SUOMEN KUNTALIITTO
Sairaalapalvelut

Terveydenhuollon ATK-päivät 26. - 27.5.1997
Lahti, Kauppahotelli Grand

Kehittämispäällikkö Heikki Tähtinen
Suomen Kuntaliitto

Tietosuojan hyvä käytäntö

SUOMEN KUNTALIITTO
Sairaalapalvelut/HT

23.5.97

Terveydenhuollon XXIII atk-päivät, 26. - 27.5.97, LAHTI

TERVEYDENHUOLLON TIETOTURVAN JA TIETOSUOJAN TOTEUTUKSEN HYVÄN KÄYTÄNNÖN PERIAATTEITA

1. Lainsäädännön velvoitteita

Terveydenhuollon tietoaineistojen käsittelyyn vaikuttavat useat säädökset, mm. julkisuuslainsäädäntö, arkistolainsäädäntö, terveydenhuollon erityislainsäädäntö, tietosuojalainsäädäntö ja valmiuslainsäädäntö sekä lukuisat salassapitoa koskevat säännökset. Tietoaineiston yhtenäinen käsittely edellyttää, että aineiston arvioinnilla ja luokittelulla on yhtenäiset lähtökohdat, joita asettavat ennen kaikkea aineiston merkitys organisaatiolle ja sen suojaustarve sekä sovellettavat säädökset, määräykset, sopimukset ja vastaavat.

Tietosuojalainsäädäntö käsittää tietojen turvaamisen kaikki elementit; tietojen suojaaminen sekä luottamuksellisuuden, eheyden, saatavuuden ja käyttökelpoisuuden turvaaminen. Edelleen siihen kuuluu säännöksiä, jotka edesauttavat näiden toteutumista sekä määrittävät seuraamuksia tietiturvan vastaisesta menettelystä. Sen soveltamisalue on laaja, muun muassa kaikki käyttöoikeuksia määrittävät ja käyttöjä kirjaavat tiedostot ovat henkilörekistereitä. Henkilörekisterilaki on paljon muun ohella myös tietoturvallisuuslaki henkilötietojen osalta.

2. Tietoturvallisuus ja sen oleelliset osa-alueet

Tietojen turvaamisella tarkoitetaan muun muassa tietojen, järjestelmien ja palvelujen asianmukaista suojaamista sekä normaali- että poikkeusoloissa lainsäädännön sekä hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tietojen **luottamuksellisuutta, saatavuutta ja käyttökelpoisuutta** suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmallisten inhimillisten tekojen uhilta ja vahingoilta. Nämä osa-alueet tulee olla sisällytetty kattavasti koko organisaation toimintaan ja tietojenkäsittelyyn. Suurin riski organisaation turvallisuudelle syntyy siitä, että organisaation henkilöstö ei tiedä tai tiedosta aidosti, mitä tietoturva kokonaisuutena tarkoittaa.

. Tietoturva koskee kaikkia terveydenhuollossa salassapidettäväksi säädettyjä tietoja sekä niitä organisaatioon liittyviä tietoja, jotka on organisaation sisällä sovittu salaisiksi ja toiminnalle tärkeiksi siten, että niiden väärinkäyttö aiheuttaa organisaation toiminnalle haittaa. Terveydenhuollon tietoturvallisuus koskee kaikkia niitä toimintoja ja toimenpiteitä, joissa käsitellään terveydenhuollon asiakkaita sekä henhilöstöä koskevia henkilötietoja.

Tietojen turvaamiseen tulee osoittaa myös riittävät voimavarat.

3. Tietoturvallisuuden toimintavastuu

Suunnitelmallinen tietoturvallisuuden toteuttaminen vaatii varsinkin suurissa organisaatioissa sellaisia taitoja ja tietoja, joita organisaatiossa ei yleensä ole. Siksi on tarpeen nimetä **tietoturvallisuuden vastuuhenkilö (tietosuojapäällikön)**, joka vastaa tietoturvallisuuden kehittämisestä, ylläpidosta, koordinoinnista ja ohjaamisesta sekä tietoturvan **sisäisen tarkastustoiminnan** järjestämisestä. Tämä ei kuitenkaan poista palvelutoiminnasta vastaavien esimiesten vastuuta tietojenkäsittelyn turvaamisesta omalla toimialueellaan.

Tietoturvallisuusvastuu liittyy erottomana osana jokaisen toimintayksikön johdon toimintavastuuseen. Kukin esimies vastaa oman toimintayksikkönsä tehtäviin, tietojärjestelmiin ja tietorekistereihin liittyvän tietoturvan totuttamisesta ja sen valvonnasta. Henkilöstön tietoturvaan liittyvästä koulutuksesta ja perehdyttämisestä vastaa omalta osaltaan yksikön esimies.

Johdon on selkeästi määriteltävä tietoturvan taso ja päätettävä organisaatiossa noudatettavasta tietoturvapolitiikasta. Tietoturva on ennen kaikkea asennekysymys. Mitkään ohjeistukset ja kontrollit eivät takaa tietoturvallisuutta, ellei sen merkitystä tiedosteta ja ellei sillä ole johdon ehdotonta tukea. Kun henkilöstö tiedostaa aidosti tietoturvan tavoitteet ja merkityksen, muuttuu toiminta ja toimintatavat. Tietoturva on kaikkien vastuulla ja jokaisen on tunnettava sen vaatimat toimenpiteet omassa toiminnassaan. Ihmiset eivät osaa salata tietoa, jota eivät tiedä salassa pidettäväksi. Siksi johdon tulee tehdä selväksi jokaiselle työntekijälle se, mitä tietoa suojataan, miksi suojataan ja miten suojataan.

Hallinnollisella turvallisuudella tarkoitetaan niitä toimenpiteitä, joilla määrätään noudatettavista periaatteista ja toimintalinjoista yleensä. Tietoturvallisuus on pohjimmaltaan hallinnollinen ongelma, jonka ratkaisu turvallisuus-, toipumis- ja valmiussuunnitelmien avulla edellyttää muun muassa vastuiden ja organisaation määrittelyä, tietovarantojen kartoitusta ja luokitusta, riskien arviointia ja hallintaa, ohjeistusta, neuvontaa ja koulutusta sekä valvontaa ja tarkastusta.

4. Terveydenhuollon asiakastietojärjestelmien käyttöympäristö

Potilaan asemasta ja oikeuksista annetun lain mukaan terveydenhuollon ammattihenkilön ja kunkin terveydenhuollon toimintayksikön on laadittava ja säilytettävä potilasasiakirjat siten kuin sosiaali- ja terveysministeriö tarkemmin määrää (12§). Samassa laissa säädetään, että potilasasiakirjoihin sisältyvät tiedot ovat salassapidettäviä (13 §).

Asiakkaan hoidosta vastaava **palvelun tuottava organisaatio** on hyvän hoidon periaatteiden ja lainsäädännön velvoittamana vastuullinen dokumentoimaan tietoa asiakkaasta. Hoidosta vastannut organisaatio vastaa syntyneen dokumentin tai asiakasasiakirjan käytöstä, säilyttämisestä, arkistoinnista ja salassapidosta sekä myös tiedon siirrosta muille hyväksytyille käyttäjille.

Terveydenhuollon toimintayksikössä työskentelevä tai sen tehtäviä suorittava henkilö ei saa ilman asiakkaan kirjallista suostumusta antaa sivullisille potilasasiakirjoihin sisältyviä tietoja. Salassapito liittyy tietojen luottamuksellisuuteen, mikä tarkoittaa, että tietojen on määrä olla vain tiettyjen, sovittujen henkilöiden käytettävissä ja sen paljastuminen ulkopuoliselle vahingoittaa tietosuojaa.

Sen estämättä, mitä jäljempänä on sanottu asiakkaan tietojen turvaamisesta on asiakaan tietojen hyväksikäyttö sallittua asiakkaan luvalla. Asiakkaan luvan saanti ja kirjaaminen edellyttää, että asiakkaalle on ymmärrettävästi kerrottu luovutettavien tietojen tuleva käyttötarkoitus. Myöskin viranomainen voi lainsäädännössä mainituissa tilanteissa myöntää luvan asiakkaan tietojen käyttämiseen. Lisäksi järjestelmästä tulee voida tuottaa lakisääteiset ilmoitukset viranomaisille.

Asiakastietojärjestelmien käytössä ja niiden tietosuojan järjestämisessä keskeisiä tarkemmin määriteltäviä osapuolia ovat:

- asiakas (asukas, yksilöasiakas, perhe, ryhmä, väestävastuuasiakas, potilas),
- hoitosuhde,
- toimintayksikkö (erikoisala, hoitoyksikkö, organisaation osa),
- käyttäjä (järjestelmän käyttäjä, henkilökunta, yksikkö),
- työtehtävä (tehtävät, joista käyttäjän työkokonaisuus muodostuu),
- tiedot (tietoryhmät), jotka kuvaavat asiakasta, hänelle annettuja palveluja ja muita suoritteita,
- käyttöoikeus tietoihin. Käyttöoikeuden saannin peruste voi olla:
  - lupa (potilaan tai viranomaisen lupa tietojen saamiseksi),
  - hoitosuhde (potilaan ja toimintayksikön tai potilaan ja käyttäjän välinen suhde),
  - lakiin perustuva oikeus tai velvollisuus.

Asiakastietojen käytöstä ja tietojen suojaamisen hallinnosta ja järjestämisestä vastaa laitoksen johtajaylilääkäri/johtava lääkäri tai vastaava, jonka tulee huolehtia tietosuojan käytännön järjestämisestä, käyttöoikeuksien antamis- ja poistamismenettelystä, toiminnan riittävästä ohjeistamisesta ja valvonnasta. Hän vastaa hoitoa koskevia toimintoja ja asiakastietoja koskevien säännösten ja määräysten noudattamisesta sekä myös laitoskohtaisista tietosuojaohjeista sekä niiden soveltamisesta.

5. *Asiakastietojärjestelmien käyttöturvallisuusvaatimukset*

Käyttöturvallisuudella tarkoitetaan henkilöstölle ja fyysiselle käyttöympäristölle asetettavia turvallisuusvaatimuksia sekä asiakastietojärjestelmien turvallisia käyttöperiaatteita ja varsinaisen tietojenkäsittelyn turvallisuuteen vaikuttavien tapahtumien hallintaa ja valvontaa sekä toiminnan jatkuvuuden turvaamiseen liittyvien menetelmien käyttöä. Käyttöturvallisuutta koskevat määräykset ja toimenpiteet koskevat soveltaen ja skaalautuvasti niin yksittäisen mikron kuin laajemman tietojärjestelmän tai tietoverkon avulla käsiteltävien henkilörekistereiden käyttöä.

5.1 Henkilöstövaatimukset

Henkilöstöturvallisuustoimenpiteet ulottuvat vakinaisen ja tilapäisen henkilökunnan virka- ja työsuhteiden alkamis- ja päättymistilanteiden, tehtäväsiirtojen ja sijaisjärjestelyjen ohella myös vierailijoihin sekä ulkopuolisten palvelujen ostoon hanke-, huolto-, siivous- tms. sopimusten puitteissa. Henkilöiden tehtävämäärittelyissä tulee määritellä myös tietoturvaan liittyvät oikeudet, velvollisuudet ja vastuut.

Henkilöiden tehtävämäärittelyissä ja tehtävien suorituksen valvonnassa tulee ottaa huomioon myös tietoturvaan liittyvät näkökohdat ja tehtävät kuten:

- ❒ jokainen on osaltaan vastuussa tehtäviinsä liittyvästä tietoturvasta ja siihen liittyvästä luottamuksellisuudesta, joka tulee mainita jo työsopimuksessa ja toimenkuvassa,
- ❒ uudelle työntekijälle annetaan hänen tehtäväänsä vastaavat käyttöoikeudet sekä perehdytetään hänet toimimaan organisaation tietoturvaperiaatteiden mukaisesti. Poislähtevän työntekijän käyttöoikeudet peruutetaan välittömästi,
- ❒ asiantuntevien varahenkilöiden määrittely ja kouluttaminen,
- ❒ käyttöoikeuksien määrittely kullekin henkilölle työtehtävien ei organisaatioaseman mukaan,
- ❒ tietoturvallisuushäiriöiden rekisteröinti, raportointi ja selvittäminen,
- ❒ työsuhteen päätyttyä huolehditaan, että henkilö palauttaa avaimet, henkilötunnisteet ja henkilökortin, joka hävitetään,
- ❒ kriittisten tehtävien tehtäväkuvausten dokumentointi niin, että joku toinen pystyy niiden avulla suorittamaan ko. tehtävän.

5.2 Fyysiset turvallisuusvaatimukset

Tietojärjestelmien ja tiedostojen fyysinen turvallisuus tulee toteuttaa siten, että tietosuojattavien tietojärjestelmien ja tietojen luvaton käyttö, käsittely ja haltuunotto voidaan estää.

Fyysinen tietoturvallisuus edellyttää, että

- ❒ läpi organisaation määritellään tietosuoja-alueet ja järjestetään niille pääsyn sekä kulunvalvonta ja kontrollointi,
- ❒ kriittisille tietojärjestelmille ja tiedostoille määritellään fyysisen suojauksen tasot ja niiden edellyttämät tilat ja toimenpiteet,
- ❒ henkilökunta varustetaan näkyvin henkilötunnistein,
- ❒ vierailijoilla tulee olla kulkuun oikeuttava näkyvä tunniste,
- ❒ konesaliin on pääsy vain käyttöhenkilöstöllä ja päätteitä sisältäviin tiloihin vain niitä käyttävällä henkilöstöllä sekä kulunvalvonta näihin tiloihin on järjestetty,
- ❒ erilaisten vaurioiden hallinta ja niistä elpyminen on järjestetty; järjestelmän kahdennus, varajärjestelmät, elpymisen aikarajat, tiedotus vaikutuksista.

5.3 Järjestelmän hankinta- ja ylläpitovaatimukset

Ennen tietojärjestelmien ja ohjelmistojen sekä laitteiden hankintaa tulee määritellä niiltä vaadittavat tietoturvaominaisuudet. Niissä on otettava huomioon myös järjestelmän laajennettavuus, riittävä tehokkuus sekä yhteensopivuus muiden järjestelmien kanssa.

5.4 Ohjelmistoturvallisuus

edellyttää, että

- ❒ ohjelmat hankitaan luotettavalta toimittajalta,
- ❒ uuden ohjelman soveltuvuus systeemikokonaisuuteen on varmistettu,
- ❒ käytettävät ohjelmat ovat laillisia, tarkastettuja, testattuja ja viruksista vapaita,
- ❒ organisaatioon ei saa tuoda eikä ottaa käyttöön ohjelmia, joita ei ole hyväksytty ja tarkastettu,
- ❒ ohjelmistot rekisteröidään,
- ❒ sovellutusohjelmistojen tekeminen ja ylläpito on keskitetty, yksityiskohtaisesti dokumentoitu ja sovellutusten toiminta tulee olla tarkastettavissa ja testattavissa,
- ❒ järjestelmädokumenttien turvallinen säilytys on hoidettu ja varmistettu,
- ❒ ohjelmistot säilytetään lukituissa tiloissa ja tärkeinpien ohjelmien varmuuskopiot säilytetään erillisissä tiloissa kassakaappivarmistettuna,
- ❒ kaikista räätälöidyistä ja organisaatiokohtaisista ohjelmista on käsikirjat, lähdekoodit ja yksityiskohtaiset järjestelmäkuvaukset,
- ❒ huolehditaan ja varmistetaan sopimuksin, että toimittajilla on riittävä ja asianmukainen valmius ylläpitää ja huoltaa ohjelmistoja.

5.5 Laitteistoturvallisuudessa

ja laitteiston huollossa ja kunnossapidossa on otettava huomioon seuraavat seikat:

- ❒ hankittavat laitteet sopivat systeemiarkkitehtuuriin ja laiteympäristöön,
- ❒ laitteiden sijainti lukituissa tiloissa: avaaminen ja sulkeminen,
- ❒ kriittisten laitteiden varajärjestelmästä on huolehdittu,
- ❒ tärkeiden laitteiden tasainen energiansaanti on järjestetty,
- ❒ keskeisten laitteiden varaosien saanti on turvattu ja vaihtoehtoisten laitteiden käytettävyys on testattu,
- ❒ huoltosopimuksilla varmistetaan, että ainoastaan hyväksytyllä huoltohenkilöllä on pääsyoikeus laitteisiin ja ohjelmistoihin. Mikäli mahdollista huollon tulee tapahtua valvotuissa olosuhteissa,
- ❒ jos käytetään etähuoltoa, on sen valvonta ja tietoturva varmistettava:huollon oikeudellisuus varmistetaan ennen kytkeytymistä järjestelmään esimerkiksi käynnistämällä se systeemistä käsin,
- ❒ henkilörekisterejä ja niitä käsitteleviä ohjelmistoja sisältävien tietovälineiden ja laitteiden siirtämisestä huollettavaksi organisaation ulkopuolelle tulee olla selkeät sopimukset ja ohjeet. Luvaton käyttö tulee estää tarvittaessa salasanoin tai salakirjoittamalla tiedot.

5.6 Käytönaikaisessa tietoturvallisuudessa

on otettava huomioon seuraavia asioita:

- ❒ laitteistojen pääsynvalvonta on toteutettu vähintään käyttäjätunnus /salasanamenettelyin,
- ❒ ohjelmien pääsynvalvonta on toteutettu vähintään käyttäjätunnus /salasanamenettelyin,
  - ◆ huolehditaan salasanoista ja niiden uusimisesta riittävän usein ja säännöllisesti. Järjestelmä voi pakottaa käyttäjää muuttamaan tunnustaan sopivin määräajoin. Jokaiselle salasanalle annetaan **määrätty voimassaoloaika**, jonka kuluttua järjestelmä katkaisee käyttöoikeuden tai se peruutetaan,
- ❒ kaikki tärkeimpien ohjelmien käyttötapahtumat kirjataan suojattuun käyttölokiin: määritellään tehtävien, valtuuksien ja vastuiden mukaisesti kohdennetut käyttöoikeudet sekä niiden edellyttämät tapahtuma- ja käyttäjäkirjaukset käyttäjälokiin,
- ❒ asiakaskohtainen tietojen käsittely toimenpiteittäin tulee olla jälkikäteen tarkastettavissa joko erillisestä rekisteristä ja/tai ko. asiakkaan tiedoista,
- ❒ uutta tekstiä syötettäessä ja korjausmenettelyä käytettäessä syntyvät **uudet tiedot** varustetaan päivämäärämerkinnällä sekä tiedon oikeellisuudesta vastaavan identifiointitiedolla,
- ❒ asiakastietoihin tehdyt **muutokset ja korjaukset** on tallennettava asiakkaan tietoihin siten, että niistä selviää asiakas ja häntä koskeva muutettava tieto, muutospäätöksen tekijä, muutoksen tai korjauksen syy, tekijä, ajankohta, työpiste sekä vastaavasti otteen ottaminen,

- ❒ näytöt ja muut tulosteet tulee rakentaa siten, että vain ko. **työtehtävissä tarvittavat tiedot** ovat näkyvissä.
- ❒ käsittelyn luotettavuus ja käyttövarmuus turvataan huolehtimalla ohjelmistojen käytön aikana automaattisesti tallentamista varmuuskopioista, niiden säilytyksesta ja hävittämisestä sekä tapahtumien oikeasta kirjautumisesta keskeytystilanteissa,
- ❒ muistialueen tyhjentäminen siten, ettei se sisällä suojattavaa jäännöstietoa. Esimerkiksi käyttöjärjestelmien ja varusohjelmien tekemät varmuuskopiot tulee muistaa hävittää,
- ❒ siltä varalta, että pääte unohtuu päälle, kun käyttäjä poistuu paikalta, ohjelmoidaan **näytön tyhjentyminen** määrätyn ajan jälkeen. Myös päätteen muisti tyhjentyy tällöin ja yhteys ao. asiakkaan tietoihin purkautuu,
- ❒ ohjelma- ja tiedonsiirtovirheiden käsittely käyttöjärjestelmän ja virheitä tunnistavan ja korjaavan protokollan puitteissa.

5.7 Tietoaineistojen ja systeemidokumenttien hallinta

edellyttää, että

- ❒ aineistot säilytetään lukituissa tiloissa,
- ❒ aineistot on varustettava tunnisteella,
- ❒ tulostuneen aineiston oikeellisuus on tarkastettava,
- ❒ aineistojen pakkaus ja kuljetus on järjestettävä turvallisesti,
- ❒ aineistojen hävitys hoidetaan turvallisesti,
- ❒ käytöstä poistetut rekisteritaltiot tyhjennetään ja uudelleenformatoidaan tai, jos se ei ole mahdollista, taltiot hävitetään.

5.8 Tietoliikenneturvallisuus

edellyttää, että

- ❒ tietoverkon laitteiden ja yhteyksien sekä virhetilanteiden hallinta on järjestetty,
- ❒ lähettäjän ja vastaanottajan sekä viestin sisällön todentaminen ja kiistämättömyys on järjestetty,
- ❒ tietoverkot on rakennettu ja suojattu siten, että luvattomat käyttäjät eivät pääse käsiksi välitettäviin tietoihin,
- ❒ liittymästä saadaan toteutettua käyttäjän ohjaamana vain sallittuja palveluja,
- ❒ on varauduttu käyttämään tarvittaessa vaihtoehtoisia tiedonsiirtotapoja,
- ❒ huolehditaan ja varmistutaan siitä, että yhteys kytkeytyy ja sanoma lähetetään vain tarkoitettuun liittymään,
- ❒ varaudutaan ottamaan käyttöön salausalgoritmit, sähköinen allekirjoitus ja muut sanoman suojaustoimenpiteet.

5.9 Virusten torjunta

- ❒ virustorjunta on ohjeistettu ja käytössä on virustorjunnan asiantuntijoita sekä ohjelmistoja,
  - ◆ ennakoiva viruspolitiikka,
  - ◆ virusten ehkäisy,
  - ◆ virusten havaitseminen,
  - ◆ toimenpiteet viruksen ilmestyessä.

Atk-järjestelmille asetettavien vaatimusten kannalta tärkeää on ensisijaisesti **organisaation sisäisen** tietoturvallisuuden ja tietosuojan järjestäminen, koska uuden tekniikan vaikutukset näkyvät eniten näillä alueilla.

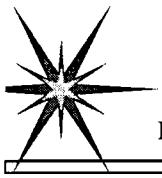
TIETOSUOJAN HYVÄN KÄYTÄNNÖN PERIAATTEITA

Suomen Kuntaliitto/Heikki Tähtinen

Lainsäädäntö

- Arkistolainsäädäntö
- Julkisuuslainsäädäntö
- Salassapitosäädökset
- Terveydenhuollon erityislainsäädäntö
- Tietosuojalainsäädäntö
- Valmiuslainsäädäntö

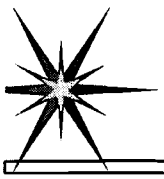
Suomen Kuntaliitto/Heikki Tähtinen



HENKILÖTIETOLAKI

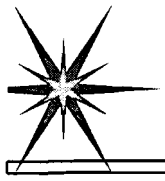
Laki yksityisyyden suojasta henkilötietojen käsittelyssä

- ✓ Henkilötietojen käytöstä säädettävä aina lailla
- ✓ Tietojenkäsittelyn yleiset edellytykset
  - ◆ Suostumus
  - ◆ Käyttötarkoitusvaatimus
  - ◆ Yhteysvaatimus
  - ◆ Tarpeellisuusvaatimus
  - ◆ Virheettömyysvaatimus

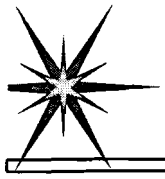


Henkilötietolaki

- ❒ Henkilötunnuksen käyttö
- ❒ Henkilötietojen luovuttaminen
- ❒ Tieto tiedon rekisteröinnistä
- ❒ Tarkastusoikeus
- ❒ Virheen oikaisu
- ❒ Tietojen suojaaminen
- ❒ Hävittäminen
- ❒ Arkistointi



- Tietoturva -- Tietoriskien minimointi
- Tietoriski -- Haittaa aiheuttava uhka
- Tietosuoja -- Henkilön:
  yksityisyyden
  etujen
  oikeuksien suojeleminen



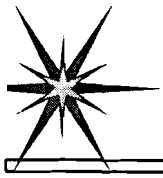
TIETOSUOJAN OSA-ALUEITA

Tiedon

- Luottamuksellisuus / Julkisuus,Salassapito
- Saatavuus
- Käyttökelpoisuus

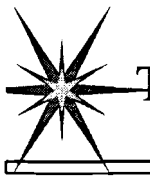
HALLINNOLLINEN TURVALLISUUS

- Toimintavastuut
- Tietoturvallisuuskäytäntö
- Tietoturvapolitiikka
- Tietoturvallisuussuunnitelma
- Toipumissuunnitelma



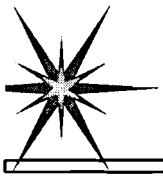
TOIMINTAVASTUUT

- Rekisterinpitäjä
- Tietosuojapäällikkö
- Toimintayksikön esimies
- Yksikön esimies
- Henkilöstö



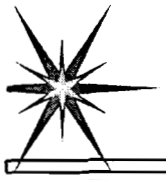
TIETOTURVALLISUUSKÄYTÄNTÖ

- Periaatepäätös noudatettavasta tietoturvallisuuspolitiikasta
- Tietoturvallisuuspolitiikan luominen
- Politiikan ohjeistaminen
- Toiminnan organisointi
- Seuranta
- Politiikan uusiminen



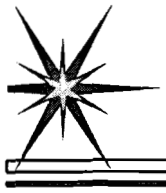
TIETOTURVAPOLITIIKKA

- Tietoturvallisuuden tasojen määrittely
- Riskien tunnistaminen ja hallinta
- Toimintapolitiikka
- Virhe- ja häiriötilanteiden hallinta
- Henkilöstön valmiudet



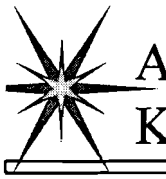
TIETOTURVALLISUUSSUUNNITTELU

- Tietojärjestelmien turvallisuusluokittelu
- Tietokantojen turvallisuusluokittelu
- Tietojärjestelmiin pääsy
- Tietokantoihin pääsy
- Tietojenkäsittelytiloihin pääsy
- Rikkomusten seuranta ja vaikutusten arviointi



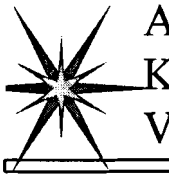
TOIPUMISSUUNNITELMA

- Tärkeät toiminnot tunnistettu ja kuvattu
- Sallitut keskeytysajat määritelty
- Varajärjestelmät ohjeistettu
- Toimintojen uudelleenkäynnistys
- Yhteyshenkilöt
- Koulutus ja testaus ajoitettu



ASIAKASTIETOJÄRJESTELMÄN KÄYTTÖYMPÄRISTÖ

- Asiakas
- Asiakasuhde/Hoitosuhde
- Toimintayksikkö
- Käyttäjä
- Työtehtävä
- Tiedot
- Käyttöoikeus



ASIAKASTIETOJÄRJESTELMÄN KÄYTTÖTURVALLISUUS-VAATIMUKSET

- Henkilöstövaatimukset
- Fyysiset turvallisuusvaatimukset
- Järjestelmien hankinta- ja ylläpitovaatimukset
- Ohjelmistoturvallisuus
- Laitteistoturvallisuus
- Käytön aikainen tietoturvallisuus
- Tietoaineistojen ja systeemidokumenttien hallinta
- Tietoliikenneturvallisuus
- Virusten torjunta