Käsitelty yhteistyötoimikunnassa 3.11.2016
Hyväksytty yhtymähallituksessa 29.11.2016

KEMI-TORNIONLAAKSON KOULUTUSKUNTAYHTYMÄ LAPPIAN TIETOTURVAPOLITIIKKA

Vastuu Kemi-Tornionlaakson koulutuskuntayhtymä Lappian toimivuudesta on sen ylimmällä johdolla. Kuntayhtymän toiminta ja palvelut ovat yhä enenevässä määrin riippuvaisia tietotekniikkapalveluiden keskeytyksettömästä saatavuudesta ja niiden turvallisesta toiminnasta. Tietotekniikan hyödyntäminen ja niin tietotekniikan kuin yleisempäänkin tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan kuntayhtymän toimintakykyyn merkittävällä tavalla. Myös lainsäädäntö asettaa omat velvoitteensa tietoturvallisuudesta huolehtimiselle.

Tietoturvapolitiikka on kuntayhtymän johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot kuntayhtymässä. Tietoturvapolitiikka annetaan tiedoksi kaikille kuntayhtymän jäsenille sekä Lappian käytössä olevien tietojärjestelmien käyttäjille ja heidän tulee toimia sen mukaisesti. Politiikkaa tarkennetaan tietojen käsittelyn säännöissä ja ohjeissa.

Tiedon turvaaminen on oleellinen osa kuntayhtymän toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja kuntayhtymässä tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua, varautumista erilaisiin uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin kuntayhtymän omien kuin sen piirissä käsiteltävien sidosryhmienkin tietojen käsittelyyn.

1. TAVOITTEET

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä (ks. LIITE 1, Määritelmät). Kuntayhtymän tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen.

Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan. Kuntayhtymän kunkin yksikön perusluonne ja mahdolliset tarpeet turvallisuuden tehostamiseen tulee ottaa huomioon. Tietojen turvaamisesta tulee erityisesti huolehtia yksiköissä, jotka käsittelevät runsaasti luottamuksellista tai muuten turvaluokiteltua tietoa. Tietojen turvaamisessa huomioidaan omina osa-alueinaan valtionhallinnon käytännön mukaan hallinnollinen, henkilöstö-, fyysinen, tietoaineisto-, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuus.

Tietoturvallisuustyö on tietojen turvaamiseksi tehtävää jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa. Sillä pyritään ennalta ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen. Normaaliajan tietojen käsittelyn turvaamisen osana kuntayhtymä varautuu myös häiriö- ja poikkeusoloihin siten, että toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa.

Kuntayhtymän tietoturvallisuudesta huolehditaan kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti sekä noudattaen valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia (ks. LIITE 2, Kuntayhtymän tietoturvallisuutta ohjaavia säädöksiä, suosituksia ja ohjeita).

2. TIETOTURVAN ORGANISOINTI JA VASTUUT

Tietoturvallisuus on koko Kemi-Tornionlaakson koulutuskuntayhtymä Lappian yhteinen asia. Kuntayhtymän oppilaitosten yleisestä tietoturvapolitiikasta päättää kuntayhtymän hallitus. Yleistä hallintoa johtaa kuntayhtymän johtaja. Osana kokonaisvastuutaan kuntayhtymän johtaja ja kuntayhtymän hallitus vastaavat tietoturvallisuuden toteutumisesta ja tarvittavien edellytyksien luomisesta.

Tietohallintojohtajan ohjauksessa toimiva tietoturvatyöryhmä valmistelee ja ohjaa kuntayhtymän tietoturvallisuuden käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa kuntayhtymän hallituksen hyväksymien tietoturvaperiaatteiden mukaisesti.

Kuntayhtymässä on tietohallintojohtajan esityksestä kuntayhtymän johtajan nimeämä tietoturvavastaava ja hänen varahenkilönsä. Tietoturvavastaava vastaa tietoturvallisuuden seurannasta, raportoinnista ja kehittämishankkeiden toteutuksesta sekä valmistelee niitä yhdessä tietoturvatyöryhmän kanssa.

Tietoteknisestä tietoturvasta kuntayhtymässä vastaa IT Lappia.

Yksiköiden johtajat, tietojärjestelmien vastuuhenkilöt, IT-tukihenkilöt ja tekniset asiantuntijat vastaavat kukin omalta osaltaan tietoturvan toteutumisesta yksiköissään ja tietojärjestelmissään.

Yksiköt varautuvat oman ympäristönsä tietoturvallisuuden toteuttamisen kustannuksiin omissa toimintasuunnitelmissaan. Tietoturvallisuuden toteuttamista yksiköissä ja niiden tietojärjestelmissä ohjaa ja valvoo kullekin yksikölle nimettävä vastuuhenkilö.

Jokainen kuntayhtymän tietoja käsittelevä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan.

Tietoturvallisuuden toteuttaminen on jatkuvaa laaja-alaista toimintaa, jota ei voida asettaa vain muutaman vastuuhenkilön kannettavaksi, vaan johon tarvitaan tiivistä ja rakentavaa yhteistyötä kaikkien kuntayhtymään kuuluvien henkilöiden ja ryhmien kesken. Tietoturvallisuuden toteuttamiseen ja valvontaan osallistuu jokainen kuntayhtymän henkilökuntaan ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan. Tietoturvallisuuden ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä turvallisuusvastuuhenkilöitä.

Tietoturvallisuuden vastuujärjestelyn tulee seurata kuntayhtymän toiminnan mahdollisia muutoksia. Monet alla mainituista vastuista voivat kuulua samankin henkilön tehtäviin ja vastuisiin. Olennaista on, että näiden tehtävien hoito on järjestetty, myös varamiesten osalta.

Kuntayhtymän johtajan, rehtorin ja/tai hallituksen vastuut:

- tietoturvallisuuden toteutuminen osana kokonaisturvallisuutta
- tietoturvallisuuden resursointi ja organisointi
- tietoturvallisuuden päälinjaukset
- toimintojen tietoturvallisuuspriorisointi
- tietoturvallisuuden seuranta.

Tietoturvatyöryhmän tehtävänä on:

- valmistella ja ohjata kuntayhtymän tietoturvallisuuden käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa kuntayhtymän johtoryhmän ja hallituksen hyväksymien tietoturvaperiaatteiden mukaisesti yhdessä tietoturvavastaavan kanssa
- uudistaa tarvittaessa kuntayhtymän tietoturvaperiaatteet
- huolehtia, että kuntayhtymällä on jatkuvuussuunnitelmat infrastruktuurin ja keskeisten järjestelmien osalta poikkeusoloja varten
- huolehtia riskianalyysin tekemisestä
- edustaa kuntayhtymän eri tahojen tietoturvallisuusnäkemyksiä
- huolehtia henkilöstön ja opiskelijoiden turvallisuustietoisuuden lisäämisestä ja tietoturvallisuuskoulutuksen suunnittelusta
- huolehtia tietoturvallisuuden toteutumisesta ostetuissa IT-palveluissa
- raportoida ylimmälle johdolle tietoturvallisuudesta
- päättää toimenpiteistä merkittävissä ja vakavissa tietoturvapoikkeamissa
- tulkita tietoturvaohjeita ja -määräyksiä epäselvissä tilanteissa
- tehdä kuntayhtymän johtajalle, rehtorille ja yksiköiden esimiehille kuntayhtymän tietoturvallisuutta koskevia ehdotuksia ja aloitteita

Tietoturvavastaavan tehtävänä on:

- valmistella tietoturvallisuuden kehittämishankkeita yhdessä tietoturvallisuuden johtoryhmän kanssa
- vastata tietoturvallisuuden kehittämishankkeiden toteutuksesta
- vastata tietoturvallisuuskoulutuksen järjestämisestä
- tiedottaa tietoturvallisuusasioista ja -ongelmista
- osallistua turvallisuusperiaatteiden määrittelyyn
- avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa
- kehittää ehdotuksin tietoturvallisuutta
- järjestää tietoturvallisuutta koskeva seuranta
- raportoida ylimmälle johdolle tietoturvallisuudesta
- toimia tietoturvatyöryhmän sihteerinä
- tehdä muut tietoturvatyöryhmän hänelle antamat tehtävät.

IT Lappian tehtävänä on:

- huolehtia teknisestä tietoturvasta kuntayhtymässä
- vastata kuntayhtymän tietoliikenneverkon turvallisuudesta
- huolehtia kuntayhtymän keskitetystä varmuus- ja suojakopioinnista
- järjestää tekniseen tietoturvaan liittyvää koulutusta ylläpitäjille

- neuvoa tekniseen tietoturvaan liittyvissä kysymyksissä.

IT Lappian sisällä toimii tietohallintojohtajasta, tietototurvavastaavasta ja käsiteltävän asian vastuualueeseen kuuluvasta IT-suunnittelijasta muodostuva reagointiryhmä, jonka tehtävänä on:

- reagoida nopeaa toimintaa vaativiin tietoturvapoikkeamiin, koordinoida tarvittavat toimenpiteet ja pyrkiä mahdollisuuksien mukaan estämään tietoturvapoikkeaman laajeneminen
- saattaa tietotekninen struktuuri kuntoon tietoturvapoikkeaman jälkeen ja tuottaa oikeata informaatiota poikkeamatilanteesta.

Yksikön johtajan/esimiehen tehtävänä on:
- yksikkönsä tietoturvallisuuden ja siihen liittyvien kehittämistoimenpiteiden resursointi ja toimeenpano asetettujen tietoturvallisuustavoitteiden mukaisesti
- seurata yksikkönsä tietoturvallisuuden ohjeiden noudattamista
- toimia yksikkönsä tietoturvallisuuden yhteyshenkilönä tai nimetä yhteyshenkilö
- nimetä yksikkönsä omistamien tietojärjestelmien vastuuhenkilöt ja
- raportoida tietoturvallisuudesta ja siihen kohdistuvista häiriöistä.

Tietoteknisten asiantuntijoiden (mm. järjestelmien ylläpitäjien, suunnittelijoiden, ohjelmoijien) tehtävänä on:
- soveltaa ja toteuttaa kuntayhtymän tietoturvallisuusperiaatteita omaa erikoisasiantuntemusta hyödyntäen
- vastata tietoturvallisuustoimenpiteistä omalla alueellaan
- noudattaa hyvää tietoturvallisuustapaa ja
- raportoida tietoturvallisuudesta ja siihen kohdistuvista häiriöistä.

Tietopalveluista ja asiakirjahallinnosta vastaavien tehtävänä on:
- toimeenpanna tietoturvallisuus tietopalveluissa ja asiakirjahallinnossa hyvän tiedonhallintatavan ja tietoturvallisuustavan mukaisesti.

Tietojärjestelmän omistajan tehtävänä on:
- vastata henkilörekisteri- ja tietojärjestelmäselosteista
- vastata tietojärjestelmän ja sen tietojen suojauksesta, käyttöoikeuksista sekä varmuus- ja suojakopioinnista
- toimeenpanna tietojärjestelmäänsä liittyvät turvallisuustoimenpiteet ja kehittää niitä
- seurata tietoturvallisuutta tietojärjestelmässä ja
- raportoida tietoturvallisuudesta ja siihen kohdistuvista häiriöistä.

Sovelluksen tai palvelun vastuuhenkilön/pääkäyttäjän tehtävänä on:
- ylläpitää henkilörekisteri- ja tietojärjestelmäselosteet ja pitää ne rekisterissä olevien saatavilla
- ylläpitää turvallisuusmenettelyt tietojärjestelmässä
- seurata järjestelmän toimintaa tietoturvallisuuden kannalta
- varautua poikkeaviin tapahtumiin ja niiden vaatimiin vastatoimenpiteisiin
- raportoida turvallisuutta vaarantavista tapahtumista ja häiriöistä.

Yksiköiden IT-henkilöiden ja tietoturvavastaavien tehtävänä on:
- ylläpitää ja valvoa vastuullaan olevien järjestelmien tietoturvallisuutta kuntayhtymän tietoturvallisuuden yleisohjeistuksen mukaisesti
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä

Loppukäyttäjien tehtävänä on:
- tuntea tietoturvallisuudesta annetut ohjeet ja noudattaa niitä
- osallistua heille suunnattuun tietoturvakoulutukseen sekä
- raportoida havaitsemistaan ongelmista, uhkista ja ohjeiden vastaisista menettelyistä.

Konsulttien ja palveluyritysten tehtävänä on:

- noudattaa hyvää tietojenkäsittely- ja tietoturvallisuustapaa
- ylläpitää ja valvoa kuntayhtymään liittyvässä toiminnassaan valtionhallinnon tietoturvallisuuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvallisuutta
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä.

Tietoturvallisuusvastuita on myös muilla keskeisillä henkilöryhmillä kuten

- hankintoja hoitavilla henkilöillä
- henkilörekisterien hoitajilla
- sopimus- ja kiinteistöhallinnon henkilöillä.

Sisäinen valvonta

Kuntayhtymässä suoritetaan sisäistä valvontaa johdon johdolla ja alaisuudessa. Valvontajärjestelmä on kokonaisuus, jonka muodostavat toimivasta johdosta riippumaton ulkoinen valvonta ja osana operatiivista johtamista toimiva sisäinen valvonta.

Sisäisellä valvonnalla tarkoitetaan kaikkia niitä toimenpiteitä ja menetelmiä, joilla pyritään toiminnan tuloksellisuuden ylläpitämiseen ja edistämiseen, sekä kirjanpidon, palkanlaskennan, maksuliikenteen ja muiden tietojärjestelmien luotettavuuden varmistamiseen. Edelleen sisäinen valvonta pyrkii erehdysten, virheiden ja väärinkäytösten ehkäisyyn ja toteamiseen sekä varojen huolellisen ja taloudellisen hoidon turvaamiseen.

Sisäisen valvonnan keinoin varmistetaan myös, että kuntayhtymän toiminnan tarkoitus ja asetetut tavoitteet on saatettu tiedoksi organisaation kaikille tasoille ja että asetettujen tavoitteiden saavuttamista seurataan.

Sisäinen valvonta on osa kuntayhtymän operatiivista johtamista ja riskien hallintaa.
Sisäisestä valvonnasta on annettu erillinen ohje.

3. TOTEUTUSKEINOT

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan niihin sisältyvillä käyttösäännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn koulutuksella ja tiedotuksella.

Tietojen turvallisesta käsittelystä solmitaan sopimukset myös kuntayhtymän tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppanien kanssa.

Tarvittavan suojaustason (perustaso / tehostetut tasot) ja tarvittavien suojaustoimien määrittäminen tehdään riskikartoituksissa. Niissä kartoitetaan ja luokitellaan kuntayhtymän ja yksiköiden merkittävät tietoaineistot ja tietojärjestelmät, näihin kohdistuvat uhat sekä arvioidaan menetyksen suuruus uhan toteutuessa. Riskikartoitukset toistetaan
määräajoin ja muutosten yhteydessä.

Tietoturvapolitiikan ja riskikartoituksen pohjalta muutetaan tarvittaessa tietoturvaohjeistusta ja tehdään erillinen kehittämissuunnitelma. Suunnitelmassa otetaan kantaa, mitkä riskit edellyttävät toimenpiteitä ja mitkä taas ovat toiminnan ja lainsäädännön vaatimusten puitteissa hyväksyttäviä.

Tietoturvallisuus sisältyy kuntayhtymän toimintaprosessien kehittämiseen ja toiminnan ja yksiköiden vuosisuunnitteluun. Perustaso määritellään kuntayhtymän tietoturvaohjeissa.

Henkilökuntaa ohjeistetaan tutustumaan tietoturvaohjeisiin. Opiskelijoille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin kuntayhtymän henkilöstön tietoturvallisuustietoisuutta lisätään tiedottein ja kirjoituksin eri tiedotuskanavissa sekä järjestä-

mällä koulutustilaisuuksia. Kuntayhtymän tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.

4. TIEDOTTAMINEN

Kuntayhtymän tietoturvallisuutta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe. Julkisuuskuvan vuoksi, luottamuksen herättämiseksi asiointiin ja palveluun sekä käyttäjien opastamiseksi tiedotetaan yleisluontoisesti tietoturvallisuusmenettelyistä.

Kuntayhtymän tietoturvallisuuteen liittyvästä tiedottamisesta kuntayhtymän ulkopuolelle ja kuntayhtymän sisällä yleisellä tasolla vastaa ja huolehtii kuntayhtymän tietoturvavastaava tietoturvasuunnitelman mukaisesti yhdessä viestintäpalveluiden kanssa. Yksiköiden sisäiseen tiedottamiseen osallistuvat myös yksiköiden johtajien nimeämät vastuuhenkilöt.

Yleisesti ottaen tietoteknisten yksityiskohtien varomaton kertominen voi vaarantaa tietoturvallisuuden, joten tiedotusvastuut on keskitettävä tietoturvavastaavalle tai hänen varahenkilölleen.

5. TIETOTURVALLISUUDEN SEURANTA JA ONGELMATILANTEIDEN KÄSITTELY

Tietoturvallisuuden ylläpito edellyttää jatkuvaa seurantaa, johon kuuluvat tietoturvallisuuden valvonta sekä sen tason ja poikkeamien raportointi. Seurantaa toteutetaan sekä automaattisesti teknisin keinoin että henkilöiden toimesta mm. osana esimiesvastuuta. Teknisestä seurannasta on erilliset ohjeensa. Tietoturvavastaava koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuudesta kuntayhtymän johdolle.

Tietoturvavastaavalla ja tietoturvatyöryhmällä on kuntayhtymän ylimmän johdon antama valtuutus ja velvollisuus tehdä kuntayhtymän tietojen käsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikkönsä tietoturvasta vastaavalle henkilölle tai johtajalle sekä tietoturvavastaavalle, joka reagoi niihin erikseen määriteltävällä tavalla.

Tietoturvapoikkeamatilanteissa IT Lappialla on kuntayhtymän johdon valtuutus sulkea palveluita ja käyttäjätilejä, sekä rajoittaa verkkoliikennettä tilapäisesti poikkeaman laajenemisen estämiseksi ja poikkeaman korjaamiseksi.

Tietoturvapoikkeamiin reagoimisesta ja tietoturvarikkomusten seuraamuksista on omat erilliset sääntönsä.

LIITE 1: MÄÄRITELMÄT

Eheys (integrity)
1) Tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus,
2) Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Fyysinen turvallisuus (physical security)
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen tietoturvallisuus (administrative and organizational information security)
Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilöstöturvallisuus (personnel security)
Henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.

Henkilöturvallisuus
Henkilöstöturvallisuus sekä henkilöstön että soveltuvin osin opiskelijain osalta.

Kokonaisturvallisuus
Kuntayhtymän turvallisuus jaetaan yhdeksään eri osa-alueeseen: toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta, valmiussuunnittelu, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus ja rikosturvallisuus.

Käytettävyys (availability)
Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Käyttöturvallisuus (operations security)
Tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi.

Laitteistoturvallisuus (computer security; facilities security)
Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.

Luottamuksellinen (confidential) **tieto**
Vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu. Valtionhallinnon **turvaluokituksen** mukaan luottamuksellinen vastaa III turvaluokkaan kuuluvaa tietoa. Kuntayhtymässä käytetyt turvaluokitukset on määritelty arkistonmuodostussuunnitelmassa.

Luottamuksellisuus (confidentiality)
Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Ohjelmistoturvallisuus (software security)
Käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Perusturvallisuus (baseline security)
Vähimmäistoimenpiteet, joilla varmistetaan tietojenkäsittelyn ja toimintaprosessien häiriötön toiminta normaalioloissa. (Tietoturvallisuuden taso, jossa järjestelmän omistaja on varautunut vastaamaan rutiininomaisin toimin normaalioloissa sattuviin vahinkoihin ja keskeytyksiin.)

Poikkeama, tietoturvapoikkeama (information security incident)
Tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen käytettävyys ei ole suunnitellulla tasolla tai tietojen eheys tai luottamuksellisuus on vaarantunut.

Poikkeusolot (extraordinary circumstances)
Kansainvälisestä tilanteesta tai suuronnettomuudesta johtuva vakava vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle.

Valmiuslain (1080/1991, muut. 198/2000) mukaan mahdollisia poikkeusoloja ovat mm.

- Suomeen kohdistuva aseellinen hyökkäys
- sota ja sodan jälkitila
- alueellisen koskemattomuuden vakava loukkaus ja sodanuhka
- vieraiden valtioiden välinen sota, josta on vaaraa Suomelle
- tuonnin vaikeutumisesta aiheutuva vakava taloudellinen uhka
- suuronnettomuus.

Poikkeustilanne (exceptional situation)
Organisaatiota kohtaava tilanne, joka voi esiintyä myös normaalioloissa, kuten tulipalo, sähkö- tai ilmastointihäiriö, tuhoisa rikos, lakko tai avainhenkilöstön menetys.

Tietoaineistojen luokitus (classification of data)
Tietojen jakaminen luokkiin tietojen omistajan asettamien perusteiden mukaisesti. Luokitusperusteena voi olla esimerkiksi tiedon luottamuksellisuus tai sen merkitys organisaation toiminnalle. Valtionhallinnon turvaluokituksen perusteena on tietojen haavoittuvuus asiattomalle käsittelylle ja paljastumiselle sekä tästä yhteiskunnalle tai valtiolle aiheutuva menetys tai haitta. Tietojen luokittelemisen perusteena voi olla esimerkiksi niiden suojaustarve, omistajuus tai tosiaikaisuusvaatimus.

Tietoaineistoturvallisuus (data security)
Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietoliikenneturvallisuus (telecommunications security)
1) tavoitetila, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta
2) lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus niin normaali- kuin poikkeusoloissa.

Tietoliikenneturvallisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

Tietotekniikan turvallisuus (IT security)
Organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvä tietoturvallisuus.

Tietoturvallisuus (information security)
1) tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille.
2) lainsäädäntö ja muut normit sekä toimenpiteet, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissa.

Tietoturvallisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Tietoturvanormi (information security norm)
Säädös tai viranomaisen määräys, joka tähtää tietojen tai tietojenkäsittelyn luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen pyrkimällä torjumaan näihin kohdistuvia uhkia tai sääntelemällä tietoturvallisuuden kehittämistoimintaa tai sitä suorittavia organisaatioita.

Tietoturvaohjeisto (information security manual)
Kuntayhtymän yhteinen, yksiköiden sisäinen ja palvelu- tai järjestelmäkohtainen ohjeistus tietojenkäsittelyn turvaamiseksi.

Tietoturvapolitiikka (information security policy)
Sama kuin tietoturvastrategia **(**information security strategy). Tietoturvalinjaukset, tietoturvaperiaatteet. Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnitelma (information security plan)
Perusturvallisuuden toteutusta ja ylläpitoa normaalioloissa koskeva suunnitelma. Suunnitelmassa esitetään organisaation tietoturvallisuustoiminnan tavoitteet, hallinto, tehtävät ja

menettelyt, osoitetaan elintärkeät tietojärjestelmät ja määritellään niiden toipumisen edellyttämät toimet.

Tietoturvasuunnittelu (information security planning)
Suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvallisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmiussuunnittelu, ja jonka tuloksena on tietoturva-suunnitelmia, -linjauksia ja -ohjeistoja.

Turvallisuus (security)
Olotila, jossa tiedossa olevat uhat eivät merkitse sanottavaa riskiä ja ne voidaan hallita.

Turvaluokiteltu tieto, turvaluokitus (security classification)
Luottamuksellisten asiakirjain ja tietojen jakaminen luokkiin salassapidettävyyden perusteella.

Turvaluokitus sisältää seuraavat luokat:
- **I turvaluokka** - erittäin salainen: äärimmäisen arkaluonteista, salassa pidettävää tietoa, jota voi käsitellä vain sen vastaanottajaksi merkitty henkilö. Tietoa ei saa lähettää sähköpostissa.
- **II turvaluokka** - salainen: arkaluonteista, salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka on virastossa oikeutettu käsittelemään salassa pidettäviä asioita. Salaista tietoa voi lähettää sähköpostissa vain riittävän vahvasti salattuna.
- **III turvaluokka** - luottamuksellinen: salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka tehtävässään sitä tarvitsevat. Tietoa voi lähettää sähköpostissa riittävän vahvasti salattuna.
- **IV turvaluokka** - viranomaiskäyttö: Tiedon paljastuminen heikentäisi viranomaisen toiminta-edellytyksiä.

LIITE 2: KUNTAYHTYMÄN TIETOTURVALLISUUTTA OHJAAVIA SÄÄDÖKSIÄ, SUOSITUKSIA JA OHJEITA

Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain ja asetuksen lisäksi useisiin eri lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat

Toinen aste, sen työntekijöitä ja opiskelijoita koskevia keskeisiä lakeja ovat:
- Arkistolaki (831/1994)
- Hallintolaki (434/2003)
- Henkilötietolaki (HetiL, 523/1999)
- Julkisuuslaki (JulkL, 621/1999)
- Laki yksityisyyden suojasta työelämässä (TETSL, 759/2004, *mm. 6. luku*)
- Rikoslaki (38. luku Tieto-ja viestintärikoksista)
- Suomen perustuslaki (731/1999, 10–12§)
- Sähköisen viestinnän tietosuojalaki (SVTSL, 516/2004)
- Tekijänoikeuslaki (404/1961)
- Laki ammatillisesta koulutuksesta (630/1998 mm. luku 5:35 §; luku 6:44)
- Vahingonkorvauslaki (412/1974, luku 4; luku 5:5-6 §; luku 6)
- Työsopimuslaki (55/2001, luku 7:1-2 §; luku 8:1 §;)

Aikuiskoulutusta, sen työntekijöitä ja opiskelijoita koskevia keskeisiä lakeja ovat:
- Arkistolaki (831/1994)
- Hallintolaki (434/2003)
- Henkilötietolaki (HetiL, 523/1999)
- Julkisuuslaki (JulkL, 621/1999)
- Laki yksityisyyden suojasta työelämässä (TETSL, 759/2004, *mm. 6. luku*)
- Rikoslaki (38. luku Tieto-ja viestintärikoksista)
- Suomen perustuslaki (731/1999, 10–12§)
- Sähköisen viestinnän tietosuojalaki (SVTSL, 516/2004)
- Tekijänoikeuslaki (404/1961)
- Laki ammatillisesta koulutuksesta (630/1998 mm. luku 5:35 §; luku 6:44)
- Vahingonkorvauslaki (412/1974, luku 4; luku 5:5-6 §; luku 6)
- Työsopimuslaki (55/2001, luku 7:1-2 §; luku 8:1 §;)

LIITE 3: KESKEISET KUNTAYHTYMÄN VOIMASSA OLEVAT TIETOTURVALLISUUTEEN LIITTYVÄT SÄÄNNÖT JA OHJEET

1. Lappia_Tietoturvapolitiikka
2. Lappia_WLAN_Tietoturvasäännöt
3. Lappia_IT-palvelujen_käyttösäännöt
4. Lappia_Sähköpostisäännöt
5. Lappia_Tietojärjestelmien_ylläpitosääntö
6. Lappia_Tietotekniikkarikkomusten seuraamusasteikko
7. Lappia_Tietotekniikkarikkomusten seuraamuskäytäntö
8. Lappia_Työntekijän sähköpostin hakeminen ja avaaminen
9. Lappia_Kuolemantapaus_ohje