Sosiaali- ja terveysministeriön julkaisuja 2007:19

Tietoturvallisuussuunnitelman laatiminen

Opas sosiaali- ja terveydenhuollon toimintayksiköille

SOSIAALI- JA TERVEYSMINISTERIÖ

Helsinki 2007

ISSN 1236-2050
ISBN 978-952-00-2398-0 (nid.)
ISBN 978-952-00-2399-7 (PDF)

Taitto: AT-Julkaisutoimisto Oy
Paino: Yliopistopaino, Helsinki 2007

Tiivistelmä

Tietoturvallisuussuunnitelman laatiminen. Opas sosiaali- ja terveydenhuollon toimintayksiköille. Helsinki 2007. 62 s. (Sosiaali- ja terveysministeriön julkaisuja, ISSN 1236-2050, 2006:19) ISBN 978-952-00-2398-0 (nid.), ISBN 978-952-00-2399-7 (PDF)

Tietoturvallisuutta koskevan lainsäädännön keskeinen lähtökohta on yksityisyyden suoja ja sen turvaaminen kaikissa olosuhteissa.

Tietoturvallisuus on osa toimintayksikön riskienhallintaa. Tietoturvallisuudella on keskeinen merkitys kaikissa turvallisuustilanteissa; normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa. Tietoturvallisuus mielletään usein tietojen suojaamiseksi valtuudettomalta käytöltä. Se on kuitenkin kokonaisuus, joka kattaa myös tietojen käytettävyyden ja hallinnoinnin. Sosiaali- ja terveydenhuollon julkisten ja yksityisten palvelujen antajien ja järjestäjien tulee lain mukaan huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä sekä tietojen ja aineistojen asianmukaisesta hävittämisestä. Asiakastietojen turvallinen käsittely korostuu entisestään siirryttäessä yhä enenevässä määrin asiakastietojen sähköiseen käsittelyyn.

Tietoyhteiskunnan toimintatavat ja siihen liittyvät uhat ovat maailmanlaajuisia. Tietoturvauhkien ilmenemismuoto, lähde ja kohde ovat riippumattomia sijaintimaasta. Uhka toteutuu kuitenkin paikallisena, joten kansainvälisiä uhkia vastaan tarvitaan kansallisia toimenpiteitä. Verkostoituminen lisää saatavilla olevan tiedon määrää sekä nopeuttaa päätöksentekoa. Ongelmia syntyy usein siitä, että kaikilla käyttäjillä ei ole verkostoitumisen edellyttämiä tietoja ja taitoja. Verkostot ovat enenevästi palveluverkostoja, ja uhkia tietoturvallisuudelle syntyy tietojen siirrosta toimintayksiköiden välillä sekä toimintayksiköiden ja toimijoiden käyttöoikeuksista toistensa järjestelmiin.

Tietoturvallisuuden keskeiset periaatteet ovat käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuuden hallinnointia ja käytännön toimenpiteitä varten tietoturvallisuussuunnittelu ja menettelytavat on ryhmitelty yleisesti seuraaviin kokonaisuuksiin: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä laitteistoturvallisuus.

Hallinnollinen tietoturvallisuus on osa toimintayksikön tietoturvallisuuspolitiikkaa, jossa on määritelty tietoturvallisuuden hallintajärjestelmä oikeuksineen ja vastuineen. Tietoturvallisuuspolitiikasta päättää ja vastaa toimintayksikön ylin johto. Tietoturvallisuuspolitiikan avulla johto määrittelee toimintayksikön tietoturvallisuuden periaatteet ja toimintatavat, ja sen perusteella

jaetaan vastuut tietoturvallisuuden jokaisen osa-alueen käytännön suunnittelua ja työtä varten.

Tämä opas on tarkoitettu sosiaali- ja terveydenhuollon toimintayksiköille edistämään niiden tietoturvallisuussuunnittelua. Kohderyhmänä ovat erityisesti sellaiset sosiaali- ja terveydenhuollon toimintayksiköt, joilla ei ole omaa tietohallinto- tai tietoturvallisuushenkilöstöä. Oppaassa käsitellään tietoturvallisuutta osa-alueittain mahdollisimman käytännönläheisesti sekä kuvataan tietoturvallisuuden keskeisiä käsitteitä. Sisällysluettelo on laadittu siten, että sitä voidaan käyttää apuna laadittaessa toimintayksikön tietoturvallisuussuunnitelmaa.

Oppaan on laatinut sosiaali- ja terveysministeriön valmiusyksikön aloitteesta ministeriön yhteydessä toimivan poikkeusolojen terveydenhuollon neuvottelukunnan turvallisuusjaoston asettama työryhmä.

Asiasanat

asiakirjat, poikkeusolot, riskit, riskienhallinta, tietohallinto, tietoturva

Sammandrag

Utarbetande av en informationssäkerhetsplan. Handbok för verksamhetsenheter inom social- och hälsovården. Helsingfors 2007. 62 s. (Social- och hälsovårdsministeriets publikationer, ISSN 1236-2050, 2007:19)
ISBN 978-952-00-2398-0 (inh.) ISBN 978-952-00-2399-7 (PDF)

Den centrala utgångspunkten i lagstiftning som gäller informationssäkerhet är att säkerställa personlig integritet under alla omständigheter.

Informationssäkerhet är en del av verksamhetsenhetens riskhantering. Informationssäkerheten har en central betydelse i samtliga säkerhetssituationer; under normala förhållanden, i störningssituationer under normala förhållanden och i undantagsförhållanden. Informationssäkerhet uppfattas ofta som skydd av information från obehörig användning. Den utgör dock en helhet som även täcker användbarhet och administration av uppgifterna. Tillhandahållare av offentliga och privata tjänster inom social- och hälsovården skall enligt lagen sörja för adekvat tillgång, användbarhet, skydd och integritet i fråga om handlingar och informationssystem och uppgifter som ingår i dessa samt för ändamålsenlig förstöring av uppgifter och material. En säker behandling av klientuppgifter accentueras ytterligare vid övergång till elektronisk behandling av klientuppgifter i tilltagande utsträckning.

Informationssamhällets sätt att verka och hot som hänför sig till detta är globala. Uttrycksform, källa och mål för informationssäkerhetshoten är oberoende av etableringslandet. Hotet förverkligas dock lokalt så det krävs nationella åtgärder mot internationella hot. Nätverksbildning ökar den tillgängliga informationen och påskyndar beslutsfattandet. Problem uppstår ofta till följd av att alla användare inte har de kunskaper och färdigheter som nätverksbildningen förutsätter. Nätverken är allt oftare servicenätverk och hot mot informationssäkerheten uppstår när uppgifter förflyttas mellan verksamhetsenheterna och på grund av verksamhetsenheters och aktörers rätt att använda varandras system.

Viktiga principer för informationssäkerheten är användbarhet, integritet och konfidentiell natur. För administration och praktiska åtgärder har informationssäkerhetsplaneringen och tillvägagångssätten indelats i följande helheter: administrativ säkerhet, personalsäkerhet, fysisk säkerhet, datakommunikationssäkerhet, driftssäkerhet, programsäkerhet, informationsmaterialsäkerhet och utrustningssäkerhet.

Administrativ informationssäkerhet är en del av verksamhetsenhetens informationssäkerhetspolitik där man har fastställt det administrativa systemet för informationssäkerheten med dess rättigheter och ansvar. Verksamhetsenhe-

tens högsta ledning beslutar och ansvarar för informationssäkerhetspolitiken. Med hjälp av informationssäkerhetspolitiken fastställer ledningen verksamhetsenhetens principer och tillvägagångssätt för informationssäkerheten och på grundval av detta fördelas ansvaret för den praktiska planeringen och arbetet inom varje område av informationssäkerheten.

Denna handbok är avsedd för verksamhetsenheterna inom social- och hälsovården för att främja deras informationssäkerhetsplanering. Målgruppen är särskilt sådana verksamhetsenheter inom social- och hälsovården som inte har egen personal för informationsadministration eller informationssäkerhet. Handboken tar upp informationssäkerhet delområdesvis så konkret som möjligt och beskriver viktiga begrepp inom informationssäkerhet. Innehållsförteckningen har utarbetats så att den kan användas som hjälp vid upprättande av verksamhetsenhetens informationssäkerhetsplan.

Handboken har på initiativ av beredskapsenheten vid social- och hälsovårdsministeriet utarbetats av en arbetsgrupp som tillsatts av säkerhetssektionen vid delegationen för hälso- och sjukvården under undantagsförhållanden i anslutning till ministeriet.

Nyckelord

handlingar, informationsadministration, informationssäkerhet, risker, riskhantering, undantagsförhållanden

Summary

Preparation of an Information Security Plan. A handbook for social and health care units. Helsinki, 2007. 62pp. (Publications of the Ministry of Social Affairs and Health, Finland, ISSN 1236-2050, 2007:19)
ISBN 978-952-00-2398-0 (pb) ISBN ISBN 978-952-00-2399-7 (PDF)

An important starting point for the legislation on information security is privacy protection and the necessity of ensuring it under all circumstances.

Information security is part of the social and health care units' risk management. It is of major importance in all security situations: in normal conditions and incidences under them, and in emergency conditions. Information security is often understood as protection of information from unauthorised use. It is, however, an entirety that also covers the accessibility and management of information. Public and private social and health service providers shall according to the law see to the adequate availability, accessibility, protection and integrity of the documents and information systems and the data included in them, as well as that the data and material are destroyed appropriately. The importance of secure processing of client data is further emphasised with the increasing electronic processing of information concerning clients.

The ways how an information society functions and related threats are global. The manifestation, source and object of data security risks do not depend on the country of location. A threat however materialises locally, and therefore national measures are needed to respond to international threats. Networking increases the amount of information available and accelerates decision-making. Problems often arise out of the fact that all users do not have the knowledge and skills required for networking. Networks are increasingly service networks, and threats to information security arise in the context of transfer of information between units and in relation to the units' and actors' rights to use each other's systems.

The central principles of information security are accessibility, integrity and confidentiality. For the management of information security and practical measures the information security planning and procedures are generally grouped as follows: administrative and organisational security, personnel security, physical security, telecommunications security, operations security, software security, data security, and facilities security.

Administrative and organisational information security is a part of the unit's information security policy, which determines the system of management of information security with related rights and responsibilities. The top management of the unit decides and is in charge of the information security policy.

The management determines by means of the information security policy the principles and methods of information security, and the responsibilities for the practical planning and work in each sub-area are divided based on that.

The present handbook is intended for social and health care units to promote their information security planning. The target group is in particular those social and health care units that have not an information management or information security personnel of their own. The handbook deals with information security by sub-area as concretely as possible and describes the most important concepts of information security. The table of contents has been drawn up so that it can be made use of when drawing up the information security plan for the unit.

The handbook has been prepared by a working group set up by the security section under the Advisory Board for Health and Welfare in Emergency Conditions on the initiative of the Preparedness Unit of the Ministry of Social Affairs and Health.

Key words

documents, emergency conditions, information management, information security, risk management, risks

Sisällys

Esipuhe

Tietoturvallisuussuunnitelma on osa toimintayksikön riskienhallintaa. Tämä opas on tarkoitettu sosiaali- ja terveydenhuollon toimintayksiköille edistämään niiden tietoturvallisuussuunnittelua. Kohderyhmänä ovat erityisesti sellaiset sosiaali- ja terveydenhuollon toimintayksiköt, joilla ei ole omaa tietohallinto- tai tietoturvallisuushenkilöstöä. Oppaassa käsitellään tietoturvallisuutta osa-alueittain mahdollisimman käytännönläheisesti sekä kuvataan tietoturvallisuuden keskeisiä käsitteitä. Sisällysluettelo on laadittu siten, että sitä voidaan käyttää apuna laadittaessa toimintayksikön tietoturvallisuussuunnitelmaa.

Tietoturvallisuudella on keskeinen merkitys kaikissa turvallisuustilanteissa; normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa. Tietoturvallisuus mielletään usein tietojen suojaamiseksi valtuudettomalta käytöltä. Se on kuitenkin kokonaisuus, joka kattaa myös tietojen käytettävyyden ja hallinnoinnin. Tietotekniikan luotettavuus-, toimintavarmuus- ja käytettävyysvaatimukset ovat tehneet tietoturvallisuudesta huolehtimisen välttämättömäksi.

Julkisuuslain mukaan viranomaisten on huolehdittava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä sekä tietojen ja aineistojen asianmukaisesta hävittämisestä.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä säädetyn lain tarkoituksena on edistää asiakastietojen tietoturvallista käsittelyä. Lakia sovelletaan julkisten ja yksityisten palvelujen antajiin ja järjestäjiin. Oppaassa on otettu huomioon lain velvoitteet tietoturvallisuussuunnittelulle.

Tietoturvallisuuden kehittämistä ja toimintojen ohjausta varten valtiovarainministeriön kehittämisosasto julkaisee VAHTI-ohjeistoa, jota voidaan soveltuvin osin käyttää myös kunnallisten tai yksityisten toimijoiden tietoturvallisuuden kehittämis- ja ylläpitotehtävissä.

Oppaan on laatinut sosiaali- ja terveysministeriön valmiusyksikön aloitteesta ministeriön yhteydessä toimivan poikkeusolojen terveydenhuollon neuvottelukunnan turvallisuusjaoston asettama työryhmä.

1 Tietoturvallisuus, sen lainsäädännöllinen perusta ja käsitteet

Tietoturvallisuutta koskevan lainsäädännön keskeinen lähtökohta on yksityisyyden suoja ja sen turvaaminen kaikissa olosuhteissa. Tähän liittyen on säädetty tietojen salassapidosta ja arkistoimisjärjestelyistä, valtuudettoman käytön estämisestä sekä viestinnän turvaamisesta.

Yhteiskunnassa, jonka toiminta perustuu tuotantotoimintaan ja sen kilpailukykyyn, henkilöiden, organisaatioiden ja toimintayksiköiden laissa säädetyt sekä muutoin luottamukselliset ja salassa pidettävät tiedot on turvattava valtuudettomalta käytöltä. Riskienhallintaan olennaisena ja erottamattomana osana kuuluu tiedon luokittelu ja sen arvon määrittely yksilön tai yhteisön näkökulmasta.

Yksityisyyden suoja on turvattu perustuslaissa. Tietosuojan perusta on henkilötietolaki. Sosiaali- ja terveydenhuollon lainsäädännössä on määritelty toimintaa koskevat tietosuoja- ja salassapitomenettelyt. Ohjelmistoja ja tietosisältöjä suojaa puolestaan tekijänoikeuslaki. Rikoslaissa on säädetty tietoturvallisuusrikkomuksista.

Laissa viranomaisten toiminnan julkisuudesta (621/1999, JulkL) ja sen 24 §:ssä on säädetty asiakirjoista, jotka on pidettävä salassa. Olennaista kyseisiä asiakirjoja luotaessa, muutettaessa, siirrettäessä, arkistoitaessa, hävitettäessä ja muutoin käsiteltäessä on, että salassa pidettävien asiakirjojen käsittely on turvaluokkien mukaan yhdenmukaista kaikkien kyseisiä tietoja ja asiakirjoja käsittelevien osalta. Asiakirja on turvaluokiteltava silloin, kun se on JulkL (julkisuuslaki) 24.1 §:n 1, 2,5,7,8,9 10 tai 11 -kohtien mukaan salassa pidettävä. Tällaiset asiakirjat käsittelevät yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi arkaluonteista ja salassa pidettävää tietoa.

Julkisuuslain soveltamisalan ulkopuolelle jääviä ovat mm. virkamiehen laatimat muistiinpanot ja sisäistä koulutusta varten hankitut asiakirjat sekä virkamiehen saamat yksityiskirjeet.

Tietoturvallisuutta koskeva keskeinen lainsäädäntö on esitetty liitteessä 1.

Valtiovarainministeriön hallinnon kehittämisosasto on antanut 19.1.2000 ohjeen salassa pidettävien tietojen ja asiakirjojen turvaluokittelusta ja merkinnästä (VM 5/01/2000).

Tietoturvallisuuden keskeiset periaatteet ovat käytettävyys, eheys ja luottamuksellisuus.

Käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla aina, kun sitä tarvitaan etukäteen määritellyssä vasteajassa. Käytettävyyteen vaikuttavat laitteet ja ohjelmistot, joilla tietoa käsitellään.

Eheys tarkoittaa tiedon muuttumattomuutta tietoja käsiteltäessä, välitettäessä paikasta toiseen tai arkistoinnin aikana.

Luottamuksellisuus tarkoittaa, että valtuudettomille ei anneta mahdollisuutta nähdä, muuttaa, tuhota tai muutoin käsitellä asiakirjaa tai tietoa.

Sähköisen asioinnin yleistyessä on tietoturvallisuuskäsitteistöön otettu lisäksi määritelmä ***kiistämättömyys***. Tämä tarkoittaa tiedon ominaisuutta ja menetelmää, joilla järjestelmän käyttäjä tunnistetaan, ja varmennetaan siten tiedon oikeellisuus sekä tapahtuman oikeudellinen sitovuus.

Tietoturvallisuudella tarkoitetaan tietojen suojaamista valtuudettomalta käytöltä, muuttumiselta ja tuhoutumiselta. Tietoturvallisuuteen kuuluu myös tietojen käytettävyyden varmistaminen. Tämä tarkoittaa tietojen ja sähköisten palvelujen, yksittäisten tietojärjestelmien sekä tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi hallinnollisin ja teknisin toimenpitein.

Tietoturvallisuus jaotellaan seuraavasti:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- käyttöturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- laitteistoturvallisuus.

Hallinnollinen turvallisuus: toiminnan järjestelyt, henkilöstön tehtävät sekä ohjeistus, vastuut, koulutus ja valvonta.

Henkilöstöturvallisuus: henkilöstön luotettavuus ja soveltuvuus, oikeuksien hallinta, sijaisjärjestelyt ja työsuhteen järjestelyt.

Fyysinen turvallisuus: tietotekniikan käyttöympäristö, kiinteistön rakenteellinen turvallisuus, valvontatekniikka, valvonta ja vartiointi sekä henkilöstön suojaaminen.

Tietoliikenneturvallisuus: tiedonsiirtoyhteyksien käytettävyys, tiedonsiirron suojaus ja salaus, käyttäjien tunnistus ja verkon varmistaminen.

Käyttöturvallisuus: turvallisen käytön toimintaolosuhteet, tekniikan toimivuuden valvonta, käyttöoikeudet, käytön ja lokien valvonta, ohjelmistotuen, ylläpidon ja huollon turvallisuustoimenpiteet, varmuus- ja suojakopiointi sekä häiriöraportointi.

Ohjelmistoturvallisuus: käyttöjärjestelmien, varus- ja hyötyohjelmistojen sekä muiden ohjelmistojen ja sovellusten suojausominaisuudet, valvonta- ja lokimenettelyt sekä ohjelmistojen ylläpidon ja päivityksen turvallisuustoimenpiteet.

Tietoaineistoturvallisuus: tietojen ja tietoaineistojen käytettävyys, oikeellisuus sekä salassapito elinkaaren kaikissa vaiheissa.

Laitteistoturvallisuus: laitteistojen käytettävyys, toiminta, ylläpito sekä laitteistojen ja tarvikkeiden saatavuus ja käytöstä poistaminen.

2 Tietoturvan uhat

Tietoturvaongelmia aiheutuu

- internetin käyttämisestä ilman ajantasaista virustorjuntaa
- langattomien verkkojen käyttämisestä ilman salausta
- ohjelmistotuen saatavuusongelmista
- käyttöympäristön turvattomuudesta
- pääsyoikeuksien ja käyttövaltuuksien puutteellisesta hallinnasta ja valvonnasta
- tietojenkäsittelylaitteistojen ja käyttöjärjestelmien ongelmista
- tahallisista ja tahattomista virheistä tai rikkomuksista
- perehdytyksen ja koulutuksen puutteista
- puutteellisista haittaohjelmien ja virusten torjuntajärjestelmistä.

Tietoyhteiskunnan toimintatavat ja siihen liittyvät uhat ovat maailmanlaajuisia. Tietoturvauhkien ilmenemismuoto, lähde ja kohde ovat riippumattomia sijaintimaasta. Uhka toteutuu kuitenkin paikallisena, joten kansainvälisiä uhkia vastaan tarvitaan kansallisia toimenpiteitä. Verkostoituminen lisää saatavilla olevan tiedon määrää sekä nopeuttaa päätöksentekoa. Ongelmia syntyy usein siitä, että kaikilla käyttäjillä ei ole verkostoitumisen edellyttämiä tietoja ja taitoja. Myöskään verkossa liikkuvan tiedon arvoa tai oikeellisuutta ei aina voi mitata. Verkostot ovat enenevästi palveluverkostoja, ja uhkia tietoturvallisuudelle syntyy tietojen siirrosta toimintayksiköiden välillä sekä toimintayksiköiden käyttöoikeuksista toistensa järjestelmiin. Oikeuksien hallinta on nopeatempoista ja tilannekohtaista. Eri osapuolten tietoturvallisuustaso saattaa poiketa toisistaan merkittävästi, eikä erojen selvittäminen ole aina ongelmatonta. Vastuunjakoon on tietoturvallisuuden takaamiseksi kiinnitettävä tällaisessa yhteistyössä erityistä huomiota. Verkostoituminen luo toisaalta myös edellytykset tietoturvallisuuden parantamiselle siten, että tieto hyväksi havaituista toimintatavoista leviää nopeasti.

Todennäköisimmät tietoturvauhat ja niistä aiheutuvat riskit ovat käyttäjälähtöisiä. Tietoturvaongelmat voivat syntyä tahattomasti tai tahallisesti. Käyttäjät voivat toimia varsin itsenäisesti ja sivuuttaa toimintayksikön tarjoamat tietoturvallisuuden hallinnolliset ja tekniset ratkaisut. Tietoturvallisuudesta ei pidä tinkiä taloudellisuuden kustannuksella.

Sähköpostin tai internetin hallitsematon käyttö saattaa aiheuttaa ongelmia yksittäiselle työasemalle tai toimintayksikön palvelimelle käyttäjän avatessa va-

hingossa haittaohjelman sisältävän tiedoston. Käytettävästä tietojärjestelmästä riippuen haittoja voidaan torjua työasemakohtaisella virusten ja haittaohjelmien torjuntaohjelmistolla, palvelinkohtaisella torjuntaohjelmistolla tai koko järjestelmää koskevalla palomuurilaitteistolla ja ohjelmistolla.

Merkittävä liikkuvuuden mukanaan tuoma uhka on luvaton pääsy laitteisiin tallennettuun tietoon ja niissä oleviin ohjelmiin. Tietojenkäsittely- ja viestintälaitteita käytetään paljon toimintayksikön ulkopuolella. Tyypillisimpiä näistä ovat salkkutietokoneet (laptop), puhelimet, kommunikaattorit ja kämmentietokoneet (PDA-laite) sekä muistitikut. Tietojenkäsittelylaitteistoja, mm. palvelimia, saattaa olla ulkopuolisen palveluntuottajan omissa toimitiloissa. Laitteen katoamisesta voi aiheutua tiedon joutuminen valtuudettomaan käyttöön.

Käyttäjän toiminta saattaa teknologian kehittyessä aiheuttaa tietoturvariskejä. Tämä johtuu siitä, että ohjelmistojen ja laitteiden käyttö on vaikeaselkoista. Ongelmaa voidaan vähentää perehdytyksellä ja koulutuksella.

Muita uhkatekijöitä ovat ohjelmistotuen puutteet ja laitteistoviat. Myös fyysisen ympäristön ongelmat, kuten sähkökatkot, tulipalot ja vesivahingot on otettava riskitarkasteluissa huomioon.

Tietoturvauhkia syntyy silloin, kun käyttäjä ei tunne laitteistonsa käyttömenetelmää, käyttöjärjestelmän toimintaa, ohjelmaa tai ohjelmistoa, jolloin mahdolliset virhetoiminnot lisäävät riskien todennäköisyyttä.

Tietoturvauhkia syntyy myös, kun käyttäjä työskentelee ympäristössä, jossa valtuudettomat henkilöt pääsevät esimerkiksi esteettä näkemään tietokoneen näytöllä olevia tietoja. Myös tulostin tai faksilaite on sijoitettava siten, etteivät sivulliset pääse käsiksi tulostettavaan salassa pidettävään aineistoon.

Vaikka yhä suurempaa osaa tietosuojan alaisesta aineistosta käsitellään sähköisessä muodossa, osaa tiedoista tullaan edelleen käsittelemään paperimuodossa tai puhuttuna. Tällöin on tärkeää tiedostaa kunkin oma vastuu salassa pidettävän tiedon käsittelystä kulloisessakin käyttöympäristössä sekä lain vaatimukset menettelytavoista.

3 Tietoturvallisuus-suunnitelman laadinta

Tietoturvallisuussuunnitelma sisältää toimintayksikön tietoturvallisuuden hallinnon järjestelyt, tietojen käsittelymenetelmät ja käytön valvontamenettelyt, laitteistojen ja järjestelmien hankintojen tietoturvallisuusnäkökohdat, toiminnan jatkuvuuden varmistamisen sekä tietoturvallisuussuunnitelman ylläpidon.

Tietoturvallisuussuunnitelmassa toimintayksikkö määrittelee käsittelemänsä tiedon luottamuksellisuuden, tiedon käsittelytavat ja käyttöoikeudet, arkistoinnin, tiedon hävittämisen sekä menettelytavat normaaliolojen häiriötilanteissa ja valmiuslain tarkoittamissa poikkeusoloissa.

Suunnitelman yhteydessä laaditaan kuvaus tiedon käsittelyn prosesseista, arvioidaan riskit ja kuvataan toimenpiteet riskien poistamiseksi, pienentämiseksi tai sietämiseksi. Tätä kuvausta käytetään hyväksi suunnitelman laadinnassa sekä siihen perustuvan toimenpide- ja investointiohjelman valmistelussa.

Tietoturvallisuussuunnitelmaan tulee sisällyttää myös kuvaus henkilöstön koulutuksesta.

Tietoturvallisuussuunnitelman jatkuvuussuunnitelmassa (valmiussuunnitelma) kuvataan toimintayksikön toimenpiteet tilanteissa, jolloin tietojen käsittely normaalein menettelytavoin on estynyt esimerkiksi sähkön saannin estyttyä tai laitevian ilmaantuessa, jolloin tietoa ei voida käsitellä tavanomaisin menetelmin. Toimintayksikön tulee näitä tilanteita varten arvioida tiedon käsittelyn tärkeysjärjestys sekä menettelytavat tiedon tallentamiseksi ja palauttamiseksi ongelmatilanteen palauduttua normaaliksi.

Tietoturvallisuussuunnitelmassa tulee määritellä menettelytavat ja nimetä vastuuhenkilöt tietoturvarikkomustilanteita varten.

Tietoturvallisuussuunnitelman ylläpitoa ja tietoturvallisuuden valvontaa varten toimintayksikössä tulee olla nimetyt vastuuhenkilöt.

Tietoturvallisuussuunnitelmarunko on esitetty seuraavassa:

TIETOTURVALLISUUSSUUNNITELMAN SISÄLTÖRAKENNE

1 HALLINNOLLINEN TIETOTURVALLISUUS
- 1.1 Tietoturvallisuuden hallinnan järjestäminen
  - 1.1.1 Tietoturvallisuuspolitiikka
  - 1.1.2 Tietoturvallisuuden organisaatio
  - 1.2.3 Tietoturvallisuuden koordinointi ja vastuiden jako
- 1.2 Tietoturvallisuuteen liittyvät suunnitelmat
- 1.3 Yhteistoiminta ulkopuolisten kanssa

2 HENKILÖSTÖTURVALLISUUS
- 2.1 Avainhenkilöriippuvuus
- 2.2 Henkilöstön työhönotto
- 2.3 Henkilöstön luotettavuus ja sitoumukset
- 2.4 Henkilöstön koulutus
- 2.5 Ulkopuoliset työntekijät ja ostopalvelut
- 2.6 Työsuhteen päättymismenettely

3 FYYSINEN TIETOTURVALLISUUS
- 3.1 Rakenteellinen suojaaminen ja valvonta
- 3.2 Lukitukset ja kulunvalvonta
- 3.3 Palontorjunta

4 TIETOLIIKENNETURVALLISUUS
- 4.1 Verkon turvallisuus
- 4.2 Energiansaannin turvaaminen
- 4.3 Sähköposti

5 KÄYTTÖTURVALLISUUS
- 5.1 Käyttöympäristön hallinta
- 5.2 Käyttöoikeus- ja valtuushallinta
- 5.3 Matkatyö, etätyö ja etäkäyttö
- 5.4 Haittaohjelmistojen ja -koodien torjunta
- 5.5 Tietotekninen valvonta
- 5.6 Jatkuvuussuunnittelu
- 5.7 Tietoturvallisuus poikkeusoloissa

6 OHJELMISTOTURVALLISUUS
- 6.1 Ohjelmistoturvallisuuden tavoitteet
- 6.2 Elinkaarimalli
- 6.3 Salausohjelmat

4 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus on osa toimintayksikön tietoturvallisuuspolitiikkaa, jossa on määritelty tietoturvallisuuden hallintajärjestelmä oikeuksineen ja vastuineen.

Tietoturvallisuuspolitiikasta päättää ja vastaa toimintayksikön ylin johto. Tietoturvallisuuspolitiikan avulla johto määrittelee toimintayksikön tietoturvallisuuden periaatteet ja toimintatavat. Tietoturvallisuuspolitiikassa määritellään:

- tietoturvallisuuden tarkoitus ja tavoitteet
- toimintayksikössä noudatettavat tietoturvallisuusperiaatteet
- käytettävien teknisten järjestelmien tietoturvallisuusperiaatteet
- tietoturvallisuuden hallintajärjestelmä
- tietoturvallisuusvastuut
- tietoturvallisuuden toteutustapa
- ohjeet
- koulutus
- seurannan järjestäminen
- ulkoistettujen palvelujen tietoturvallisuuden periaatteet
- tietoturvallisuusrikkomusten seurausvaikutukset
- tiedottaminen.

4.1 Tietoturvallisuuden hallinnan järjestäminen

Tietoturvallisuus on kiinteä ja olennainen osa toimintayksikön arvomaailmaa, johtamista ja riskienhallintaa. Tämän vuoksi tietoturvallisuuden hallinnointia ei tule ulkoistaa.

Kaikilla työntekijöillä on vastuu tietoturvallisuudesta omien työtehtäviensä osalta. Työnantajan velvollisuutena on huolehtia siitä, että työntekijä saa tarvittavan opastuksen ja koulutuksen tehtäviinsä sekä tarvitsemiinsa käyttöliittymiin, -järjestelmiin ja -ohjelmiin.

Tietoturvallisuuden toteuttamiseksi tulee määritellä vastuut henkilöille, joilla on siihen riittävä osaaminen ja käytännön mahdollisuus. Toimintayksiköllä tulisi olla joko vakinainen tai oman toimen ohella toimiva tietoturvallisuuspääl-

likkö sekä yksikön laajuudesta ja hallintomallista riippuen vastuualuekohtaisia tietoturvallisuusvastaavia. Tärkeää on huolehtia siitä, ettei teknisen tietoturvan ja tietoturvallisuuden hallinnon tehtäviä anneta samoille henkilöille.

Tietoturvallisuusuhkien ja riskien minimoimiseksi henkilöstö tulee sitouttaa toimintayksikön tietoturvallisuuskulttuuriin ja käytännön toimenpiteisiin. Tämä edellyttää henkilöstön perehdyttämistä toimintayksikön tietoturvallisuusohjeisiin. Malli käyttäjän tietoturvallisuusohjeesta sekä siihen liittyvästä sitoumuslomakkeesta on esitetty liitteissä 2 ja 3.

Tietoturvallisuuden yleisen kehittämisen ja seurannan vastuiden lisäksi tulee antaa vastuut myös käyttöjärjestelmistä, ohjelmista ja ohjelmistoista sekä laitteista ja laitteistoista. Vastuun jakaminen tässä tarkoittaa sitä, että jokaisella järjestelmäkokonaisuudella tai laitteistokokonaisuudella on nimetty ns. omistaja. Omistajan tehtävänä on vastata kyseisten järjestelmien, ohjelmistojen tai laitteistokokonaisuuksien toiminnasta ja tietoturvallisuusominaisuuksien ylläpidosta yhdessä toimintayksikön muiden asiantuntijoiden kanssa.

4.2 Tietoturvallisuuteen liittyvät suunnitelmat

Keskeisin tietoturvallisuuteen liittyvä suunnitelma on toimintayksikön tietoturvallisuussuunnitelma. Tarpeen mukaan laaditaan toimintayksikölle elpymissuunnitelma, jota kutsutaan myös toipumissuunnitelmaksi tai valmiussuunnitelmaksi. Elpymissuunnitelma on toimintayksikön menettelytapaohje tilanteissa, joissa tietojärjestelmä on joko suunnitellusti tai jonkin yllättävän ja ennalta arvaamattoman ongelman takia pois käytöstä. Siinä määritellään järjestelmän käyttökatkon aikainen tietojenkäsittelymenettely ja vastuuhenkilöt. Lisäksi siinä annetaan ohjeet ongelmatilanteen ja käyttökatkon päättymisen jälkeisestä tietojärjestelmän käyttöönotosta.

Muita tietoturvallisuuteen liittyviä suunnitelmia voivat olla mm. tietoturvallisuuden hallintaan, käyttöön ja tietojärjestelmiin liittyvä ulkoinen arviointisuunnitelma sekä koulutussuunnitelma.

4.3 Yhteistoiminta ulkopuolisten kanssa

Toimintayksiköllä tulee olla hyväksytyt ohjeet menettelystä ulkopuolisten palveluntarjoajien kanssa. Toimintoja ulkoistettaessa tulee varmistua siitä, että palvelun tarjoaja on selvillä palvelujen kohteena olevan toimintayksikön tietoturvallisuuspolitiikasta sekä tietoturvallisuuskäytännöistä. Palvelua ostavan toimintayksikön tulee myös varmistua siitä, että palvelua tarjoavalla yrityksellä on olemassa omat päivitetyt tietoturvallisuusohjeet.

Toimintayksikön kanssa sopimussuhteessa olevat ulkopuoliset henkilöt tai sopimussuhteessa olevien yritysten henkilöt tulee sitouttaa toimintayksikön tietoturvallisuuskäytäntöihin samalla tavoin kuin toimintayksikön omakin henkilöstö. Tällä varmistetaan, ettei salassa pidettäviä tietoja joudu valtuudettomien ulkopuolisten käsiin.

Yhteistoiminnan pelisääntöihin kuuluu myös ns. ”sosiaalisen hakkeroinnin” estäminen. Tämä tarkoittaa, että toimintayksikön henkilöiden tulee toimia niin työpaikalla kuin sen ulkopuolellakin siten, että työyhteisölle arvokkaat ja salassa pidettävät tiedot eivät joudu miltään osin valtuudettomasti ulkopuolisten tietoon.

Tietoturvallisuuden käytännön menettelytavoista ja tietojen suojauksesta sekä salauksesta annetut ohjeet luovat perustan tietoturvallisuuskulttuurin kehittämiselle ja ylläpitämiselle. Vastuu ohjeistuksesta ja siitä tiedottamisesta kuuluu toimintayksikön ylimmälle johdolle.

5 Henkilöstöturvallisuus

Henkilöstöturvallisuuden toimenpiteet kohdistuvat henkilöstöön liittyvien riskien hallintaan. Avainhenkilöriippuvuus, henkilöstön luotettavuus, työhönottomenetelmät, henkilöstön koulutus ja menettelytavat ulkopuolisten työntekijöiden osalta ovat keskeisiä pohdinnan kohteita.

Henkilöstöturvallisuuden tavoitteena on vähentää suojattaviin aineistoihin kohdistuvia henkilöiden aiheuttamien virheiden riskiä sekä varkaus-, petos- ja väärinkäytösriskejä.

Henkilöstöturvallisuudella vaikutetaan toimintayksikön keskeisten arvojen säilymiseen ja ylläpitoon. Jo henkilöstön rekrytointivaiheessa tulee kiinnittää huomiota henkilöstön soveltuvuuteen tehtäviinsä. Henkilöstön toimenkuvista ja tehtävistä päätettäessä tulee ottaa huomioon sijaisjärjestelyt, tiedonsaantioikeudet, käyttöoikeudet, suojaamismenettelyt sekä turvallisuuskoulutuksen ja valvonnan järjestelyt.

Tyypillisiä henkilöstöturvallisuuteen liittyviä uhkia ovat:

- puutteelliset toimintatavat
  - tietoturvaohjeistuksen, säännöistä tiedottamisen, valvonnan sekä koulutuksen puutteet
- tahattomat teot
  - käyttövirheet
  - operointivirheet
  - virusten tahaton levittäminen
  - henkilöstön ylikuormittuminen
  - ylläpitovirheet
  - huoltotoimenpiteiden ongelmat
- tahalliset teot
  - tiedon tuhoaminen
  - tietokantoihin tunkeutuminen
  - tietojen anastus
  - tiedon muuttaminen
  - tietoverkon salakuuntelu ja -katselu
  - toisten käyttöoikeuksilla toimiminen
- ylivoimainen este
  - avainhenkilön menetys.

5.1 Avainhenkilöriippuvuus

Avainhenkilöriippuvuus tarkoittaa sitä, että toimintayksikön eri tasoilla on sellaisia työntekijöitä, joiden tietotaito on ratkaisevan tärkeää toimintayksikön toiminnan ylläpitämiselle ja tuloksen tekemiselle. Avainhenkilön tai useiden avainhenkilöiden äkillinen tai yhtäaikainen poissaolo tai poistuminen työyhteisön piiristä joko pitkäksi ajaksi tai pysyvästi saattaa aiheuttaa toimintayksikölle suuria kustannuksia, jos vastaava palvelu tai osaaminen joudutaan hankkimaan toimintayksikön ulkopuolelta. On tärkeää, että avainhenkilöille on määrätty varahenkilöt, joilla on riittävät toimivaltuudet.

Avainhenkilöiden tehtäväkentän laajuus ja ainutkertaisuus tulee arvioida riskienhallinnan menetelmin. Erityisesti tulee ottaa huomioon avainhenkilöiden poissaolon vaikutukset toimintayksikön elintärkeiden ja jatkuvuuden kannalta keskeisten sekä taloudellisesti merkittävien toimintojen mahdollisten keskeytysten seurauksiin.

5.2 Henkilöstön työhönotto

Toimintayksikköön palkattavan henkilön luotettavuuden arviointiin on kiinnitettävä huomiota erityisesti silloin, kun valitaan henkilöä työyhteisön riskienhallinnan kannalta keskeisiin ja kriittisiin tehtäviin. Työnhakijan esittämien työtodistusten lisäksi voi olla tarkoituksenmukaista hankkia aikaisemmilta työnantajilta henkilöä koskevia tietoja tai pyytää poliisilta turvallisuusselvitys. Voimassa oleva lainsäädäntö edellyttää, että tähän on saatava aina työnhakijan suostumus. Lasten kanssa työskentelevien taustat on lain mukaan aina selvitettävä, eikä tähän tarvitse pyytää tehtävään esitetyn suostumusta.

Työnantaja voi myös edellyttää työnhakijalta, että henkilö suostuu soveltuvuustesteihin tai huumetestiin. Työnantaja ei voi kuitenkaan pakottaa hakijaa kumpaankaan. Työnantajan vastuulla on selvittää, että käytettävät testausmenetelmät ovat riittävän laadukkaita.

5.3 Henkilöstön luotettavuus ja sitoumukset

Henkilöstöturvallisuuden tarkoituksena on saada ihmiset toimimaan sovitulla tavalla. Lähtökohtana on työntekijöiden ja työnantajan välillä vallitseva keskinäinen luottamus. Toimintayksikön keskeisten arvojen toteutuminen edellyttää, että tehtävien ja työn tukena on toimintayksikön johdon päättämät toimintapolitiikat ja strategiat sekä näitä täydentävät yksityiskohtaisemmat menettelytapaohjeet. Tietoturvallisuuskulttuurin edistämiseksi ja ylläpitämi-

seksi on tarkoituksenmukaista saada kaikilta työntekijöiltä sitoumus keskeisten menettelytapojen osalta. Sitoumuksessa sovitaan tietoturvallisen työskentelyn pelisäännöt, joista käy selkeästi ilmi, mikä on sallittua ja mikä ei.

Työntekijän luotettavuutta voidaan mitata säännöllisesti työsuhteen aikana. Ensisijaisesti arvioinnin tekee esimies, mutta ulkopuolistenkin toteuttamia testejä voidaan käyttää. Testaamalla suoritettavaan arviointiin on aina saatava työntekijän suostumus.

5.4 Henkilöstön koulutus

Tietoturvallisuuskulttuurin luomisessa ja ylläpidossa ei riitä, että on olemassa sääntöjä, ohjekirjeitä ja menettelytapaohjeistuksia, vaan henkilöstölle on tarjottava myös perehdytystä ja koulutusta. Suotavaa olisi, että koulutusta antaisi toimintayksikön oma henkilöstö. Ostopalveluja käytettäessä tulee varmistaa, että koulutuksen sisältö vastaa työnantajan näkemyksiä toimintayksikön toimintapolitiikoista, strategioista sekä menettelytavoista.

5.5 Ulkopuoliset työntekijät ja ostopalvelut

Ulkopuolisilla työntekijöillä tarkoitetaan henkilöitä, jotka työskentelevät toimintayksikön lukuun jossain muussa yrityksessä tai yhteisössä eli tuottavat erilaisia palveluita toimintayksikölle. He voivat olla myös itsellisiä yrittäjiä, jotka tekevät työtään joko kyseisen toimintayksikön tiloissa tai muiden kuin tilaajana toimivan toimintayksikön hallinnoimissa toimitiloissa. Ulkopuolisten työntekijöiden henkilöstöturvallisuuden osalta menetellään täsmälleen samoin kuin omankin henkilöstön kyseessä ollessa lainsäädännölliset ja sopimusjuridiset seikat huomioon ottaen. Erityistä huomiota sopimuspolitiikkaan ja menettelytapoihin tulee kiinnittää silloin, kun ulkopuolinen työntekijä työskentelee jossain muussa maassa kuin Suomessa ja kyseisen maan lainsäädäntö poikkeaa suomalaisesta lainsäädännöstä.

5.6 Työsuhteen päättymismenettely

Työntekijän työsuhteen päättyessä työnantajan ja esimiehen velvollisuutena on huolehtia yhdessä työntekijän kanssa siitä, että työntekijän henkilökohtaisessa käytössä olleiden työasemien tai muiden sähköisten tallennusvälineiden kovalevyjen ja muistikorttien sisältämät työnantajalle kuuluvat tiedot saadaan talteen ja että salassa pidettävää tietoaineistoa ei joudu valtuudettomien käyttöön. Tie-

tojen avaamisessa ja talteen otossa tulee ottaa huomioon yksityisyyden suojasta työelämässä säädetyssä laissa annetut määräykset menettelytavasta. Tietojärjestelmien käyttöoikeudet ja kulunvalvontaoikeudet tulee poistaa työsuhteen päättymispäivänä. Tietoturvalliseen työsuhteen päättymismenettelyyn kuuluu myös, että työntekijän työhuoneen arkistot ja työpöydän laatikot siivotaan, ja niiltä osin kuin työnantajalle kuuluvia tietoja ei tarvita, ne tuhotaan tiedon suojaustason edellyttämällä tavalla. Erikseen tulee antaa ohjeet työasemien kovalevyjen ja muiden tallennusvälineiden tietojen tuhoamismenettelystä.

6 Fyysinen tietoturvallisuus

Fyysiseen tietoturvallisuuteen kuuluu toimitilaturvallisuus ja toimitilojen suojaaminen. Tavoitteena on riskienhallinnan keinoin estää toimintayksikön tilojen vahingoittuminen minimoimalla niihin kohdistuvat uhat.

Fyysinen turvallisuus tarkoittaa toimintayksikön tuotanto- ja toimitilojen suojaamista siten, että estetään toimintayksikön hallitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. Tämä tietoturvallisuuden alue kattaa kulunvalvonnan, teknisen valvonnan ja vartioinnin, murtovahinkojen, palo-, vesi-, sähkö-, lämmitys- ja ilmastointivahinkojen torjunnan sekä tietoaineistoja sisältävien lähetysten turvallisuuden.

Uhkien kartoittamisessa ja tunnistamisessa tarkasteltavia seikkoja ovat:

- kiinteistön turvallisuus
- työ- ja laitetilojen turvajärjestelyt
- asiakaspalvelutilojen turvallisuus
- varavoimajärjestelmät.

6.1 Rakenteellinen suojaaminen ja valvonta

Rakenteellisella suojaamisella, valvonnalla ja vartioinnilla toimintayksikkö pyrkii suojaamaan omistamiaan ja hallinnoimiaan tietoja mahdollisia tunkeutujia vastaan. Suojarakenteilla, kuten aidoilla ja iskunkestävillä ikkunalaseilla, pyritään pitkittämään tunkeutujan sisälle pääsyä. Valvonnan avulla pyritään lyhentämään vasteaikaa vartijoiden ja muiden kohdesuojaukseen osallistuvien tahojen hälyttämiseksi.

Kiinteistövalvonnan tehtävänä on pyrkiä estämään tai paljastamaan kiinteistöön kohdistuva ilkivalta sekä kiinteistön sähkö-, vesi-, lämmitys- ja ilmastointijärjestelmien viat. Toimintayksikön toiminta ei missään olosuhteissa saa vaarantua toimitilojen käytön estymisen johdosta tai toimintayksikön toiminnalle elintärkeiden tietojen tai tietojärjestelmien tuhoutumisen tai käytön estymisen vuoksi.

6.2 Lukitukset ja kulunvalvonta

Lukituksilla ja kulunvalvonnalla on tarkoitus rajata ulkopuolisten pääsyä tiloihin, joissa säilytetään tai käsitellään sellaista tietoa, joka ei saa joutua valtuudettomien käsiin. Ulkopuolisten lisäksi voidaan tarvittaessa rajata myös toimintayksikön oman henkilöstön kulkuoikeuksia.

6.3 Palontorjunta

Palontorjunnan tehtävänä on estää palojen synty sekä mahdollisissa palotilanteissa minimoida toimitiloille, laitteille, tietojärjestelmille ja tiedoille aiheutuvia vahinkoja.

On otettava huomioon, että jo 60 celsiusasteen lämpötila tuhoaa sähköisillä tallenteilla (levykkeet, CD-ROM-levyt ym.) olevat tiedot joko osittain tai kokonaan. Varmuuskopiot ja -tallenteet tulee siksi säilyttää palonkestävissä kaapeissa.

Sammuttimien valinnassa tulee ottaa huomioon, että on olemassa erityisesti sähköpalojen sammuttamiseen tarkoitettuja sammutintyyppejä. Sammutinjärjestelmiä valittaessa tulee ottaa huomioon toimitiloissa olevien tietojärjestelmälaitteiden käytettävyyden turvaaminen palotilanteiden ja sammutustoimenpiteiden jälkeenkin.

7 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan häiriötöntä viestintää.

Tietoliikenneturvallisuuteen kuuluu mm. tietoliikennelaitteiston kokoonpano, laitteiston luettelointi, ylläpidon järjestelyt ja muutosten valvonta sekä dokumentointi.

Tietoliikenteen häiriöttömyys edellyttää verkon valvontaa, viestinnän varmistamista, merkityksellisten tapahtumien tarkkailua (esim. poikkeuksellisen suuri sähköpostiliikenne), tietoliikenneohjelmien testausta ja ongelmatilanteiden kirjausta.

Uhkien tunnistamisessa tarkkailtavia asioita ovat:

- verkon valvonta (hallinta, reititykset, käyttö, varajärjestelyt)
- salauksen toimivuus
- palomuuriohjelmiston ajantasaisuus
- ulkopuolisten yhteyksien ja palvelujen toimivuus.

7.1 Verkon turvallisuus

Toimintayksikön tietoliikenteen verkkoja suunniteltaessa ja rakennettaessa tulee arvioida tarvittavien yhteyksien kriittisyys työasemien ja palvelimien välillä ottaen huomioon toimintayksikön toimintojen haavoittuvuus mahdollisten vikojen ilmaantuessa. Toimintahäiriöiden vaikutusta voidaan vähentää rakentamalla kehäverkkoja tai kahdentamalla yhteydet.

Langattomien verkkojen kautta tapahtuvassa tietoliikenteessä tulee ottaa huomioon salauksen tarve silloin, kun verkkoa käytetään salassa pidettävien tietojen välittämiseen. Tämä koskee myös toimintayksiköstä ulospäin suuntautuvaa tai toimintayksikköön eri verkkojen kautta saapuvaa liikennettä.

7.2 Energiansaannin turvaaminen

Oleellinen tekijä tietoliikenneturvallisuuden ylläpidossa on energian saannin turvaaminen. Riskikartoituksessa tulee kartoittaa toiminnalle kriittiset tietojärjestelmät (palvelimet, reitittimet ja kytkimet) seuraavasti:

- käyttökatkoja ei sallita
- lyhyet käyttökatkot (sekuntiluokkaa) sallitaan
- minuuttiluokan käyttökatkot sallitaan
- tuntiluokan käyttökatkot sallitaan.

Kriittisten palvelimien toimintatekniikan tulee mielellään olla sellainen, että palvelin käynnistyy itsestään sähkökatkon jälkeen.

Tietoverkon rakentamisessa tulee ottaa huomioon verkon herkkyys sähköhäiriöille ja ylijännitepiikeille. Kaapeloinnin laadulla sekä tietoliikennekaapeleiden erottamisella muista sähkönsiirtokaapeleista voidaan välttää valtaosa häiriötekijöistä.

Tietojärjestelmäverkon riskiluokittelussa voidaan käyttää seuraavaa ryhmittelyä:

- atk-konehuoneet
- verkon reitittimet ja reitityslinjalla olevat kytkimet
- tärkeät yksittäiset käyttäjäpisteet
- muut merkittävät toimintokokonaisuudet
- tavalliset rivikäyttäjät.

Energiansaannin suunnittelun lähtökohdaksi voidaan asettaa, että kaikkia verkon reitittimiä, kytkimiä ja käyttäjien työpisteitä ei ole välttämätöntä saattaa katkottoman sähkön piiriin. Tämä tarkoittaa, että kaikkia tietoliikennelaitteita ei varusteta UPS-laitteilla eli varmistusakuilla jo senkin takia, että sähkönsaannin varmentamiseen tarvittavat investoinnit ja ylläpitokustannukset ovat suuret suhteessa saatavaan hyötyyn.

Valtaosa tietoliikennelaitteista tulee kuitenkin kytkeä varavoimakoneesta saatavaan sähköenergiaan. Sähkönsaanti yleisistä verkoista on hyvä suunnitella siten, että toimintayksikköön on saatavissa energiaa kahden eri muuntopiirin kautta.

Atk-konehuoneen suunnittelun lähtökohtina voidaan pitää soveltuvin osin seuraavia seikkoja:

- kahdennetut järjestelmät
- UPS-laitteistot (varakäyntitavoite vähintään 30 minuuttia)
- varavoimageneraattoreiden käynnistysvirran saamisen varmentaminen
- jäähdytysjärjestelmän sähkönsyöttö ja sen varmentaminen
- turvavalaistus ja sen varmentaminen
- paloilmoitinjärjestelmät ja niiden sähkönsaannin varmistus
- sammutusjärjestelmät ja niiden soveltuminen kohteeseen
- rikosilmoitusjärjestelmä ja sen sähkönsaannin varmistaminen
- lukitusjärjestelmä ja sen sähkönsaannin järjestäminen (jos käytetään sähkölukkoja)
- kulunvalvontajärjestelmä ja sen sähkönsaannin varmistaminen

- tv- ja videovalvontajärjestelmät ja niiden sähkönsaannin varmistaminen
- savunpoistojärjestelmä ja sen sähkönsaannin varmistaminen.

7.3 Sähköposti

Sähköpostijärjestelmät käyttävät viestinvälitykseen pääasiassa internet-järjestelmää. Tämän vuoksi sähköposti ei ole turvallinen tapa lähettää salassa pidettävää aineistoa, ellei viestiä salata päästä päähän lähettäjältä vastaanottajalle. Jos käytetään salaustekniikoita, salauskoodin tulisi olla vähintään 132-bittinen koodin murtamisen vaikeuttamiseksi.

Sähköpostijärjestelmän toiminnan turvaamiseksi palomuurissa tulee käyttää mm. seuraavia menetelmiä virusten sekä roskapostin torjumiseksi:

- ***Viestin edelleen välittämisen estäminen (releointi).*** Sähköpostijärjestelmä ei välitä automaattisesti ulospäin sellaisia viestejä, jotka ovat lähtöisin muualta kuin toimintayksikön omasta osoitteistosta ja joiden vastaanottajan osoite ei ole toimintayksikön sähköpostiosoite.
- ***Tuntemattomista toimialueista tai koneista välitetyt viestit.*** Postipalvelin tekee nimipalvelutarkastuksen. Mikäli järjestelmä ei tunnista lähettävää toimialuetta tai konetta, postitus estyy automaattisesti siihen saakka, kunnes järjestelmä on varmistanut lähettäjän.
- ***Postin välitysesto.*** Sähköpostijärjestelmä ei välitä postia palvelimilta tai yksittäisiltä työasemilta, joilta saapuu roskapostia tai joiden ylläpitäjän tiedetään tukevan roskapostittajia.
- ***Postin välitysesto koneista, joiden verkko-osoite on jatkuvasti vaihtuva (dynaamisesti varattava).*** Sähköpostijärjestelmä estää postin välittämisen koneista, joiden verkko-osoite vaihtuu jatkuvasti.
- ***Palvelinkohtainen pääsylista.*** Sähköpostijärjestelmään voidaan tarvittaessa ohjelmoida palvelinkohtaisia pääsylistoja haittapostin torjumiseksi. Listan avulla voidaan verkon kuormituksen hallitsemiseksi sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja.
- ***Kapasiteetin turvaamiseen perustuva suodatus.*** Sähköpostipalvelimen lokeja reaaliaikaisesti tarkkailemalla havaitaan normaalista poikkeavat postilähetykset. Kapasiteetin liiallista kuormittumista osoittavat usein epätavallisen pitkät yhteysajat postipalvelimeen, poikkeuksellinen määrä viestejä samasta lähteestä tai viestin vastaanottajien suuri määrä.
- ***Viestien koon ja liitetiedostojen määrän rajoittaminen.*** Sähköpostiviestien kokoa ja niiden sisältämien liitetiedostojen määrää voidaan

rajoittaa, mikäli käytössä oleva palvelinkapasiteetti sitä edellyttää ja rajoitteista on tiedotettu.

- ***Haittaohjelmien tunnistaminen ja poistaminen.*** Haittaohjelmien välittämiseen tyypillisesti käytettäviä tiedostotyyppejä tulee seurata. Välitettävistä viesteistä voidaan poistaa haittaohjelmat tai tuhota haittaohjelman sisältävä viesti.
- ***Roskapostin tunnistaminen ja suodattaminen.*** Sisällöllisessä analyysissä haitalliseksi luokiteltu viesti tulee aina merkitä roskapostiksi. Viesti tulee toimittaa suodatettuna vastaanottajan sähköpostiin. Posti voidaan suodattaa myös erilliselle karanteenialueelle, josta se on vastaanottajan luettavissa, tai saattaa viesti muutoin vastaanottajan tietoon kohtuullisen ajan kuluessa.
- ***Viestien toimittamisen viivästäminen.*** Viestien mukana tulevien haittaohjelmien tunnistamiseksi voidaan tarvittaessa viivästää viestien toimittamista vastaanottajalle asian selvittämisen vaatiman ajan.

Tiedot toimintayksikön käyttämistä suodatusmenetelmistä tulee olla kuvattuna ja kaikkien saatavilla.

8 Käyttöturvallisuus

Käyttöturvallisuus kattaa tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvän turvallisuuden. (Tavoitteena on tietokoneiden, ohjelmistojen ja tietoliikennelaitteiden päivittäisen käytön hallinta ja ylläpito.)

8.1 Käyttöympäristön hallinta

Käyttöympäristön (IT-infrastruktuurin) hallinta kuvataan toimintayksikköä varten laaditussa käsikirjassa. Ohjeistossa kuvataan tietotekniikkahenkilöstön päivittäisiä laitteisto-, ohjelmisto- ja tietoliikenneympäristöön liittyviä rutiininomaisia tehtäviä ja menettelyjä ongelmatilanteiden ratkaisemiseksi. Näitä ovat esimerkiksi:

- oikeuksien määrittäminen
- oletussalasanojen vaihtomenettelyt
- menettelytavat tietojärjestelmiä muutettaessa
- järjestelmien, laitteiden jne. käyttöönoton hyväksymis- ja siirtomenettelyt
- varusohjelmisto- ja korjauspäivitykset
- huoltokatkojen suunnittelu ja tiedotus
- varmuuskopiointi
- suojakopiointi
- järjestelmäkellojen synkronointi
- käytön tuen järjestäminen
- häiriöraportointi
- järjestelmädokumentaation suojausmenettelyt
- järjestelmän hallinta- ja analysointivälineiden suojaus
- laite-, kytkentä- ja operointitilojen valvonta.

8.2 Käyttöoikeus- ja valtuushallinta

Käyttöoikeus- ja valtuushallinta käsittää järjestelmien käyttöoikeusperiaatteiden määrittelyn. Siinä otetaan huomioon tietojärjestelmien käytölle tarvittavat käyttäjäkohtaiset rajoitukset.

Käyttöoikeudet ja -valtuudet myönnetään kunkin tietojärjestelmän osalta erikseen peruskäyttäjille ja pääkäyttäjille. Oikeuksista ja valtuuksista tulee pitää rekisteriä. Oikeuksien ja valtuuksien muuttamis- ja poistamismenettelyt tulee ohjeistaa.

Salasanakäytännöistä tulee olla erilliset ohjeet. Ohjeissa tulee korostaa salasanan laatukysymyksiä, eli salasanan tulisi olla vähintään kahdeksan merkkiä pitkä ja sen tulisi sisältää sekä isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. Salasanojen säilytysmenettelystä tulee antaa selkeät ohjeet.

8.3 Matkatyö, etätyö ja etäkäyttö

Toimintayksikön tulee määritellä, mitä työtehtäviä voidaan suorittaa etätyönä. Työnantaja vastaa etätyön tekemiseen soveltuvan suorituspaikan fyysisten turvatekijöiden määrittelystä. Työnantaja vastaa etätyössä tarvittavan välineistön, käyttöjärjestelmien, hyötyohjelmistojen sekä työn edellyttämien tietoliikenneyhteyksien investointi- ja käyttökustannuksista.

Työnantajalla on oikeus määrittää etätyön tekemiseen tarvittavien tietoteknisten välineiden ja ohjelmistojen yhteensopivuusvaatimukset siten, että järjestelmät eivät ole ristiriidassa työpaikalla käytettävien tietojärjestelmien kanssa.

Etätyöstä tulee aina tehdä sopimus työnantajan ja työntekijän välillä. Sopimuksen tulee sisältää maininta myös työn valvonnasta, lokitietojen tarvittavasta seurannasta sekä käyttäjätuesta.

8.4 Haittaohjelmistojen ja -koodien torjunta

Toimintayksiköllä tulee olla ohjeet haittaohjelmistojen ja -koodien torjunnasta. Torjunta tulee ohjeistaa erikseen palvelimien ja yksittäisten työasemien sekä kannettavien tietokoneiden osalta. Toimintayksiköllä tulee olla myös ohjeet virustorjuntatietokantojen päivittämisestä sekä käyttöönotosta toimintayksikössä. Samoin tulee ohjeistaa ilmoitusmenettelyt ongelmatilanteissa.

8.5 Tietotekninen valvonta

Tietotekniseen valvontaan kuuluu operointipäiväkirjan pitäminen. Toimintayksikön tulee suunnitella seuraavat ohjelmistojen käyttöä koskevat kirjaamismenettelyt (lokitiedot):

- virhelokien seuranta ja toimenpiteet
- järjestelmään tunkeutumisen havaitseminen ja toimenpiteet
- järjestelmän ja verkon valvonta
- työasemakäytön valvonta
- vikatilanteen havaitseminen ja toimenpiteet.

8.6 Toipumissuunnittelu

Toipumissuunnittelun (jatkuvuussuunnittelun) lähtökohtana on keskeytysvaikutusanalyysin laatiminen. Analyysissä määritellään järjestelmäkohtaisesti palvelutasovaatimukset, käytettävyystavoitteet sekä sallitut keskeytysajat. Analyysin tuloksena saadaan toimintojen ja järjestelmien tärkeysluokitus, jolla ohjataan järjestelmien resurssitarpeiden määrittelyä.

Toipumissuunnittelussa määritellään toiminnallinen varautuminen sekä tekninen varautuminen tietoaineiston varmistamismenettelyineen. Toipumissuunnitelmassa tulee ohjeistaa häiriöiden ja keskeytysten havaitsemis-, kirjaamis- sekä korjausmenettelyt. Suunnitelman kaikki tehtävät tulee vastuuttaa joko omalle henkilöstölle varahenkilöineen tai ostopalvelujen kyseessä ollessa palveluntuottajan nimeämille henkilöille. Myös tilannejohtaminen on ohjeistettava ja vastuutettava.

8.7 Tietoturvallisuus poikkeusoloissa

Tietoturvallisuuden suunnitteluun poikkeusoloja varten kuuluu toimintayksikön poikkeusolojen aikaisten tehtävien määrittäminen. Suunnittelussa on otettava huomioon toiminnan uhat sekä sidosryhmien tarpeet tietojen saamiseksi tai niiden tuottamiseksi. Toimintayksikön tärkeysluokituksen perusteella varataan valmiuden ylläpitämiseksi henkilöstö, tilat, laitteet, varaosat ja tarvikkeet. Lisäksi selvitetään huollon ja ylläpidon turvaamismenettelyt. Suunnittelussa tulee kuvata menettelyt tietotekniikan käytöstä luopumisesta sekä paluusta normaalioloihin.

9 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus käsittää käyttöjärjestelmien, varusohjelmistojen sekä sovellus- ja tietoliikenneohjelmien turvallisuuden ylläpidon.

Ohjelmistoturvallisuuskokonaisuuteen kuuluvat ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt sekä ohjelmistojen laadunvarmistus- ja turvallisuustoimet. Palveluja ulkoistettaessa tulee pyrkiä vastaavaan turvallisuustasoon kuin omassa toimintayksikössäkin.

9.1 Ohjelmistoturvallisuuden tavoitteet

Tavoitteena on turvata ohjelmistojen käyttöoikeuksien lisäksi ohjelmistojen käytettävyys kaikissa olosuhteissa. Ohjelmistojen laadun ja käytettävyyden varmistamiseksi tulee välttää ilmaisjakelussa olevia ohjelmia. Kaikille ohjelmille tulee hankkia lisenssit ja ne tulee rekisteröidä ohjelman valmistajan edellyttämällä tavalla. Tällä varmistetaan ohjelmistojen versio- ja korjauspäivitykset.

Tietoturvallisuuden takaamiseksi tulee selvittää ja varmistaa ohjelmistojen tarjoamien suojausominaisuuksien riittävyys siinä toimintaympäristössä, jossa ohjelmistoa on tarkoitus käyttää. Suojausominaisuuksiin kuuluvat ylläpitomenettelyt, muutoshallinta, vastuuhenkilötoimintayksikkö (omistaja, pääkäyttäjä, tekninen ylläpitäjä) ja seuraavat kontrollit:

- sisäänkirjautuminen
- muut liittymät
- tiedon syöttö
- tiedon siirto ja käsittely
- tiedon säilytys
- raportointi ja tulostus.

Liitteessä 4 on esitetty menetelmä järjestelmän tai ohjelmiston turvallisuusluokan määrittämiseksi toimintakriittisyyden perusteella.

9.2 Elinkaarimalli

Elinkaarimalli kuvaa ohjelman tai ohjelmiston elinkaaren hankintapäätöksestä siihen hetkeen saakka, kun ohjelma tai ohjelmisto poistetaan käytöstä ja arkistoidaan dokumentteineen ja tietojärjestelmälaitteineen. Tämänkin jälkeen ohjelmaa tai ohjelmistoa saatetaan tarvita sellaisia tiedonkäsittelytoimenpiteitä varten, joihin myöhemmin käyttöönotetut ohjelmat eivät sovellu.

9.3 Salausohjelmat

Salausohjelmilla voidaan salata kaikki siirrettävä tietoliikenne, yksittäinen viesti tai erillinen tietoaineisto. Salausohjelmien käyttöpolitiikka riippuu siirrettävän tiedon arkaluontoisuudesta ja kriittisyydestä.

10 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden tavoitteena on varmistaa tietoaineistojen
- käytettävyys
- eheys
- luottamuksellisuus.

Tietoaineistoturvallisuutta tukevia keinoja ovat mm. tietoaineistojen luokitus ja luettelointi sekä tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen.

10.1 Tietoaineiston luokittelu

Tietoaineiston luokittelusta on säädetty viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999, 18:4 §) ja asetuksessa (1030/1999). Henkilötietolaissa (523/1999) on säädetty erikseen henkilötiedoista ja niiden käsittelystä.

Laissa yksityisyyden suojasta työelämässä (759/2004) on säädetty työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Laissa on säädökset menettelytavoista ja salassapitokäytännöistä työnantajalle kuuluvien tietojen käsittelyn ja toisaalta työntekijälle kuuluvien tietojen osalta.

10.2 Tietoaineiston turvaaminen, varmistus ja palauttaminen

Tietoaineiston turvaamisella tarkoitetaan paperimuotoisen aineiston turvaamisen lisäksi sähköisesti käsiteltävän tai puhutun tiedon turvaamista. Turvaamismenetelmien vaatimustaso riippuu tietoaineiston luokittelusta. Salassa pidettävien tietojen fyysisen käsittely-ympäristön lisäksi tulee kiinnittää huomiota työaseman käyttötapaan joko toimintayksikön omissa tiloissa tai työskenneltäessä kannettavan työaseman kanssa toimipaikan ulkopuolella. Vaatimuksena on turvata salassa pidettävien tietojen käsittely siten, etteivät valtuudettomat pääse käsiksi tietoihin. Tämä koskee myös puhuttua tietoa joko toimintayksikön tiloissa tai tilojen ulkopuolella.

Salasanamenettelyn sekä pääsyoikeuspolitiikan ja -menettelyjen avulla määritellään ja turvataan pääsyoikeudet toimintayksikön eri käyttöjärjestelmiin, tiedon käsittelytiloihin sekä itse tietoihin. Käyttäjän kannalta yksinkertaisin käyttötapa on ns. ”single sign on” -menetelmä, jolloin yhdellä käyttäjätunnuksella ja salasanalla käyttäjä pääsee kirjautumaan kaikkiin käyttäjälle oikeutettuihin tiedostoihin ja järjestelmiin.

Tietojen varmistus tehdään yksinkertaisimmin tallentamalla käsiteltänä oleva tieto työskentelyn aikana säännöllisin väliajoin työaseman kovalevylle, palvelimelle tai muulle tallenteelle. Näin varmistetaan tiedon säilyminen ja käytettävyys, jos aineisto jostakin syystä tuhoutuu kesken käsittelyn.

Toimintayksikön elintärkeä ja salassa pidettävä turvaluokiteltu tieto ja/tai tiedon varmuuskopiot tulisi säilyttää palo- ja murtoturvallisessa paikassa, esimerkiksi paloturvallisuusluokitellussa kassakaapissa. Sähköisten varmennustallenteiden osalta tulee ottaa huomioon ohjeet sähköisten arkistoiden käsittelystä ja säilytyksestä. Tietojen eheyden säilyminen edellyttää, että sähköiset tallenteet kopioidaan säännöllisesti tiettyjen määrävuosien välein uusille tallennusaihioille.

Nykymenetelmin pystytään useimmiten palauttamaan lähes täysin esimerkiksi tulipalossa olleen työaseman kovalevyllä ollut tieto.

10.3 Tietoaineiston arkistoturvallisuus

Tietojen ja tietoaineistojen arkistoinnissa tulee ottaa huomioon lainsäädännön vaatimukset säilyttämisajoista ja -tavoista (arkistolaki 831/1994). Sosiaali- ja terveydenhuollon tietojen arkistointia koskevien määräysten ja ohjeiden lisäksi toimintayksiköllä tulee olla ohjeet muun salassa pidettävän tiedon ja asiakirjojen säilytyksestä ja arkistoinnista. Laki edellyttää, että toimintayksikössä on vastuullinen arkistotoimesta vastaava henkilö.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä säädetyn lain (159/2007) mukaan asiakastietoja tulee käsitellä siten, että turvataan tietojen saatavuus ja käytettävyys. Asiakastietojen tulee säilyä eheinä ja muuttumattomina koko niiden säilytysajan. Palvelun antajan tulee kerätä lokitiedot kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta.

Julkisen terveydenhuollon palvelujen antajan on lain mukaan liityttävä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi. Samoin tulee tehdä myös yksityisen terveydenhuollon palvelujen antajan, jos potilasasiakirjojen pitkäaikaissäilytys tapahtuu sähköisesti.

Tietojen arkistoinnin ja palauttamisen osalta on otettava huomioon tietotekniikan menetelmäkehitys. Toimintayksikön tulee varmistaa myös vanhojen toimintayksikölle tärkeiden tietojen käytettävyys ja eheys säilyttämällä toi-

mintayksikössä esimerkiksi tiedon syntyhetkellä tiedon tuottamiseen käytössä olleet käyttö- ja tietojärjestelmät sekä mahdollisesti sen aikainen tietokone tai tiedon käsittelylaite, jotta tiedon saa palautetuksi ja muokatuksi sopivaksi uusien käyttö- ja tietojärjestelmien kanssa.

10.4 Tietoaineiston tuhoaminen

Toimintayksikön tietoturvaohjeistossa on kuvattava tiedon hävittämismenetelmät. Ohje on samalla osa toimintayksikön jäteohjetta. Hävittäminen toteutetaan tiedon luottamuksellisuuden mukaisesti. Tiedon hävittämisen koko logistiikkaketju tulee kuvata toimintayksikön ohjeissa. Jos tietosuojattua jätettä toimitetaan ulkopuoliselle palveluntuottajalle tuhottavaksi, on jokaisesta tuhottavasta erästä pidettävä kirjaa, ja menetelmä on ulkoisesti arvioitava aika ajoin, jotta voidaan varmistaa järjestelmän aukottomuus.

Liitteessä 5 on esitetty valtionvarainministeriön VAHTI-ohjeistosta taulukko erilaisten tietoaineistojen hävittämismenettelyistä.

11 Laiteturvallisuus

Laiteturvallisuuden tavoitteena on varmistaa laitteiden ja tieto-omaisuuden vahingoittumattomuus sekä estää niiden katoaminen.

Laiteturvallisuus käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon, kierrätyksen, poiston ja laadunvarmistuksen.

11.1 Laitteet, tarvikkeet ja hankinnat

Hankintoja suunniteltaessa ja toteutettaessa tulee varmistua laitteistojen yhteensopivuudesta sekä soveltuvuudesta. Tätä varten määritellään edellytykset, jotka tietojärjestelmälaitteiston tulee täyttää. Järjestelmäkuvaukseen sisällytetään palvelimet ja keskuslaitteet, sisäverkon reitittimet, työasemat, kannettavat tietokoneet, langattomat verkot sekä muut tietojärjestelmälaitteet.

Elinkaaritarkastelussa tulee laitteiston käyttöikä määritellä etukäteen. Lisäksi tulee varmistaa, että laitteistoa voidaan uusia tai laajentaa ja että laitteiston ylläpidolle ja huollolle löytyy tuki.

Laitteet tulee rekisteröidä ja turvamerkitä. Laitteilla tulee olla nimetyt vastuuhenkilöt.

Laitteistojen omille ohjelmille tulee saada versio- ja korjauspäivitykset.

Laitteistoturvallisuuteen kuuluu myös suunnitella laitteiden kierrätys ja käytöstä poistaminen.

Arkistoidessaan sähköisessä muodossa tietoa toimintayksikön tulee varmistua siitä, että tiedot saadaan myöhemminkin tarvittaessa käyttöön. Siksi tulee säilyttää myös vanhoja, poistettuja tietojärjestelmälaitteita sekä niiden sovellusohjelmistoja.

11.2 Kannettavat tietokoneet

Kannettavien tietokoneiden käytöstä ja säilytyksestä tulee toimintayksikön antaa ohjeet. Hankittaessa kannettavaa tietokonetta kannattaa valita sellainen malli, johon voi kiinnittää lukittavan varkaudenestovaijerin. Lukitusvaijerin kiinnipito myös omissa toimitiloissa työskenneltäessä tulisi ohjeistaa.

Käytettäessä kannettavaa tietokonetta etätyöskentelyyn joko langallisen tai langattoman yhteyden avulla, tulee yhteys suojata VPN-järjestelmällä. Lähtökohtana tulee olla, että kannettavan tietokoneen kovalevylle ei tallenneta mitään toimintayksikön salassa pidettävää tai luottamuksellista tietoa. Kannettavalla tietokoneella työskennellään etäyhteyden avulla, jolloin kaikki käsiteltävä tieto on saatavissa toimintayksikön palvelimelta ja tallennettavissa sille. Vastaavia turvaohjeita tulee soveltaa CD-ROM-levyille tai muille sähköisille tallennusvälineille (esimerkiksi ulkoinen kovalevy) tallennetun salassa pidettävän tiedon käsittelyssä.

11.3 Tietotekniikkahuolto

Tietotekniikkahuolto tulee järjestää siten, että toimitiloihin tuleva huoltohenkilö tai muualla toimitilojen ulkopuolella sijaitsevan huoltoliikkeen henkilöstö ei pääse käsiksi salassa pidettävään tietoon. Huoltohenkilöstöltä voidaan pyytää tietoturvasitoumus, jossa henkilöstö sitoutuu lain mukaiseen menettelytapaan, ja olemaan käyttämättä vahingossa haltuunsa saamaa tietoa tai edes paljastamaan, että henkilöllä on sellainen tieto hallussaan.

12 Tietoturvaloukkaus

Tietoturvaloukkaustilanteessa toimintayksikön omistamaa tai hallinnoimaa tietoa on joutunut valtuudettoman henkilön käyttöön tai joku on tahallaan tai tahattomasti estänyt menettelytavoillaan toimintayksikön tietojen käsittelyn toimintayksikölle ominaisella tavalla ja sen omistamilla tai hallinnoimilla tietojenkäsittelylaitteilla.

12.1 Tietoturvaloukkausten sanktiot

Tietojen valtuudeton käyttö, tunkeutuminen tietojärjestelmiin tai tietojenkäsittelyn häirintä loukkaavat tietojenkäsittelyn yksityisyyttä. Havaittuihin tapahtumiin tulee suhtautua vakavasti, koska loukatulle oikeudelle on olemassa rikoslain suoja. Asia voidaan lievissä tapauksissa hoitaa toimintayksikön sisäisin kurinpitomenettelyin. Vakavat tapaukset, kuten valtuudeton henkilötietojen luovutus, voivat johtaa viranomaiskäsittelyyn. Kaikissa tapauksissa rikkomuksista on ilmoitettava toimintayksikön johdolle sekä tietoturvallisuudesta vastaaville henkilöille.

Tietoturvallisuusrikokset voidaan jakaa vaikutusten kannalta seuraavasti:

- tiedonkäsittelyrauhan rikkominen, tiedonkäsittelyn estäminen
- tiedon valtuudeton käyttö
- tietojärjestelmän, käyttöjärjestelmän tai ohjelman valtuudeton käyttö.

Tietosuojarikkomus on asianomistajarikos, ja asian vireille saattaminen edellyttää pääsääntöisesti sen henkilön rikosilmoitusta, jonka tietoja on käytetty valtuudetta. Poliisi voi tutkintaa varten ottaa tilapäisesti haltuunsa tai hallintaansa tarpeellisiksi katsomiaan asiakirjoja, työasemia, palvelimia tai tallennusvälineitä.

12.2 Tietoturvaloukkausten havainnointi-, raportointi- ja käsittelymenettely

Tietoturvaloukkaustilanteessa selvitetään aiheutettu haitta ja sen vaikutukset. Tämä voidaan yleensä tutkia suoraan päätelaitteelta tai palvelimelta seuraavin keinoin:

- estetään tutkittavan päätelaitteen tai palvelimen käyttö sulkemalla käyttäjätunnuksen tai haitallisen IP-osoitteen (IP = päätelaitteen yksilöivä tunnus) oikeudet selvitystyön ajaksi
- seurataan tunnuksen käyttöä sekä tallennetaan käyttö lokiin todistusaineistoksi varmentaen, että tunnuksen käyttö ei vaaranna muun järjestelmän tietoturvallisuutta tai käytettävyyttä.

Tietoturvaloukkaus ja tietosuojarikkomus tulee aina selvittää sisäisesti kuitenkin siten, että salassa pidettävää tietoa ei paljasteta selvitystyön yhteydessä enempää kuin on tarpeellista.

Tietosuojan tai tietoturvallisuuden rikkomuksista asetettujen sanktioiden merkitys on ymmärrettävää ja täytöntöönpano selkeää, jos yhteisöllä on valmiiksi mietitty tietoturvallisuuspolitiikka, johdonmukaisesti määritellyt henkilövastuut ja yksiselitteiset menettelyohjeet sekä yhteisö on kouluttanut henkilöstön.

TIETOTURVALLISUUS LAINSÄÄDÄNNÖSSÄ

1. Yleiset tietoturvallisuutta koskevat säädökset

1.1 Tietoaineistoa koskevia säädöksiä

Perustuslaki (731/1999)

- yksityiselämän suoja (10 §)
- sananvapaus ja julkisuus (12 §)

Henkilötietolaki (523/1999)

- yksityiselämän suoja ja muut yksityisyyden suojaa turvaavat perusoikeudet (1 §)
- tietoturvallisuus ja tietojen säilytys (32-35 §)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

- julkisuusperiaate (1 §)
- velvoite hyvään tiedonhallintatapaan (3 §)
- tiedonsaanti salassa pidettävästä asiakirjasta (10 §)
- asianosaisen oikeus tiedonsaantiin (11 §)
- viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (17 §)
- hyvä tiedonhallintatapa (18 §)
- salassapitovelvoitteet (22 § - 25 §)
- asiakirjasalaisuus (22 §)
- vaitiolovelvollisuus ja hyväksikäyttökielto (23 §)
- salassa pidettävät viranomaisen asiakirjat (24 §)
- salassapidosta poikkeaminen ja sen lakkaaminen (26 §-32 §)

Asetus viranomaisen toiminnan julkisuudesta (1030/1999)

- selvitykset hyvän tiedonhallintotavan toteuttamiseksi (1 §)
- erityissuojattavan tietoaineiston luokitus (2 §)
- erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet (3 §)
- ohjeet, valvonta ja seuranta (4 §)
- selosteet tietojärjestelmistä (8 §)

Arkistolaki (831/1994)

- käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
- turvaaminen tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä (12 §)

Laki turvallisuusselvityksistä (177/2002)

- lain soveltamisala (1 §)
- perusmuotoinen turvallisuusselvitys, hakija (4 §)
- turvallisuusselvityksen tekeminen; perusteena olevat rekisteritiedot (8 §)
- turvallisuusluokitus (14 §)
- laajan turvallisuusselvityksen tekeminen (15 §)
- suppean turvallisuusselvityksen tarkoitus (19 §)

Sisäasiainministeriön asetus turvallisuusselvitysten hakemismenettelystä (710/2002)

Laki lasten kanssa työskentelevien rikostaustan selvittämisestä (504/2002)

- työnantajan velvollisuus pyytää rikosrekisteriote nähtäväksi (3 §)
- yksityisten sosiaalipalvelujen tai yksityisten terveydenhuollon palvelujen tuottajan rikosrekisteriote (4 §)
- merkintä rikosrekisteriotteen esittämisestä ja otteen palauttaminen (7 §)
- vaitiolovelvollisuus (8 §)

Hallintolaki (434/2003)

- asiamiehen ja avustajan salassapitovelvollisuus (13 §)
- asiakirjan lähettäminen viranomaiselle ja hallintoasian vireilletulo (16 § – 22 §)

1.2 Tietoaineistoa ja tietotekniikkaa koskevat säädökset

Laki sähköisestä asioinnista hallinnossa (1318/1999)

- varmentamistoiminta (4 § - 12 §)
- sähköisten asiointipalvelujen järjestäminen, tietoturvallisuus (18 §)
- asian vireillepano sähköisellä asiakirjalla (22 §)

Laki sähköisestä viestinnästä oikeudenkäyntiasioissa (594/1993)

Laki sähköisistä allekirjoituksista (14/2003)

- sähköisten allekirjoitusten käyttö, niihin liittyvien tuotteiden ja palvelujen tarjonta sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuoja ja tietoturva

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

- hallintoasian, tuomioistuinasian, syyteasian ja ulosottoasian sähköinen vireillepano, käsittely ja tiedoksianto
- asioinnin sujuvuuden, ja joutuisuuden sekä tietoturvallisuuden lisääminen edistämällä sähköisten tiedonsiirtomenetelmien käyttöä

Laki yksityisyyden suojasta työelämässä (759/2004)

- työntekijä koskevien tietojen käsittely, työntekijälle tehtävät testit ja tarkastukset, tekninen valvonta työpaikalla, työntekijän sähköpostien hakeminen ja avaaminen

Laki yksityisyydensuojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)

- televiestinnän turvallisuus (4 §)
- teleyrityksen tietoturvallisuusvelvoitteet (6 §)
- teleoperaattorien vaitiolovelvollisuus (7 §)
- rajoitukset suoramarkkinoinnille (21 §)

Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain muuttamisesta (459/2002)

- suoramarkkinoinnin tunnistettavuus (21 a §)

Telemarkkinalaki (396/1997) ja laki telemarkkinalain muuttamisesta (566/1999)

- suojauksen purkujärjestelmän kielto (25 §)

Rekisterihallintolaki (166/1996)

Rikoslaki muutoksineen (578/1995, 951/1999)

- luvaton käyttö (28. luku 7 § - 9 §)
- vahingonteko (35.luku 1 § - 3 §)
- viestintäsalaisuuden loukkaus (38. luku 3 §)
- tietomurto (38. luku 8 §)
- virkasalaisuuden rikkominen (40. luku 5 a §)
- vaaran aiheuttaminen tietojenkäsittelylle (34. luku 9 a §)

Pakkokeinolaki (450/1987) muutoksineen (18/2003, 64/2003, 646/2003)

- telekuuntelun edellytykset (2 §)
- televalvonnan edellytykset (3 §)

- teknisen tarkkailun edellytykset (4 §)
- DNA-tunnisteiden määrittäminen ja tallettaminen (5 §)
- telekuuntelun edellytykset (2 §)
- 1 luku Kiinniottaminen. pidättäminen ja vangitseminen; pidättämisen edellytykset (3 §)
- 5 luku Etsintä. paikkaan kohdistuva etsintä; Kotietsintä esineen löytämiseksi (1 §)
- 5 a luku Telekuuntelu, televalvonta ja tekninen tarkkailu; (1 § – 3 §, 3a §, 4 §, 4 a §, 4 b §, 5 §)

Poliisilaki (493/1995)
- 3 luku, Tiedonhankintaa koskevat säännökset (28 § - 36 §)
- vaitiolovelvollisuus (43 §)
- vaitiolo-oikeus (44 §)

Tekijänoikeuslaki (404/1961)
- ohjelmistojen tekijänoikeudet (Laki tekijänoikeuslain muuttamisesta 446/1995)
- tietokantojen käyttö (Laki tekijänoikeuslain muuttamisesta 250/1998)

Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002)
- sopimusta koskevien muotovaatimusten täyttäminen sähköisesti (12 §)
- vastuuvapaus tiedonsiirto- ja verkkoyhteyspalveluissa (13§)
- vastuuvapaus tallennettaessa tietoja välimuistiin (14 §)
- vastuuvapaus tietojen tallennuspalveluissa (15 §)
- tiedon saannin estoa koskeva määräys (16 §)
- sisällön tuottajan oikeusturva (18 §)

2. *Poikkeusolojen valmiutta koskevat säädökset*

Valmiuslaki (1080/1991)

Laki huoltovarmuuden turvaamisesta (1390/1992)

Valtioneuvoston päätös huoltovarmuuden tavoitteista (350/2002)
- Varautumisen tavoitteet, yhteiskunnan tekniset perusrakenteet

3. *Sosiaali- ja terveydenhuollon toimintoja koskevat erityissäädökset*

Laki potilaan asemasta ja oikeuksista (785/1992) muutoksineen (489/1999, 653/2000, 411/2001)

- potilaan tiedonsaantioikeus (5 §)
- tiedonsaantioikeus ja toimivalta (9 §)
- potilasasiakirjat ja hoitoon liittyvä muu materiaali (12 §)
- potilasasiakirjoihin sisältyvien tietojen salassapito (13 §)
- salassapitovelvollisuuden rikkominen (14 §)

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)

- asiakkaan oikeus saada selvitys toimenpidevaihtoehdoista (5 §)
- tietojen antaminen asiakkaalle tai hänen edustajalleen (11 §)
- asiakkaan ja hänen edustajansa tietojenantovelvollisuus (12 §)
- asiakirjasalaisuus (14 §)
- vaitiolovelvollisuus ja hyväksikäyttökielto (15 §)
- suostumus tietojen antamiseen (16 §)
- salassa pidettävien tietojen antaminen asiakkaan hoidon ja huollon turvaamiseksi (17 §)
- salassa pidettävien tietojen antaminen asiakkaan suostumuksesta riippumatta eräissä muissa tilanteissa (18 §)
- vaitiolovelvollisuudesta poikkeaminen ja sen lakkaaminen (19 §)
- velvollisuus antaa sosiaalihuollon viranomaiselle salassa pidettäviä tietoja (20 §)
- tietojen luovuttaminen teknisen käyttöyhteyden avulla (21 §)
- sosiaalihuollon viranomaisen oikeus saada virka-apua (22 §)
- asiakirjojen käsitteleminen ja säilyttäminen (26 §)
- tietosuojaa ja virka-apua koskevien säännösten soveltamisala (27 §)
- merkintä tietojen hankinnasta ja antamisesta (28 §)
- rangaistusvastuu (29 §)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

- asiakastietojen käytettävyys ja säilyttäminen (4 §)
- käytön ja luovutuksen seuranta (5 §)
- potilasasiakirjojen tietorakenteet (6 §)
- tunnistaminen (8 §)
- asiakirjan sähköinen allekirjoittaminen (9 §)
- potilastietojen luovuttaminen (10 §)
- hakutiedot (11 §)

- hakutietojen luovutuskielto (12 §)
- potilaan suostumus (13 §)
- valtakunnalliset tietojärjestelmäpalvelut (14 §)
- velvollisuus siirtyä tietojärjestelmäpalvelujen käyttäjäksi (15 §)
- vastuut tietojärjestelmäpalvelujen hoidossa (16 §)
- potilaan informointi (17 §)
- asiakkaan tiedonsaantioikeus (18 §)
- katseluyhteys (19 §)
- ohjaus, valvonta ja seuranta (20 §)
- rangaistussäännökset (23 §)

Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001)

- soveltamisala (1 §)
- potilasasiakirjat (2 §)
- yleiset rekisterinpitäjän velvoitteet (3 §)
- tietojen käyttöoikeudet (4 §)
- palvelujen hankkiminen toiselta (5 §)
- oikeus tehdä merkintöjä potilasasiakirjoihin (6 §)
- potilasasiakirjamerkintöjä koskevat keskeiset periaatteet ja vaatimukset (7 §)
- potilasasiakirjoihin merkittävät perustiedot (10 § - 21 §)
- potilasasiakirjojen säilyttäminen (22 § - 23 §)

Laki sähköisestä lääkemääräyksestä (61/2007)

- lain tarkoitus (1 §)
- lain soveltamisala (2 §)
- määritelmät (3 §)
- potilaan informoiminen (4 §)
- lääkemääräyksen tietosisältö (6 §)
- lääkemääräyksen allekirjoittaminen (7 §)
- lääkemääräyksen salaaminen (8 §)
- potilasohje (9 §)
- apteekin tiedonsaantioikeus (11 §)
- sähköisen lääkemääräyksen toimittaminen (12 §)
- lääkärin ja hammaslääkärin tiedonsaantioikeus (13 §)
- tietojen luovuttaminen viranomaisille (15 §)
- potilaan tiedonsaantioikeus (16 §)
- katseluyhteys (17 §)
- tietojen säilyttäminen (19 §)
- sähköisen lääkemääräyksen tietotekninen toteutus (20 §)
- lääkemääräys- ja toimitusohjelmistot (21 §)

- sähköisen lääkemääräyksen käyttöönotto (23 §)
- ohjaus, seuranta ja valvonta (24 §)
- maksut (25 §)
- rangaistus- ja viittaussäännökset (26 §)

Asetus terveydenhuollon ammattihenkilöistä (546/1994)

(Toimintayksikkö)

KÄYTTÄJÄN TIETOSUOJAOHJEET (malli)

(Annetaan sitoumuksen tehneelle henkilölle)

Työasemien (sisältää tietoverkkoon langallisesti/langattomasti liitetyt atk-laitteet), tietoliikenneverkon ja atk-järjestelmien käyttöoikeudet annetaan vain niille, jotka ovat allekirjoittaneet tämän salassapito- ja käyttäjäsitoumuksen.

1. Salassapito

- Palvelussuhteen/muun työtehtävän aikana tai sen päätyttyä ei työssä saatuja (toimintayksikkö)_____, sen toimintayksikköjä, asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia luottamuksellisia tai salassa pidettäviä tietoja saa ilmaista ulkopuoliselle tai sivulliselle. Potilaiden/asiakkaiden (terveydentila)tietojen lisäksi tällaisia tietoja ovat myös liike- ja ammattisalaisuudet sekä tiedot turvallisuus- ja valmiusjärjestelyistä.
- Rekisterien katselu- tai käyttöoikeutta ei ole muihin kuin työtehtävien edellyttämiin tietoihin.
- Salassapitovelvollisuudesta (asiakirjasalaisuus ja vaitiolovelvollisuus) säädetään useissa laeissa.
- Laki potilaan asemasta ja oikeuksista (POTL 785/92, muut. 653/2000, 13 §) ja Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki viranomaisen toiminnan julkisuudesta (621/1999, 24 §)
- Henkilötietolaki (523/1999, 33 §)
- Potilastiedot/asiakastiedot ovat potilaslain/sosiaalihuollon asiakaslain mukaan salassa pidettäviä.

2. Käyttäjätunnus ja salasana

- Käyttäjätunnukset ovat henkilökohtaisia. Poikkeuksena on rajoitetussa käytössä oleva ryhmäkohtainen työasemasidonnainen käyttäjätunnus. Tunnuksella on aina vastuullinen haltija (henkilö), jonka nimiin tunnus on myönnetty. Kukin vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja tapahtumista. Työsuhteen päättyessä poistetaan automaattisesti myös käyttöoikeudet.
- Salasana on vaihdettava heti sen saamisen jälkeen ja myöhemmin sovituin aikavälein tai tarvittaessa.
- Käyttäjätunnus ja salasana on pidettävä salassa. Niitä ei saa antaa muiden tietoon. Työnantajataholta ei koskaan kysytä käyttäjätunnusta tai salasanaa.

3. Työaseman käyttö

- Työasema on tarkoitettu vain työtehtävien suorittamista varten.
- Vähäinen määrä henkilökohtaista käyttöä on sallittu esimiehen antamalla luvalla.
- Työasemassassa saa käyttää vain toimintayksikön hyväksymiä ja lisenssoituja ohjelmia, jotka ovat tulosalueen tietohallintopalveluista vastaavan yksikön asentamia ja tukemia tai erillisellä tulosalueen tietohallintopalveluista vastaavan yksikön hyväksymällä tavalla muun toimittajan asentamia ja tukemia.
- Tulosalueen tietohallintopalveluista vastaavan yksikön luomia asetuksia ei saa muuttaa. Tämä koskee myös näytönsäästäjiä ja taustakuvia.
- Toimintayksikön hankkimia ohjelmia ei saa kopioida.
- Työasemaa ei saa liittää verkkoon tai siirtää toiseen työskentelypaikkaan luvatta. Tämä koskee myös kannettavia tietokoneita.
- Tietojärjestelmistä on kirjauduttava ulos tai työasema on lukittava välittömästi käytön jälkeen myös poistuttaessa työaseman välittömästä läheisyydestä silloin, kun työaseman käyttöä ei pysty valvomaan.
- Työasemaa saa käyttää vain omalla käyttäjätunnuksella ja salasanalla.
- Samoja levykkeitä tai muita tietovälineitä ei saa käyttää työpaikalla ja sen ulkopuolella, jollei ole varmistautunut niiden viruksettomuudesta.
- Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Kuvia, grafiikkaa ja äänitiedostoja saa välittää verkossa tai tallentaa palvelimelle vain työtehtävien vaatiessa.
- Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi.
- Työasemaa ei saa käyttää tiedostojen pysyvään säilytykseen.
- Työasemaan talletettujen tiedostojen varmuuskopioimisesta vastaa kukin käyttäjä itse. (Palvelimilla olevien tiedostojen varmistuskopiointi hoidetaan keskitetysti tai järjestelmän pääkäyttäjän toimesta.)

4. Sähköpostin ja Internet-yhteyksien käyttö

- Internet/WWW-selaimen käytöstä kertyy loki- ja varmistustietoja, joita seurataan säännöllisesti.
- Internetistä ei saa kopioida ohjelmia.
- Arkaluonteisia ja muita salassa pidettäviä tietoja ei saa lähettää ulkoisen sähköpostin välityksellä.
- Virusriskin vuoksi ulkopuolelta tulevan sähköpostin liitetiedostoja ei saa avata, jos viesti tulee epämääräisestä lähteestä. Viesti on hävitettävä.
- Sähköpostia (esim. etunimi.sukunimi@hus.fi) ei saa ohjata automaattisesti edelleen toimintayksikön ulkopuolelle.
- Sähköpostiketjukirjeitä ja muuta niin sanottua roskapostia ei saa lähettää eikä välittää eteenpäin, vaan ne on tuhottava.

5. Järjestelmäkohtaiset ohjeet

- Kunkin käyttäjän on tutustuttava toimintayksikön sekä oman toimintayksikkönsä tietosuojaohjeisiin sekä käyttämiensä tietojärjestelmien käyttöohjeisiin ja rekistereiden rekisteriselosteisiin.
- Tietojärjestelmien käytöstä kertyy sormenjälkitietoa, ja järjestelmien käyttöä seurataan.

6. Seuraamukset

- Sääntöjen ja sitoumuksen mukaisten periaatteiden rikkomisesta käyttöoikeudet tietojärjestelmiin peruutetaan määräajaksi tai toistaiseksi, kunnes rikkomus on käsitelty.
- Rikkomuksista tiedotetaan aina esimiehelle. Jos kyseessä on tahallinen tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli tahallisesta rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, on aiheuttaja myös vahingonkorvausvelvollinen.
- Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

7. Ilmoitusvelvollisuus

- Tietokoneviruksista on aina ilmoitettava tulosalueen tietohallintopalveluista vastaavaan yksikköön.
- Kaikista käyttäjätunnusta ja salasanaa koskevista epäselvistä tiedusteluista tulee ilmoittaa välittömästi tulosalueen tietohallintopalveluista vastaavaan yksikköön (atk-tuki).
- Havaitsemistasi tietosuojarikkomuksista tai sellaisen yrityksistä tulee aina ilmoittaa lähiesimiehelle sekä tulosalueen tietohallintopalveluista vastaavaan yksikköön (atk-tuki).

8. Työnantajan velvolisuus

- (Toimintayksikön nimi) työnantajavelvollisuutena on suojata työntekijöitään tietoturvan ja tietosuojan loukkauksilta.

Sitoumus tehty / 200……..

(Toimintayksikkö) _____

SALASSAPITO- JA KÄYTTÄJÄSITOUMUS (malli)

Olen perehtynyt minulle esitettyyn tällä hetkellä voimassa olevaan _____:n salassapito- ja käyttäjäsitoumukseen, _____:n tietoturvapolitiikkaan ja ohjeisiin sekä tietosuojavelvoitteisiin.

Sitoudun noudattamaan niitä samoin kuin muita erikseen annettuja salassapitoon ja tietoturvaan liittyviä ohjeita ja määräyksiä.

Olen lukenut ja ymmärtänyt salassapito- ja käyttäjäsitoumuksen periaatteet ja sitoudun noudattamaan niitä.

Toimipaikka

Pvm. / 200

Allekirjoitus _____

Nimen selvennys _____

Henkilötunnus _____

Esimiehen allekirjoitus _____

☐ Tietosuojaohjeet annettu

Tämä sitoumus säilytetään palvelussuhteen ajan ja arkistoidaan palvelussuhteen päätyttyä kymmenen vuoden ajaksi.

MENETELMÄ JÄRJESTELMÄN TURVALLISUUSLUOKAN MÄÄRITTÄMISEKSI TOIMINTAKRIITTISYYDEN PERUSTEELLA

Selvitetään kehitettävän tietojärjestelmän/tiedonkäsittelymenetelmän turvallisuusluokka (kriittisyys) toimintavaikutusten perusteella:

- selostus kehitettävästä järjestelmästä/käyttöönotettavasta tiedonkäsittelymenetelmästä
- selvitys turvatason valintaan vaikuttavista järjestelmistä ja mekanismeista
- selvitys järjestelmistä tai menetelmistä, joihin kyseisen järjestelmän turvatason valinta vaikuttaa
- määritetään kehitettävän järjestelmän osalta arvioinnin lähtökohdat:
  - järjestelmän käytettävyysvaatimukset ja ongelmien vaikutus toimintaan
    - käyttökatkon maksimipituus enintään (ei koskaan, enintään minuutteja, enintään tunteja, enintään pari päivää, enintään viikko, useita viikkoja)
  - eheysvaatimukset ja ongelmien vaikutus toimintaan
  - luottamuksellisuushäiriöiden vaikutukset toimintaan
- mahdolliset tarkentavat kysymykset ja näkökohdat, joilla on vaikutusta järjestelmän/tiedonkäsittelymenetelmän turvallisuusluokan määrittämiseen.

SALASSA PIDETTÄVIEN TIETOJEN JA ASIAKIRJOJEN TUHOAMINEN

Tieto-aineisto	Turvaluokka			
		Ei-julkinen/salassa pidettävä		
	Julkinen	Luottamuksellinen	Salainen	Erittäin salainen
Paperi-aineisto	Toimitetaan uusio-käyttöön	Silputtava enintään 4 x 60 mm kokoisiksi silpuiksi ristiin silppuavalla leikkurilla ennen uusiokäyttöön luovuttamista (DIN standardi 32757, turvaluokka3)		Silputtava enintään o,8 x 15 mm kokoisiksi silpuiksi (DIN standardi 32757, turvaluokka 5)
Mikro-filmit	Sisältää hopeaa:	hävitetään hopeaa poistavissa erikoisliikkeissä tai polttamalla ongelmajätelaitoksissa		Silputtava enintään 0,2 x 0,2 mm silpuiksi (DIB standardi 32757, turvaluokka 5, mikrofilmit)
	Ei sisällä hopeaa	hävittäminen silppuamalla enintään 1 x 1 mm kokoisiksi silpuiksi (DIN standardi 32757, turvaluokka 3, mikrofilmit)		Silputaan kuten muutkin mikrofilmit
		Mikrofilmeistä syntyvä jäte toimitetaan kaatopaikalle jätelakia noudattaen.		
Magneettiset tietovälineet	Hävitetään alustamalla.	Alustuksessa on varmistettava, että menettely tuhoaa tiedon, eikä vain vapauta tilaa.		Hävittäminen rikkomalla levyt ja levykkeet, silppuamalla magneettinauhat ja kasetit
	Tietosuoja-luokiteltu tieto:	Hävitetään kirjoittamalla vapautetun tilan päälle merkkejä tarkoitukseen sopivilla ohjelmilla.		
	Kasetit, magneettinauhat ja levykkeet:	Demagnetoimalla HUOM! Salassa pidettävä tieto tulee salakirjoittaa tietovälineelle. Hävittäminen rikkomalla levyt ja levykkeet, silppuamalla magneettinauhat ja kasetit. Jäte toimitetaan kaatopaikalle jätelakia noudattaen.		
Muut tietovälineet:	Lisätietoja:	Tietosuojavaltuutetuntoimisto ja Arkistolaitos		

TIETOLÄHTEITÄ

Valtionhallinnon tietoturvallisuuden johtoryhmän julkaisut (VAHTI):

1. Valtion etätyön tietoturvallisuussuositus, VAHTI 1/1999
2. Valtion tietohallintotoimien ulkoistamisen tietoturvallisuus-suositus, VAHTI 2/1999
3. Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000
4. Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
5. Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuus-suositus, VAHTI 3/2000
6. Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000
7. Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
8. Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
9. Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
10. Sähköisten palvelujen ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
11. Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001
12. Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001
13. Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
14. Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
15. Etätyön tietoturvaohje, VAHTI 3/2002
16. Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2002
17. Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
18. Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003
19. Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
20. Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
21. Käyttäjän tietoturvaohje, VAHTI 5/2003
22. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003

23. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
24. Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004
25. Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
26. Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
27. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 4/2004
28. Valtionhallinnon sähköpostien käsittelyohje, VAHTI 1/2005
29. Tietoja valtion tietohallinnosta ja tietotekniikasta vuodelta 2004, VAHTI 2/2005
30. VAHTIn toimintakertomus vuodelta 2005, VAHTI 1/2006
31. Electronic Mail-handling Instruction for State Government, VAHTI 2/2006
32. Selvitys valtionhallinnon tietoturvaresurssien jakamisesta, VAHTI 3/2006
33. Selvitys valtion ympärivuorokautisen tietoturvatoiminnan järjestämisestä, VAHTI 4/2006
34. Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006
35. Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006
36. Muutos ja tietoturvallisuus – alueellistamisesta ulkoistamiseen – hallittu prosessi, VAHTI 7/2006
37. Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
38. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006
39. Henkilöstön tietoturvaohje, VAHTI 10/2006
40. Tietoturvakouluttajan opas, VAHTI 11/2006
41. Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006
42. Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 1/2007

www.vn.fi

ISO/IEC 17799:fi; Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen Standardisoimisliitto SFS.

ISO/IEC 27001:FI; Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS.

Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Ohje sosiaali- ja terveydenhuollon

organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi; STAKES, Raportteja 5/2005, Tero Tammisalo, Helsinki 2005.

Opas sosiaali- ja terveydenhuollon organisaation tietoturvan hallinnointiin. Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietoturvan hallinnointiin ja hallinnointimenettelyiden kehittämiseen. STAKES, Tero Tammisalo, moniste.

SOSIAALI- JA TERVEYSMINISTERIÖN JULKAISUJA
ISSN 1236-2050

2007:

1 Tasa-arvo valtatiellä. Hallituksen tasa-arvo-ohjelman 2004–2007 loppuraportti. (Julkaistaan ainoastaan verkossa www.stm.fi)
ISBN 978-952-00-2258-7 (PDF)

2 Men and Gender Equality Policy in Finland.
ISBN 978-952-00-2269-3 (pb)
ISBN 978-952-00-2270-9 (PDF)

3 Hyvinvointi 2015 -ohjelma. Sosiaalialan pitkän aikavälin tavoitteita.
ISBN 978-952-00-2275-4 (nid.)
ISBN 978-952-00-2276-1 (PDF)

4 HTP-arvot 2007. Haitallisiksi tunnetut pitoisuudet.
ISBN 978-952-00-2307-2 (nid.)
ISBN 978-952-00-2308-9 (PDF)

5 Seulontaohjelmat. Opas kunnille kansanterveystyöhön kuuluvien seulontojen järjestämisestä. Screeningprogram. Handbok för kommuner om ordnande av screening som ett led i folkhälsoarbetet.
ISBN 978-952-00-2309-6 (nid.)
ISBN 978-952-00-2310-2 (PDF)

6 Leena Tamminen-Peter, Maj-Britt Eloranta, Marja-Leena Kivivirta, Eija Mämmelä, Irma Salokoski, Arja Ylikangas. Potilaan siirtymisen ergonominen avustaminen. Opettajan käsikirja.
ISBN 978-952-00-2313-3 (nid.)
ISBN 978-952-00-2314-0 (PDF)

7 Sairauspoissaolokäytäntö työpaikan ja työterveyshuollon yhteistyönä.
ISBN 978-952-00-2317-1 (nid.)
ISBN 978-952-00-2318-8 (PDF)

8 Arbetsplatsen och företagshälsovården i samarbete om sjukskrivningspraxis
ISBN 978-952-00-2319-5 (inh.)
ISBN 978-952-00-2320-1 (PDF)

9 Nationell beredskapsplan för en influensapandemi. (Publiceras bara på Internet www.stm.fi).
ISBN 978-952-00-2325-6 (PDF)

10 National preparedness plan for an influenza pandemic. (Published only at Internet www.stm.fi).
ISBN 978-952-00-2326-3 (PDF)

2007: 11 Toimeentulotuki. Opas toimeentulotukilain soveltajille. 6. korj. p.
ISBN 978-952-00-2334-8 (nid.)
ISBN 978-952-00-2335-5 (PDF)

12 Utkomststöd. Handbok för tillämpning av lagen om utkomststöd.
ISBN 978-952-00-2336-2 (inh.)
ISBN 978-952-00-2337-9 (PDF)

13 Asumista ja kuntoutusta. Mielenterveyskuntoutujien asumispalveluja koskeva kehittämissuositus.
ISBN 978-952-00-2338-6 (nid.)
ISBN 978-952-00-2339-3 (PDF)

14 Sosiaalialan ammatillisen henkilöstön tehtävärakennesuositus.
Toim. Pirjo Sarvimäki, Aki Siltaniemi.
ISBN 978-952-00-2366-9 (nid.)
ISBN 978-952-00-2367-6 (PDF)

15 Säker läkemedelsbehandling. Nationell handbok för genomförande av läkemedelsbehandling inom social- och hälsovården.
ISBN 978-952-00-2368-3 (inh.)
ISBN 978-952-00-2369-0 (PDF)

16 Kvalitetsrekommendation för främjande av hälsa.
ISBN 978-952-00-2372-0 (inh.)
ISBN 978-952-00-2373-7 (PDF)

17 Seksuaali- ja lisääntymisterveyden edistäminen.
Toimintaohjelma 2007–2011.
ISBN 978-952-00-2376-8 (nid.)
ISBN 978-952-00-2377-5 (PDF)

18 Sosiaalihuollon ammatillisen henkilöstön kelpoisuusvaatimukset valtio-, kunta- ja yksityissektorilla
ISBN 978-952-00-2392-8 (nid.)
ISBN 978-952-00-2393-5 (PDF)

19 Tietoturvallisuussuunnitelman laatiminen.
Opas sosiaali- ja terveydenhuollon toimintayksiköille.
ISBN 978-952-00-2398-0 (nid.)
ISBN 978-952-00-2399-7 (PDF)