohdistuvat uhkat ja riskit, joiden perusteella tiedot luokitellaan ja niille määritellään suojaustaso sekä tarvittavat pääsyoikeudet.

**henkilöstöturvallisuus**

Tämä osakokonaisuus määrittelee periaatteet henkilöstön turvallisuuden hallintaan. Ihmisten toiminta, joko tahallinen tai tahaton, on suurin turvallisuutta uhkaava tekijä. Siksi henkilöstöturvallisuuteen liittyen on määritelty tarkat toimet aina työsuhteen solmimisesta sen loppumiseen asti. Ne sisältävät sopimukselliset velvoitteet, työtehtävien, vastuiden ja tarvittavan osaamistason määrittämisen sekä toimenpiteet turvaloukkaustilanteissa.

**fyysisen ympäristön turvallisuus**

Fyysisen ympäristön suojauksella käsitetään sekä organisaation tuotanto- että toimitilojen ja niissä sijaitsevien tietojenkäsittelylaitteiden fyysistä suojaamista. Osakokonaisuus määrittelee menetelmät, millä estetään valtuudeton pääsy organisaation tiloihin, tietoihin ja tietojärjestelmiin ja miten vartiointi hoidetaan, millä suojataan fyysinen ympäristö ja kiinteistöt sekä turvataan virransyöttö ja ilmastointi, ja miten tietojenkäsittely suojataan esimerkiksi tulipaloilta, vesivahingoilta ja murroilta.

**tietojärjestelmien käytön ja tiedonvälityksen turvallisuus**

Tietojärjestelmien oikeanlainen ja turvallinen käyttö sekä tiedonvälityksen ja tietoliikenteen turvaaminen ovat tämän osakokonaisuuden tavoitteet. Myös järjestelmien operointi, huolto ja hoito sekä pääkäyttäjiltä näissä vaadittavien toimenpiteiden taso määritellään. Järjestelmien ja tietoliikenneverkkojen katkoton ja turvallinen käyttö suojataan tarvittavilla toimilla ja määritellään ne toimet, joilla voidaan palauttaa vikaantunut järjestelmä toimintakuntoiseksi.

**pääsynhallinta**

Osakokonaisuudessa määritellään tietoihin ja tietojärjestelmiin pääsy – miten henkilöt tunnistetaan ja todennetaan, kenellä on pääsy mihinkin tietoihin, miten he ovat oikeutettuja käsittelemään tietoja ja millaisilla välineitä ja tietoliikenneyhteyksiä heillä on käytössään tietojen käsittelemiseksi. Kokonaisuudessa määritellään myös hyväksyttävät salasanakäytännöt, järjestelmien etäkäyttömenetelmät ja etäkäytössä käytettävät tunnistamistavat, etätyötavat, sähköpostin ja liitetiedostojen käyttötavat sekä hyväksyttävät ja kielletyt verkkopalvelut.

**tietojärjestelmien kehitys ja ylläpito**

Osakokonaisuus määrittelee sen toiminnan, millä varmistetaan, että organisaatiossa käytettävät – itse kehitettävät tai kolmansilta osapuolilta hankittavat – tietojärjestelmät ja ohjelmistot ovat tietoturvallisia ja millaisia ominaisuuksia ja piirteitä niiltä edellytetään. Myös ohjelmisto- ja järjestelmätoimittajat sekä alihankkijat arvioidaan ja ainoastaan riittävän luotettavilta ja riittäviä oheispalveluita tuottavilta yrityksiltä hankitaan tuotteita ja palveluita organisaation käyttöön.

**toiminnan jatkuvuus**

Toiminnan jatkuvuussuunnittelussa varaudutaan sellaisiin kriisitilanteisiin, jotka voivat estää tai keskeyttää organisaation toiminnan, vaikuttaa organisaation toimintakykyyn tai muutoin vahingoittaa sen toimintaa. Osakokonaisuus määrittelee, miten kriisitilanteilta suojaudutaan ja toteutuneista kriiseistä toivutaan normaalitilaan suunnitellusti ja mahdollisimman nopeasti.

**laillisuus ja sääntöjen mukaisuus**

Organisaation toimintaan vaikuttavat lait, säännökset ja tietynlaiseen toimintaympäristöön velvoittavat standardit arvioidaan ja toiminnassa noudatetaan näitä lakeja, säännöksiä ja standardeja. Muutokset evaluoidaan ja tarvittaessa muutetaan toimintatapoja tai teknisiä ympäristöjä vastaamaan uusia vaatimuksia. Erityisesti sosiaali- ja terveydenhuoltoa koskevia säädöksiä on runsaasti. Nämä velvoittavat sekä oikeisiin toimintatapoihin että oikeanlaisten menetelmien ja teknologioiden käyttöön.

**poikkeustilanteet**

Tässä osakokonaisuudessa määritellään, miten normaalista toiminnasta ja normaaleista tilanteista poikkeavaa toimintaa ja tilanteita valvotaan ja seurataan, miten ne havaitaan, millaisia hälytyksiä lähetetään, miten ja keitä hälytetään sekä millaisiin toimenpiteisiin ryhdytään ongelmien korjaamiseksi ja poikkeustilanteesta normaalitilaan palaamiseksi. Mahdolliset seuraamukset määritellään, johtuivatpa tilanteet henkilöiden puutteellisesta tai väärästä toiminnasta tai teknisistä ongelmista.

# Liite 5 Malli tietosuojapolitiikaksi

Seuraavassa on esitettynä malli tietosuojapolitiikaksi, joka on käytettävissä sellaisenaan. Organisaatio voi lisätä malliin tarpeen mukaan omia tietojaan. Dokumentin nimeäminen tietosuojapolitiikaksi ei välttämättä kuvaa dokumentin sisältöä riittävän hyvin kohderyhmälle. Siksi sille voidaan antaa nimeksi myös esimerkiksi *'kuvaus henkilötietojen käsittelystä', 'yksityisyyden suojaaminen tietojenkäsittelyssä'* tai *'tietosuojaseloste'*.

Termi "tietosuoja" on juridinen, joten asiakirja keskittyy tietojenkäsittelyn lainmukaisuuteen. Sen ei tarvitse sisältää yksityiskohtaista tietoa. Tarpeen mukaan voidaan viitata myös tietoturvapolitiikkaan, joka voidaan jakaa lisätietoja haluaville. Asiakirja on julkinen.

## Johdanto

`<Organisaation nimi, esimerkiksi 'Keskussairaala Abc'>` noudattaa potilaidensa ja asiakkaidensa henkilötietojen ja muiden luottamuksellisten tietojen käsittelyssä voimassa olevaa lainsäädäntöä ja hyvää, turvallista ja standardien mukaista tietojenkäsittelytapaa. Lähtökohtaisesti kaikki viranomaisen toiminta on julkista. Toisaalta laki myös edellyttää, että henkilön yksityisyydensuoja on turvattava. Tämän yksityisyydensuojan takaamiseksi kaikki `<organisaation nimi>` hallussa olevat henkilöä koskevat tiedot on suojattu. Niitä voidaan käsitellä ainoastaan valtuutettujen henkilöiden toimesta, luovuttaa ainoastaan henkilön itsensä suostumuksella ja niitä säilytetään ja käsitellään siten, että ulkopuolisilla ei ole mahdollisuutta päästä tietoihin käsiksi.

Tietojenkäsittelyn turvallisuus on `<organisaation nimi>` toiminnan ja palveluiden laadun kannalta erittäin tärkeää. Tietoturvallisuutta toteutetaan käyttämällä ennalta määrättyä, turvallista tietojenkäsittelytapaa ja turvallisia menetelmiä ja teknologioita. Koko henkilöstö on tietoinen tietoturvallisuudesta ja sen merkityksestä, koulutettu ja ammattitaitoinen toimimaan turvallisella tavalla. Jokainen noudattaa työssään kaikkia turvallisuuteen liittyviä ohjeita ja määräyksiä. Kaikista tietojärjestelmistä on olemassa käyttöohjeet, joista käyttäjä saa tarvitsemansa tiedon järjestelmien ja niissä olevien tietojen oikeanlaisesta käytöstä. Kaikille käyttäjille järjestetään riittävä määrä tietojärjestelmien käyttökoulutusta ja turvakoulutusta. Turvallisuuteen liittyen käytössä on useita määräyksiä ja ohjeita. Yleiset tietoturvaperiaatteet on julkaistu dokumentissa *tietoturvapolitiikka*.

Tietoturvallisuustyöstä ja sen lainmukaisuudesta vastaa `<toimintaa johtava elin, esimerkiksi 'keskussairaalan johtaja'>`, joka johtaa ja valvoo koko organisaation turvallisuustoimintaa ja vastaa potilasasiakirjoihin liittyvistä ohjeista, tietojenkäsittely- ja menettelytavoista toimintayksikössä. Tietoturvallisuudesta, arkaluonteisten tietojen käsittelystä ja erityisesti potilastiedoista on säädetty useassa eri laissa, joista tässä yhteydessä oleellisimmiksi voidaan katsoa laki viranomaisen toiminnan julkisuudesta (621/1999), henkilötietolaki (523/1999), laki potilaan asemasta ja oikeuksista (785/1992) ja Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001).

## Tietoturvatoiminnan tavoitteet ja periaatteet

Tietoturvalla ja tietoturvallisuudella tarkoitetaan tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Suojaaminen sisältää erilaisia hallinnollisia ja teknisiä päätöksiä, periaatteita, menettelytapoja ja toimenpiteitä, joilla varaudutaan tietoihin kohdistuviin uhkiin ja estetään riskien toteutuminen tai vähennetään niiden vaikutuksia. Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien tietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton, esimerkiksi järjestelmän vikaantuminen, tapaturma tai luonnonkatastrofi.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jonka päämääränä on turvata <organisaation nimi> toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen oikeanlainen ja keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille, estää niiden valtuudeton käyttö, tahaton tai tahallinen tietojen tuhoutuminen tai vääristyminen sekä vähentää tietoturvariskejä ja minimoida niistä aiheutuvat vahingot.

Tietosuoja on oleellinen osa tietoturvallisuutta. Sillä tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista. Lainsäädäntö suojaa henkilötietoja usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Tietosuojalainsäädännössä säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa liittyen.

Terveydenhuollon ammattihenkilökunnan toimintaa ohjaavat lain- ja määräysten mukaiset velvollisuudet ja oikeudet sekä näiden lisäksi ammattietiikka, johon sisältyy vastuu hyvästä toimintatavasta ja velvollisuus tietojen salassapidosta ja vaitiolosta.

## Tietojen säilytyksen ja luovutuksen periaatteet

<Organisaation nimi> voi saada haltuunsa potilasta koskevia tietoja useista lähteistä: hoitosuhteen aikana tietoja sekä saadaan potilaalta itseltään että niitä syntyy hoitotapahtuman yhteydessä. Säilytyksessä voi olla tietoja potilaan edellisistä hoitosuhteista. Niitä voi olla vastaanotettu muilta hoitoyksiköiltä tai muilta viranomaisilta. Jos tietojen suojaamiseksi näitä tietoja tarvitsee ryhmitellä erillisiksi kokonaisuuksiksi esimerkiksi säilytystä tai luovutusta varten, näin voidaan tarpeen mukaan tehdä.

Tietojen säilytyksestä on säädetty laissa, ja siitä on erikseen annettu ministeriön ohjeita. Erilaisia potilastietoja koskevat erilaiset säilytysvaatimukset. On myös erikseen säädetty, milloin vanhat tiedot täytyy poistaa. Väärien, vanhentuneiden ja virheellisten tietojen käsittely on kielletty, ja näiden oikaiseminen on tehtävä tarpeen mukaan. Tietoja voidaan luovuttaa ainoastaan potilaan nimenomaisella suostumuksella.

Edellä mainitusta huolimatta voi olla olemassa tilanteita, joissa hoitohenkilökunnalla saattaa olla tietty oikeus käsitellä potilaan tietoja ilman hänen lupaansa. Näitä tilanteita voivat olla esimerkiksi potilaan tajuttomuustila vaikeassa loukkaantumisessa, potilaan vajaakykyisyys päättää itse asiasta tai oikeusviranomaisen määräämä pakkokeino. Säilytykseen ja luovutukseen liittyvien määräysten osalta voi tarkemmin tutustua edellä mainittuihin lakeihin ja asetuksiin sekä Sosiaali- ja terveysministeriön oppaaseen terveydenhuollon henkilöstölle, oppaita 2001:3: *Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen*.

## Tietojen käsittelyn ja tietojärjestelmien turvallisuus

Tietoihin ja tietojärjestelmiin pääsy on tarkoin määritelty. Henkilöillä on tietojen saantioikeus vain silloin, kun siihen on olemassa peruste. Tällainen peruste voi olla esimerkiksi hoitosuhteen olemassaolo, jolloin hoitavalla lääkärillä voi olla pääsy henkilön tietoihin, kuitenkin vain niihin, joita hoitosuhteen aikana potilaan hoidossa tarvitaan. Tietoja saa käsitellä vain siinä käyttötarkoituksessa ja laajuudessa kuin on välttämätöntä. Tämän lisäksi myönnettävät pääsyoikeudet riippuvat potilasta hoitavan henkilön roolista: esimerkiksi sairaanhoitajalla on eritasoinen pääsy tietoihin kuin lääkärillä. Potilaan mahdollinen tietojen käyttö muualla, esimerkiksi toisessa sairaalassa, on potilaan itse päätettävissä: kaikkiin tietojen luovutuksiin tarvitaan potilaan lupa.

Tietojärjestelmiä käyttävät henkilöt tunnistetaan ja todennetaan siten, että henkilön esiintyminen toisena ei ole mahdollista. Käytössä on tarvittavat käyttäjätunnus-, salasana-, toimikortti- ja PIN-koodimenettelyt. Tietojärjestelmiä käytettäessä tietoihin pääsy voidaan estää siten, että henkilöllä ei ole edes mahdollisuutta nähdä tietoja, joihin hän ei ole oikeutettu. Tämä ei usein ole mahdollista esimerkiksi paperimuodossa olevien asiakirjojen osalta.

Käytössä olevat tietoliikenneyhteydet ovat turvallisia, ja tietoliikenne on salattua eikä salakuuntelu ole mahdollista. Käytettävät tietojärjestelmät ja ohjelmistot ovat turvallisia, ja niiltä edellytettävät turvaominaisuudet on testattu ennen käyttöönottoa. Toimitilat, joissa tietojärjestelmiä säilytetään, on fyysisesti suojattu sekä valtuudetonta pääsyä ja murtautumista että erilaisia vikatilanteita, sähkökatkoja ja tulipaloja vastaan. Kaikkia normaalista poikkeavia tapahtumia ja tilanteita valvotaan ja seurataan, ja korjaushenkilökunta hälytetään tarvittaessa ongelmanselvitystyöhön. Kaikista väärinkäytöksistä rangaistaan.

## Henkilön oikeus omiin tietoihinsa

Henkilötietolain mukaan rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee esimerkiksi rekisterinpitäjän yhteystiedot ja rekisterin suojaus, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityihin liittyvistä tiedoista ja se, mihin tietoja säännönmukaisesti luovutetaan. Rekisteriselosteen on oltava saatavilla. Sen saa pyydettäessä <paikka, esimerkiksi 'vastaanotosta tai lääkäriltä'>.

Henkilötietolain mukaan jokaisella on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Tiedot voi haluttaessa tarkastaa ottamalla yhteyden <yhteydenottopiste, esimerkiksi 'vastaanottoon tai lääkäriin'>, jossa voi täyttää tarkastuslomakkeen, jonka perusteella rekisteröidyn tiedot tarkastetaan ja annetaan tutustuttaviksi. Jos rekisterissä oleva henkilötieto on virheellinen, tarpeeton, puutteellinen tai vanhentunut, rekisterinpitäjän on oikaistava, poistettava tai täydennettävä tieto oma-aloitteisesti tai henkilön vaatimuksesta.

<Organisaation nimi> johto on sitoutunut tietoturvalliseen toimintaan ja suhtautuu vakavasti kaikkeen saamaansa palautteeseen. Kaikki palaute havaituista epäkohdista voidaan antaa vastaanottoon, jossa palautteen antamista varten on erillinen lomake. Myös verkkosivut <verkkosivun osoite, esimerkiksi 'http://www.abc.fi/palaute'> ovat käytettävissä. Jos henkilö havaitsee epäkohtia rekisteriselosteessa tai sen saatavuudessa, tietojensa tarkastamisessa, oikeellisuudessa tai mahdollisuudessa niiden korjaamiseen, tai jos hän havaitsee tai epäilee mahdollisia tietosuojaloukkauksia, hän voi saattaa asian myös tietosuojavaltuutetun käsiteltäväksi.

# Liite 6 Mallilomake työsähköpostien käsittelyyn ja lukemiseen

Alla on esitettynä mallilomake työntekijän suostumuslomakkeeksi sähköpostiviestien käsittelyyn hänen poissaolonsa ajaksi. Malli on käytettävissä sellaisenaan. Organisaatio voi lisätä lomakkeeseen tarpeelliseksi näkemiään tietoja. Asiakirja on luottamuksellinen.

On huomattava, että *laki yksityisyyden suojasta työelämässä* edellyttää työnantajalta huolellisuusvelvoitetta: työntekijälle on annettava mahdollisuus käyttää sähköpostissaan automaattista poissaoloilmoitusta tai ohjata viestit toiselle henkilölle tai toiseen osoitteeseen. Työntekijän on annettava suostumus, että toinen henkilö voi lukea hänen sähköpostinsa poissaolon, esimerkiksi sairauden tai loman aikana, tai työsuhteen loputtua.

On myös huomattava, että menettelytavat ja toimenpidejärjestys on ennalta määrätty, kun työnantaja selvittää työntekijän sähköpostista tietoja tai tiettyjen sähköpostiviestien sisällön. Sähköpostista tapahtuvan tiedonhankinnan täytyy olla välttämätöntä työnantajan toimintojen turvaamiseksi tai esimerkiksi asiakkaiden palvelemiseksi. Viesteistä on ensin selvitettävä tunnistamistiedot, jonka jälkeen työnantajalle kuuluvien viestien (erotellaan esimerkiksi vastaanottajan, lähettäjän ja otsikon perusteella) lukeminen voi tapahtua esimerkiksi järjestelmän pääkäyttäjän valtuuksilla. Lukutapahtumassa on oltava läsnä myös toinen henkilö. Tapahtumasta on laadittava pöytäkirja ja selvitys työntekijälle. Pöytäkirjaan on suositeltavaa kirjata tiedot esimerkiksi ajasta ja paikasta, toimenpiteiden kohteesta (työntekijä, jonka sähköposti avataan), läsnäolijoista, työntekijän suostumuksesta, perusteluista ja toimenpiteistä (otsikkotietojen luku, avatut viestit ja yhteydenotot eri osapuoliin). Pöytäkirja allekirjoitetaan läsnäolijoiden toimesta. Siihen voidaan myös liittää kopio avatuista viesteistä. Pöytäkirja ja avatut viestit ovat luottamuksellisia ja vaitiolovelvollisuuden piirissä.

| **Työntekijän suostumus työnantajan suorittamaan työsähköpostiviestien käsittelyyn poissaolon aikana** |
|---|
| **Työntekijän nimi** |
| **Sähköpostiosoite (tai -osoitteet)** |
| **Työnantajan nimi** |
| **Annan suostumukseni siihen, että työnantaja saa hakea, käsitellä ja lukea minulle osoitettuja tai lähettämiäni työhöni liittyviä sähköpostiviestejä yllä mainitusta sähköpostiosoitteesta.**<br><br>**Suostumus koskee seuraavia tilanteita:**<br>☐ etukäteen tiedossa oleva poissaoloni ajalla _____<br>☐ aina, kun poissaoloni (sairaus, loma, virkavapaus, muu syy) on kestänyt yhtäjaksoisesti vähintään __ päivää<br>☐ työsuhteeni päättymisen jälkeen<br><br>**Suostumus on voimassa _____ asti / toistaiseksi.**<br><br>Sähköpostiviestien haussa, käsittelyssä ja lukemisessa noudatetaan voimassa olevia lakeja ja työnantajan laatimia tietoturvallisia sähköpostin ja tietojen käsittelyn pelisääntöjä. Minulla on oikeus perua suostumukseni milloin tahansa. |
| **Paikka ja päiväys** _____<br><br>**Allekirjoitus** _____ |

Lomake 1 – suostumuslomake

# Liite 7 ISO 27799 standardiluonnoksen suosittamat pakolliset tietoturvavaatimukset terveydenhuollon organisaatioille

Standardissa *ISO 27799* määritellään pakolliset tietoturvallisuusvaatimukset, jotka terveydenhuollon organisaation on toteutettava. Standardi ei ole valmis, mutta alla on alustava luettelo näistä vaatimuksista.

a) Potilastietoja käsittelevän terveydenhuollon organisaation on laadittava ja kuvattava kriteerit tietoturvariskien hallintaan.
b) Terveydenhuollon organisaation on laadittava tietoturvapolitiikka.
c) Organisaatiossa on käytettävä salassapito- ja muita sopimusmenettelyitä, joita noudatetaan jokaisen potilastietoja käsittelevän henkilön ja kaikkien ulkopuolisten osapuolten kanssa.
d) Terveydenhuollon organisaation on arvioitava riskit, joita ulkopuolisten osapuolten toiminnasta aiheutuu potilastietojen tietoturvalle.
e) Terveydenhuollon organisaation on taattava riittävä tietoturvallisuuskoulutus potilastietoja käsitteleville henkilöille.
f) Terveydenhuollon organisaation on vastattava, että kaikki käyttövaltuudet ja pääsy tietoihin poistetaan mahdollisimman nopeasti, kun pääsyä ei enää tarvita riippumatta siitä, onko kyse organisaation omasta tai kolmannen osapuolen työntekijästä.
g) Terveydenhuollon organisaation on taattava, että yhtään potilastietojen käsittelyssä käytettävää tietojärjestelmää, laitteistoa, ohjelmistoa tai tietovälinettä ei poisteta ilman nimenomaista lupaa.
h) Käytöstä poistettavat tietojärjestelmät, laitteistot ja tietovälineet on tyhjennettävä potilastiedoista tai fyysisesti tuhottava siten, että poistettuja tietoja ei voi lukea.
i) Kaikkeen organisaation tilojen ulkopuolella tapahtuvaan potilastietojen käsittelyyn tarvitaan erikseen myönnettävä lupa.
j) Tietojärjestelmiin ja tietojenkäsittely-ympäristöihin tehtävissä muutoksissa on käytettävä etukäteen määriteltyä ja dokumentoitua muutoksenhallintaprosessia.
k) Terveydenhuollon organisaation on eriytettävä potilastietojen käsittelyyn ja säilytykseen tarkoitettujen tietojärjestelmien kehitys- ja testausympäristöt tuotannollisista ympäristöistä.
l) Terveydenhuollon organisaation on määriteltävä ja dokumentoitava säännöt ja hyväksymiskriteerit, joilla tuotannollisia ympäristöjä otetaan käyttöön, joilla niitä päivitetään uudempiin versioihin ja millaisia testaustoimia vaaditaan ennen järjestelmien hyväksymistä käyttöön.
m) Terveydenhuollon organisaation on toteutettava asianmukaiset ja sopivat kontrollit sekä riittävä käyttäjien koulutus, joiden avulla havaitaan haittaohjelmat, suojaudutaan niiltä ja voidaan ehkäistä niiden vaikutuksia.
n) Terveydenhuollon organisaation on otettava asianmukaiset varmuuskopiot potilastiedoista ja tallennettava ne siten ja fyysisesti sellaiseen paikkaan, että tiedot säilyvät ja on otettavissa käyttöön.
o) Terveydenhuollon organisaation on säilytettävä käytönseuranta- ja lokitietoja turvallisesti, hallittava ja valvottava niihin pääsyä ja estettävä niiden väärinkäyttö.
p) Terveydenhuollon organisaation on määriteltävä formaalit käyttäjien ja pääsynhallinnan periaatteet ja menetelmät niille tietojärjestelmille, joilla käsitellään potilastietoja.
q) Käyttäjien rekisteröintimenettelyissä on varmistettava, että käyttäjän todentamisen taso vastaa valtuuksien tasoa, joka käyttäjälle myönnetään.
r) Jokainen käyttäjä on todennettava henkilökohtaisesti uniikilla tunnisteella jokaisessa potilastietojen käsittelyyn tarkoitetussa tietojärjestelmässä. On suositeltavaa käyttää vahvaa todennusta.