



KANGASALAN KUNNAN SOSIAALI- JA TERVEYSKESKUKSEN TIETOTURVAPERIAATTEET

Hyväksytty: Sosiaali- ja terveystieteiden lautakunta 1.11.2011 § 85

1. JOHDANTO

Tietoturvallisuus on osa riskienhallintaa ja tietoturvaperiaatteet kuuluvat organisaation tiedon hallinnan kokonaisarkkitehtuuriin. Periaatteet koskevat organisaation omaa toimintaa sekä organisaatiolle palveluita tuottavia tahoja. Periaatteet toteutetaan hyväksymisen jälkeen. Sähköisten toimintojen osalta periaatteet otetaan käyttöön viimeistään eReseptin osalta liityttäessä valtakunnalliseen Reseptikeskukseen ja kaikkien potilastietojen osalta viimeistään liityttäessä Kelan eArkistoon.

Alueella hoidettavien potilaiden ja asiakkaiden koko hoito- ja palveluketjun ja siihen liittyviä palveluja tuottavien tahojen tietoturvan tulee olla yhtenäinen ja eri osapuolien tiedossa.

Asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukainen saatavuus, käytettävyys, suojaaminen, eheys sekä tietojen ja aineistojen asianmukainen hävittäminen ovat osa tietoturvaperiaatteita. Asiakastietojen turvallinen käsittely korostuu entisestään siirryttäessä asiakastietojen sähköiseen käsittelyyn. Tämä tarkoittaa tietojen ja sähköisten palvelujen, yksittäisten tietojärjestelmien sekä tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi hallinnollisin ja teknisin toimenpitein.

Tietoturvallisuuden päämäärä on turvata koko organisaation toiminnalle tärkeiden arkistojen, tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää asiakirjojen ja tietojen sekä tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen, varautua toiminnan keskeytymisiin ja niistä palautumiseen sekä minimoida vahingot.

Tietoturvallisuuteen liittyvän varautumisen tavoitteena on kaikissa turvallisuustilanteissa, että:

- Toimintayksiköt kykenevät takaamaan palvelujensa jatkuvuuden ja tiedon turvaamisen
- Tietoturvaan varautuminen on jokapäiväistä toimintaa
- Tietoturvaan varautuminen on osa tietohallinnon ja sen käyttämien palveluntuottajien, yleisen turvallisuuden ja varautumisen kokonaisuutta
- Yksiköiden on tunnistettava prosessiensa ja toimintojensa kriittisyys ja asetettava niille myös tietoturvaan liittyvät käytettävyys- ja palvelutasovaatimukset
- Työjärjestyksissä ja tehtäväkuvauksissa määritetään palveluiden jatkuvuuden hallintaan, tiedon turvaamiseen ja varautumiseen liittyvät vastuut, tehtävät ja johtosuhteet.



2. HALLINNOLLINEN TURVALLISUUS

Hallinnollinen tietoturvallisuus on organisaation tietoturvatyötoimintojen johtamista, organisointia ja ylläpitoa, mikä muodostaa perustan tietoturvatyötoiminnalle. Tavoitteena on sekä tietoturvallisuuden toteutuminen että johdon ja henkilöstön sitoutuminen tietoturvallisuuden suunnitelmalliseen kehittämiseen ja hoitamiseen.

Hallinnollisen tietoturvallisuustyön tulos on kuvaus tietoturvallisuustoiminnan periaatteista, tietoturvatyön järjestelyistä, organisoinnista, arvioinnista, ylläpidosta ja kehittämisjärjestelmästä sekä kunkin työhön osallistuvan tieto omista vastuistaan ja tietoturva-tehtävistään.

Hallinnollisessa tietoturvallisuudessa määritellään resurssit sekä tietoturvatyölle yleensä että tietoturvan ohjeistukselle, koulutukselle, valvonnalle ja raportoinnille. Hallinnollinen turvallisuus sisältää myös tietoturvallisuuden hallintajärjestelmän oikeuksineen ja vastuineen.

Hallinnollisen tietoturvallisuuden periaatteet:

Organisaatio on julkaissut kirjallisen tietoturvapoliittikan, jossa ilmaistaan organisaation sitoutuminen tietoturvatyöhön ja tietoturvatyön organisointiin. Tietoturvapoliittikka on nähtävissä osoitteessa www.kangasala.fi.

Tietoturvaan ja tietosuojaan liittyvillä tehtävillä on nimetyt vastuuhenkilöt, jotka ovat organisaatiossa työskentelevien ja sidosryhmien vastuuhenkilöiden tiedossa. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuullean annetut tehtävät.

Organisaatio kehittää toimintaansa vastaamaan voimaan tulevia toimialan viranomais-suosituksia, valtakunnallisten tietojärjestelmäpalveluiden asettamia tietoturva-vaatimuksia sekä alueen sosiaali- ja terveydenhuollon salassa pidettävien tietojen käsittelyssä edellytetyjä tietoturvakäytäntöjä.

Organisaation johtamismalliin liitetään tietoturvan eri osa-alueita kuvaavat mittarit. Tietoturvatilannetta seurataan jatkuvasti raporteilla ja valvontajärjestelmillä sekä erikseen tehtävillä riskikartoituksilla. Havaintojen pohjalta tehdään vuosittainen tietoturvan kehittämissuunnitelma, jonka johto hyväksyy.

Tietoturvallisuusasioista annetaan ohjeet. Tietoturvallisuustietämyksen jatkuvasta ajan tasalla pysymisestä huolehditaan säännöllisen koulutuksen, tiedotuksen ja motiivoinnin keinoin.



Palveluiden hankinnoissa edellytetään, että tiedon käsittelyyn liittyvät suojaustoimet, vastuut ja tekniset tietoturvavastuut sisältyvät ostopalvelusopimuksiin. Palveluiden tuottajilta edellytetään:

- sovittua palvelutasoa vastaavaa tietoturvasoa,
- kuvausta palvelun tietoturvasostasta sekä tietoturvapoikkeamien valvonta-, havaitsemis-, ilmoittamis- ja käsittelykäytännöistä,
- että se pitää organisaatiolle toimitetut dokumentit ajantasaisina ja
- että se raportoi ostopalveluun liittyvistä tietoturvapoikkeamista.

Ohjelmistojen ja laitteiden tarjouspyynnöissä ja hankinnoissa edellytetään voimassa olevien standardien noudattamista ja ennen hankintapäätöksiä tehtyä tietoturvallisuuskäytännön arviointia.

3. HENKILÖSTÖTURVALLISUUS

Henkilöstöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvahäiriöiden hallintaa. Henkilöstöturvallisuustyön tulos on luotettava ja tehtäviinsä soveltuva henkilöstö, joka tuntee omaan toimenkuvaansa, tehtävänsä ja rooliinsa asetetut tietoturva-vaatimukset. Oman ja ostopalveluita organisaatiolle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin töitä koskeviin järjestelyihin liittyvät toimet, oma tietosuojansa sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä.

Henkilöstöturvallisuuden toimenpiteet kohdistuvat henkilöstöön liittyvien riskien hallintaan. Keskeisiä asioita ovat avainhenkilöriippuvuus ja sijaisjärjestelyt, palvelussuhteen järjestelyt, henkilöstön luotettavuus ja soveltuvuus, oikeuksien hallinta, työhönottomenetelmät, henkilöstön koulutus ja menettelytavat ulkopuolisten työntekijöiden osalta.

Henkilöstötietoturvallisuuden periaatteet

Henkilöstön tehtäväkuvauksia ylläpidetään siten, että tehtävistä on johdettavissa tehtävien edellyttämät henkilökohtaiset tietojärjestelmien käyttöoikeudet. Tietojärjestelmien käyttäjistä pidetään ajantasaisista rekistereistä, josta ilmenee käyttäjän yksilöllisyyden lisäksi käyttäjärooli. Ostopalveluiden tuottajien tai muuten organisaation tietojärjestelmiä käsittelevistä henkilöistä edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.

Uuden henkilöstön perehdytykseen kuuluu sosiaali- ja terveydenhuollon salassapitosääntöjen läpikäynnin lisäksi tietoturvakoulutus ja ennen tietojärjestelmäoikeuksien myöntämistä tietoturvasitoumuksen allekirjoittaminen.

Työntekijältä, jonka tehtävät edellyttävät alueellisten tai valtakunnallisten asiakas- ja potilastietojärjestelmäpalveluiden käyttöä, edellytetään virallisen henkilötodistuksen esittämistä ennen käyttöoikeuksien saamista. Valtakunnallisten tietojärjestelmäpalveluiden käyttö edellyttää henkilökohtaista VRK:n (Väestörekisterikeskuksen) myöntämää varmennekorttia. Käyttäjätunnuksen ja salasanan saaminen myös muihin asiakastietojärjestelmiin edellyttää työntekijän henkilöllisyyden varmistamista luotettavalla tavalla.



On ohjeistettu, että tietojärjestelmien käyttöoikeudet ja valvoton pääsy tiloihin, joissa on yhteys suojattuun tietojärjestelmäympäristöön, työtehtävien loppuessa päättyvät.

Työntekijät saavat säännöllisesti tietoturvakoulutusta. Tietämystasoa ja osallistumista koulutukseen seurataan ja tulokset raportoidaan organisaation vastuuhenkilölle.

Organisaation toiminnan turvaamiseksi tietojärjestelmien kriittisten tehtävien vastuuhenkilöllä on sovittu varahenkilö.

Työnkuviissa on huolehdittu, ettei synny tilanteita tai käyttöoikeuksia, jotka mahdollistavat tietojen käsittelyn ilman toisen työntekijän mahdollisuutta kontrolloida käsittelyä.

4. FYYSINEN TURVALLISUUS

Fyysiseen tietoturvaluuteen kuuluu toimitilaturvallisuus ja toimitilojen suojaaminen. Fyysinen turvallisuus tarkoittaa toimintayksikön tuotanto- ja toimitilojen suojaamista siten, että estetään toimintayksikön hallitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen väärin käsiin. Tämä tietoturvaluuden alue kattaa kulunvalvonnan, teknisen valvonnan ja vartioinnin, murtovahinkojen, palo-, vesi-, sähkö-, lämmitys- ja ilmastointivahinkojen torjunnan sekä tietoaineistoja sisältävien lähetysten turvallisuuden. Tavoitteena on riskienhallinnan keinoin estää toimintayksikön tilojen vahingoittuminen minimoimalla niihin kohdistuvat uhat. Uhkien kartoittamisessa ja tunnistamisessa tarkasteltavia seikkoja ovat mm: työ- ja laitetilojen turvajärjestelyt (konesalit, jakamotilat, tilat, joissa säilytetään paperiasiakirjoja) sekä varavoima- ja UPS-järjestelmät.

Sähkönsyöttö ja varautuminen sähkönsyötön katkoksiin tietojärjestelmän laitteille ja tiedonsiirtoverkolle vastaa ohjelmistojen kriittisyyttä toimintayksikön asiakaspalvelussa ja potilashoidossa.

Fyysisen tietoturvaluustyön tulos on tietojen hallittu käyttöympäristö, jossa tiedon käsittely ja siinä tarvittava tekniikka on suojattu fyysisten rakenteiden ja niiden vikojen aiheuttamilta tuhoilta ja vahingoilta. Työ liittyy kiinteistöjen ja laitetilojen suunnitteluun ja valvontaan sekä käsittää asiattoman pääsyn eston tiloihin, joissa tietoa käsitellään.

Fyysisen tietoturvaluuden periaatteet

Asiaton pääsy toimintayksikön tai sen palvelutuottajan tiloihin, joissa on pääsy suojattuun tietojärjestelmäympäristöön, estetään valvonnalla ja pitämällä lukittuna tilat, joissa ei ole henkilökuntaa tai kameravalvontaa. Tilojen avaimet ovat henkilökohtaisia ja avainten haltijoista pidetään rekisteriä.

Arkistojen ja tietoteknisten laitteiden sijoittelussa on huomioitu vesi, lämpö- ja tulivahinkojen riski. Palvelinten ja muiden järjestelmään kuuluvien laitteiden ja tiedonsiirtoverkon suojaus ja valvonta ulkoisilta uhkilta vastaa tietojärjestelmien kriittisyyttä toimintayksikön asiakaspalvelussa ja potilashoidossa.



5. TIETOLIIKENNETURVALLISUUS

Tietoliikenneturvallisuudella tarkoitetaan häiriötöntä viestintää, tiedonsiirtoyhteysien käytettävyyttä, tiedonsiirron suojausta ja salausta, käyttäjien tunnistusta ja verkon varmistamista.

Tietoliikenneturvallisuustyön tulos on turvatut tiedonsiirtoyhteydet. Työ kattaa asiakirjaliikenteen, tietoliikenneverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan sekä tietoliikenneverkon tapahtumien määrällisen ja laadullisen hallinnan.

Tietoliikenneturvallisuuden periaatteet

Organisaation tietojärjestelmäympäristö on suojattu palomuurilla, jota valvotaan. Palomuuuri sallii vain määritellyn liikenteen järjestelmiin. Yhteydet ulkoisiin järjestelmiin ja portaaleihin ovat vahvasti salattuja.

Asiakas- ja potilastietojärjestelmien käyttöön liittyvä tietoliikenne langattomassa sisäverkossa ja etäyhteyksissä on salattua. Myös hallinta – ja huoltotehtävien etäyhteydet on toteutettu suojattuna etäyhteyden käyttö edellyttää kirjautumista luotettavasti sähköisesti tunnistettuna.

6. LAITTEISTOTURVALLISUUS

Laitteistoturvalisuustyön tulos on päätelaitteiden, palvelimien ja muiden tiedon käsittelyssä käytettävien laitteiden tarkoituksenmukaisuus, käytettävyys ja saatavuus sekä toiminnan tarpeita tyydyttävä toiminta. Laitteistoturvalisuuden tavoitteena on varmistaa laitteiden ja tieto-omaisuuden käytettävyys, toiminta, ylläpito sekä laitteistojen ja tarvikkeiden saatavuus (vahingoittumattomuus ja katoamisen estäminen) ja käytöstä poistaminen. Perustietotekniikan hankinnat, ohjelmistojen asennukset ja poistot hoidetaan keskitetysti. Peruskäyttäjän tunnuksella ei pysty asentamaan ohjelmistoja.

Laitteistotietoturvalisuuden periaatteet

Kaikki hankittavat laitteistot ovat kokonaisarkkitehtuurin mukaisia tai muuten yhteensopivia organisaation tietojärjestelmäympäristön sekä sosiaali- ja terveydenhuollon tiedonvälitysverkoston kanssa.

Potilaiden hoito ja asiakastyö on pysyvää toimintaa, jota tehdään keskeytymättä ympäri vuorokauden. Toiminta on tietointensiivistä eikä se voi onnistua vaatimusten mukaisesti, jos tietojen saatavuudessa on merkittäviä katkoja. Työasemista ja oheislaitteista, esim. tulostimista, on tunnistettu kriittiset laitteet potilashoidon ja asiakastyön toteuttamisen jatkuvuuden sekä palvelutasovaatimusten kannalta. Palvelimien, verkon ja muiden laitteiden kriittisyys määräytyy niissä ylläpidettävien ohjelmistojen ja työaseman kriittisyyden perusteella. Kriittisille laitteistoille taataan katkoton sähkön syöttö ja korkea palvelutaso asiakas- ja hoitopalvelun aukioloaikoja vastaavasti. Tietojenkäsittelyn suo-



rituskyky varmistetaan riittävällä laite- ja verkkokapasiteetilla, ja näiden toimivuutta ja suorituskykyä seurataan automaattisella valvonnalla.

Laitteistot valitaan siten, että niiden voidaan olettaa kestävän kohtuullisen ajan tietojärjestelmien jatkuva eri osissa tapahtuva kehittäminen ja lisääntyvät tehokkuus- ja turvallisuusvaatimukset.

Laitteistoja hankittaessa otetaan huomioon kriittisyysluokituksen mukainen varaosien, huollon ja vararatkaisujen vaatimustenmukaisuus ja saatavuus myös poikkeuksellisten olojen, esimerkiksi lakkojen aikana.

7. TIETOAINEISTOTURVALLISUUS

Tietoaineistoturvallisuuden tavoitteena on varmistaa tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa.

Tietoaineistoturvallisuustyön tulos on tietoaineistojen hallinta siten, että säädösten mukaisesti taltioidut tiedot säilyvät ja ovat saatavissa käyttötilanteen edellyttämässä ajassa, tarkoituksenmukaisessa muodossa ja järjestyksessä sekä hävitetään asian mukaisesti.

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

Sosiaali- ja terveydenhuollon arkisto- ja asiakirjaohjeet määrittelevät asiakirjojen/tietojen luokittelusta, säilyttämisestä ja hävittämisestä sekä tietojen luovuttamisesta. Henkilörekisterin perustamiseen tarvitaan lupa ja rekisteriseloste.

Tietoaineistoturvallisuuden periaatteet

Tietoaineistoturvallisuuden periaatteet koskevat kaikkea asiakirja- ja tietoaineistoa. Asiakas- ja potilasturvallisuuden ja toiminnan jatkuvuuden kannalta on keskeistä, että työntekijä pystyy hyödyntämään tarpeellisia tai vähintään välttämättömiä asiakas- ja potilastietoja ja lisäksi hoito- ja asiakastilanteissa edellytettävällä sujuvuudella. Potilaita ja asiakkaita koskevat tietoaineistojen kriittisyys luokitellaan potilas- ja asiakasturvallisuuden ja palvelun jatkuvuuden lähtökohdista. Kriittisen tiedon saatavuus erityistilanteissa, kuten tietojärjestelmäkatkojen aikana, on suunniteltu toiminnan jatkuvuus- ja toipumissuunnitelmassa.

Käyttäjällä on oltava tehtävä, joka oikeuttaa asiakas- ja potilastietojen käsittelyyn. Sähköisessä muodossa olevia asiakas- ja potilastietoja saa käsitellä vain yksilöitävissä oleva henkilö, ja valtakunnallisten tietojärjestelmäpalveluiden kautta saatavien tietojen osalta, vain VRK:n myöntämällä varmennekortilla tunnistautunut henkilö. Tietoaineistojen käyttöä seurataan säännöllisesti ja seurannan periaatteet on käsitelty YT menettelyn mukaisesti organisaation työntekijöiden kanssa.



Sosiaali- ja terveystieteiden keskuksen tietoa-aineiston säilytys tapahtuu arkistonmuodostussuunnitelman mukaisesti, joka on laadittu arkistosäädöksiä ja asiakas- ja potilastietojen kansallista tehtäväluokitusta noudattaen. Tietoa-aineiston säilyminen luottamuksellisena, eheänä ja muuttumattomana on huomioitu tiedon koko elinkaaren aikana aineiston hävittämiseen asti.

Tietoa-aineiston lakisääteisen tarkastusoikeuden ja tiedonsaantioikeuden käytön toteuttamista varten on sovittu palvelusta vastaavat henkilöt ja prosessin toteuttamistapa on kuvattu.

Tietoa-aineiston käyttämisestä tai luovuttamisesta laskutus, tilastointi-, raportointi-, kehittämis- ja tutkimustarkoituksiin on annettu ohjeet, jotka sisältävät näiden tietojen käsittelyyn oikeuttavat työtehtävät.

Asiakas- ja potilastietoja ei lähetetä organisaation sisällä eikä organisaatiosta ulos salaamattomina eikä suojaamatonta yhteyttä pitkin.

Asiakas- ja potilastietojen käsittelystä on laadittu henkilökunnalle organisaatiokohtaiset ohjeet, joiden ylläpidosta vastaava henkilö on nimetty. Organisaatiossa noudatettavia yhtenäisiä käytännön menettelytapoja kuvaavat ohjeet tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja.

8. OHJELMISTOTURVALLISUUS

Ohjelmistoturvallisuus käsittää käyttöjärjestelmien, varusohjelmistojen sekä sovellusten suojausominaisuudet, näiden ylläpidon ja päivityksen sekä turvallisuustoimenpiteet, valvonta- ja lokimenettelyt. Ohjelmistoturvallisuustyön tulos on toiminnan tarpeita tyydyttävä ohjelmistojen käytettävyys, saatavuus ja toimivuus sekä se, että käytössä olevat ohjelmistot suojaavat sisältämänsä tiedon asetettujen vaatimusten mukaisesti.

Ohjelmistotietoturvallisuuden periaatteet

Ohjelmistoille on määritelty selkeät käyttötarkoitukset siten, että käyttäjä tietää mitä ohjelmistoa hänen tulee käyttää eri tehtävissä ja tarkoituksissa. Ohjelmistojen yhteistoiminnallisuus on varmistettu siten, että tietoa-aineisto pysyy eheänä ilman erillisiä käyttäjän toimia tallennusvaiheessa tai tietoa haettaessa.

Uuden ohjelman hankinnan edellytys on sen tekninen ja toiminnallinen yhteensopivuus käytössä jo olevien ohjelmistojen tai kokonaisarkkitehtuurissa ilmaistun tavoitetilan kanssa. Ohjelmistojen rajapinnoilta edellytetään avoimuutta siten, että rajapinnan tietojen rakenteen ja merkityksen oikeellisuus on varmistettavissa.

Ohjelmistojen kehittäminen perustuu toiminnan lähtökohdista todettuihin tarpeisiin, ja kehittämisprosessi on kuvattu. Ohjelmiston uudet piirteet hyväksytään ennen version vaihtoa. Versio hyväksytään käyttöön vasta, kun se on testattu tulevassa ympäristös-



sään ja todettu tilausta vastaavaksi teknisesti ja toiminnallisesti. Ohjelmiston tai sen version käyttöönotto perustuu hyväksytyyn käyttöönottosuunnitelmaan, jossa kuvataan myös mahdollisten ongelmien luokittelu, korjausmenettelyt ja niiden vasteaika.

Valtakunnallisten tietojärjestelmäpalveluiden kanssa asioiva ohjelmisto on testattu hyväksyttävästi valtakunnallisen palvelun järjestäjän edellyttämällä tavalla ja järjestelmä on todettu kansallisten auditointivaatimusten mukaiseksi.

KanTa-palvelun kautta luovutetun potilastiedon käsittely ohjelmistolla on mahdollista vain VRK:n toimikortilla tunnistetulle henkilölle, joka on nimenomaisesti saanut käyttöoikeuden katsoa luovutettua tietoa tai luovuttaa organisaation tietoja.

Ohjelmistojen toimivuuden valvonta ja ylläpidon palvelutaso vastaavat niiden määritellyä kriittisyyttä toiminnalle.

Salattuja tietoja sisältävistä ohjelmistoista on dokumentti, jossa kuvataan ohjelmiston suojaus haittaohjelmilta ja asiattomalta tunkeutumiselta sekä suojausten valvonta.

Ohjelmistossa käsiteltävien tietojen tietoturva vastaa tietoaineistojen kriittisyyttä ja määriteltyä elinkaarta. Ohjelmistoilla on jatkuvuus- ja toipumissuunnitelma, jotka potilashoidosta ja asiakaspalvelusta vastaavat henkilöt ovat hyväksyneet.

Ohjelmistojen ylläpitoa varten avatut etäyhteydet ovat suojattuja ja sanomaliikenne salattua. Etäyhteyden käyttö edellyttää luotettavaa tunnistautumista. Ohjelmiston ylläpito-toimien laajuus sekä niistä riippuvat hyväksymiskäytännöt ja ajoitus on sovittu ja dokumentoitu. Poikkeamista sovituista malleista seurataan ja siihen puututaan.

Työasemien ja palvelinten käyttöjärjestelmien sekä ohjelmistojen turvapäivityksiä varten on toimintasuunnitelma. Päivitystarvetta seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan. Turvaohjelmien päivitykset sijoitetaan toiminnan kannalta vähiten häiritsevään ajankohtaan, mikäli päivityksen aiheuttanut uhka ei aivan välttämättä vaadi päivityksen tekemistä heti.

9. KÄYTTÖTURVALLISUUS

Käyttöturvallisuus kattaa tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvän turvallisuuden. Se kattaa turvallisen käytön toimintaolosuhteet, tekniikan toimivuuden valvonnan, käyttöoikeudet, käytön ja lokien valvonnan, ohjelmistotuen, ylläpidon ja huollon turvallisuustoimenpiteet, varmuus- ja suojakopioinnin sekä häiriöraportoinnin.

Käyttöturvallisuustyön tulos on hallittu tietoaineiston käsittely, jossa tietojen käyttäjä on suojattu tietämättömyyden, osaamattomuuden, tahattomien virheiden ja vahinkojen se-



kä tahallisten tekojen aiheuttamilta tilanteilta, joissa käyttäjä voisi syyllistyä tietojen asiattomaan tai oikeudettomaan käsittelyyn.

Käyttöturvallisuuden periaatteet

Asiayhteys käyttäjän ja potilaan/asiakkaan välillä on aina sosiaali- ja terveydenhuollon salassa pidettävien tietojen käytön edellytys. Tahaton käyttö ilman asiayhteyttä estetään informoinnin, teknisten järjestelmien ja tehtäväkuvien selventämisen avulla.

Henkilötietoja sisältävän tietojärjestelmän käyttäjällä tulee olla henkilökohtainen ja yksilöivä käyttäjätunnus ja vain omassa tiedossa oleva salasana tai varmennekortti tai vastaava tunnistautumisväline.

Käyttöoikeuksien myöntämisen periaatteet on dokumentoitu ja niiden noudattamista valvotaan. Poikkeavien käyttöoikeuksien myöntämisprosessi on kuvattu ja myöntämiseen oikeutetut henkilöt on nimetty. Käyttöoikeuksien haltijoista pidetään rekisteriä, jota säilytetään 12 vuotta. Käytöstä kerätään lokitiedot, joiden avulla käyttö voidaan jäljittää yksilötasolle. Potilastietojen käsittelystä kerätään säädösten edellyttämät lokirekisterit, joita säilytetään 12 vuotta. Muita lokitietoja säilytetään kaksi vuotta.

Tietojärjestelmien käyttökoulutus ja tehtävien mukaisen käytön opetus kuuluu jokaisen käyttäjän perehdytykseen. Käyttäjien osaamista seurataan ja tulokset huomioidaan henkilöstön koulutuksessa.

Tietojärjestelmien muutokset, jotka saattavat vaikuttaa käyttöturvaan, tehdään suunnitellusti siten, että muutosten mahdolliset seurausvaikutukset ja riskit käytölle selvitetään. Riskien hallinnan suunnitelma hyväksytään ennen muutoksen tekemistä.

Palvelun toimittajalta, joka tuottaa kirjautumiseen, tunnistautumiseen tai muita käyttöturvallisuuteen liittyviä tietojärjestelmäpalveluita, edellytetään säännöllisiä raportteja palvelun valvonnasta, käytöstä, palvelutasosta ja palvelutason poikkeamista.