TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Hyväksytty: Teuvan kunnanhallitus 10.3.2025 § 69

Sisällys

Tietoturvan ja tietosuojan käsitteitä

Tietoturva	Tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä.
Tietosuoja	Henkilötietojen suojaamista ja rekisteröidyn oikeus omiin tietoihinsa.
Tietoturvallisuus	Käytetään usein tietoturvasta puhuttaessa, sisältää käytännössä myös tietosuojan turvaamisen toimenpiteet
Rekisteröity	Henkilö, jonka tietoja käsitellään eri tietojärjestelmissä.
Henkilötieto	Kaikki tieto, jolla yksittäinen henkilö voidaan tunnistaa joko suoraan tai epäsuorasti.
Keinoäly/tekoäly/AI	Ohjelma, joka kykenee tekemään älykkäinä pidettäviä toimintoja, kuten kääntämään tekstiä kieleltä toiselle tai tunnistamaan puhetta.
Käyttöoikeus	Määrittelee sen, mihin tietoaineistoihin ja järjestelmiin käyttäjällä on oikeus päästä.
Haittaohjelma	Ohjelma, joka laitteelle asentuessaan voi vaarantaa tietoturvan toteutumisen, esimerkiksi pyrkimällä varastamaan käyttäjätunnuksia. Pyrkii leviämään edelleen uusille laitteille ja voi aiheuttaa suurta haittaa.
Kiristyshaittaohjelma	Ohjelma, joka laitteelle asentuessaan salakirjoittaa laitteen tiedot ja pyytää niiden avaamisesta lunnaita. Voi levitä myös verkon muille laitteille, jolloin vahinkojen määrä nousee erittäin korkeaksi.
Tietoaineisto	Tietojärjestelmien, tai välineiden, ja niihin tallennettujen tietojen muodostama kokonaisuus. Tietoaineisto voi olla sekä sähköisessä että paperimuodossa.
Tietojärjestelmä	Tiettyä tarkoitusta varten koottu, tiettyjä tietoja sisältävä tietokokonaisuus.
Tietojenkalastelu eli Phishing	Viestillä tai puhelimitse tapahtuva yritys saada tietoon salassa pidettävää tietoa. Usein tietojenkalastelu kohdistuu tunnusten ja salasanojen kalasteluun.
Tietoturvaloukkaus, tietomurto.	Luvaton tunkeutuminen organisaation sisäisiin verkkoihin ja järjestelmiin. Pelkkä tietomurron yritys on rangaistava teko.
Deepfake	Yleensä tekoälyn tuottamia kuvia tai videoita, joissa olemassa oleva henkilö on väärennetty tilanteeseen, jossa hän ei ole ollut tai laitettu sanomaan sellaista, mitä hän ei ole sanonut.

1. JOHDANTO

Tietoturva- ja tietosuojapolitiikka ja sen liitteet määrittävät tietoturvallisuuden linjaukset, päämäärät ja käytännön toteutuksen. Politiikka on johdon hyväksymä ja se on voimassa toistaiseksi. Päivityksiä tehdään tarpeen mukaan, kuten lakien ja määräysten tai organisaatiorakenteen muuttuessa.

Tietoturva- ja tietosuojapolitiikan tarkoituksena on yhdenmukaistaa organisaation tietoturvan ja tietosuojan toteuttamiskäytäntöjä sekä vahvistaa tietojenkäsittelyn turvallisuutta. Tietoturvallisuuden toteuttaminen ja kehittäminen yhteistyössä sopimuskumppanien ja muiden sidosryhmien kanssa on osa organisaation tietoturvatyötä.

Tietoturva- ja tietosuojapolitiikka koskee jokaista työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee tietoaineistoja. Tätä politiikkaa sovelletaan kaikkeen tietoaineistoon, riippumatta sen esitystavasta, muodosta, elinkaaren vaiheesta, tallennusympäristöstä tai siirtotiestä.

Tietoturva- ja tietosuojapolitiikka toimii pohjana tietoturvaa ja tietosuojaa koskeville ohjeille, kuten henkilöstön tietoturva- ja tietosuojaoppaalle. Tietoaineistojen käsittely tapahtuu näin yhdenmukaisten tietoturva- ja tietosuojaperiaatteiden mukaisesti, joiden lisäksi eri palvelualueilla saattaa olla käytössä tarkentavia ohjeita ja määräyksiä, joita tulee noudattaa.

Ensisijainen vastuu tietoturvan ja tietosuojan toteutumisesta, seurannasta ja tiedottamisesta läpi organisaatiorakenteen, on organisaation ylimmällä johdolla, joka varmistaa tietoturva- ja tietosuojatyön riittävän resursoinnin ja seurannan.

2. TIETOTURVA- JA TIETOSUOJAPERIAATTEET

Tietoturva- ja tietosuojatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tämä politiikka määrittää periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan tietoturvallisuuden toteuttamiseksi ja kehittämiseksi.

Tietoturva- ja tietosuojatoimenpiteiden toteuttamisella pyritään tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamiseen ja suojaamiseen siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu.

Teknisin ratkaisuin mahdollistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely ja rajoitetaan työn kannalta tarpeettomaan tietoon pääsyä.

Henkilöstön ja toimeksiannosta tai muun sopimuksen perusteella toimivien yhteistyötahojen velvollisuus on tutustua tietoturva- ja tietosuojapolitiikan sekä henkilöstön tietoturva- ja tietosuojaoppaan sisältöön ja alakohtaisiin ohjeisiin.

Esihenkilöiden ja johdon vastuulla on tietosuojan vaikutustenarviointien toteuttaminen tietosuoja-asetuksen mukaisesti silloin, kun hankinta tai muutos kohdistuu henkilötietoja sisältäviin järjestelmiin.

Tietoturva koostuu:

Tiedon luottamuksellisuus	• Tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä • Tiedot eivät päädy ulkopuolisten tietoon
Tiedon eheys	• Tietojen muuttumattomuus, säilyvyys ja muutoksen havaitseminen laitteisto- tai järjestelmäviasta huolimatta
Tiedon saatavuus	• Tieto on saatavilla ja käytettävissä silloin, kun niitä tarvitaan
Todentaminen, kiistämättömyys	• Tietoturvan kolmeen pääperiaatteeseen voidaan nykyään liittää myös käyttäjän luotettava todentaminen ja tietojen käytön kiistämätön todistaminen

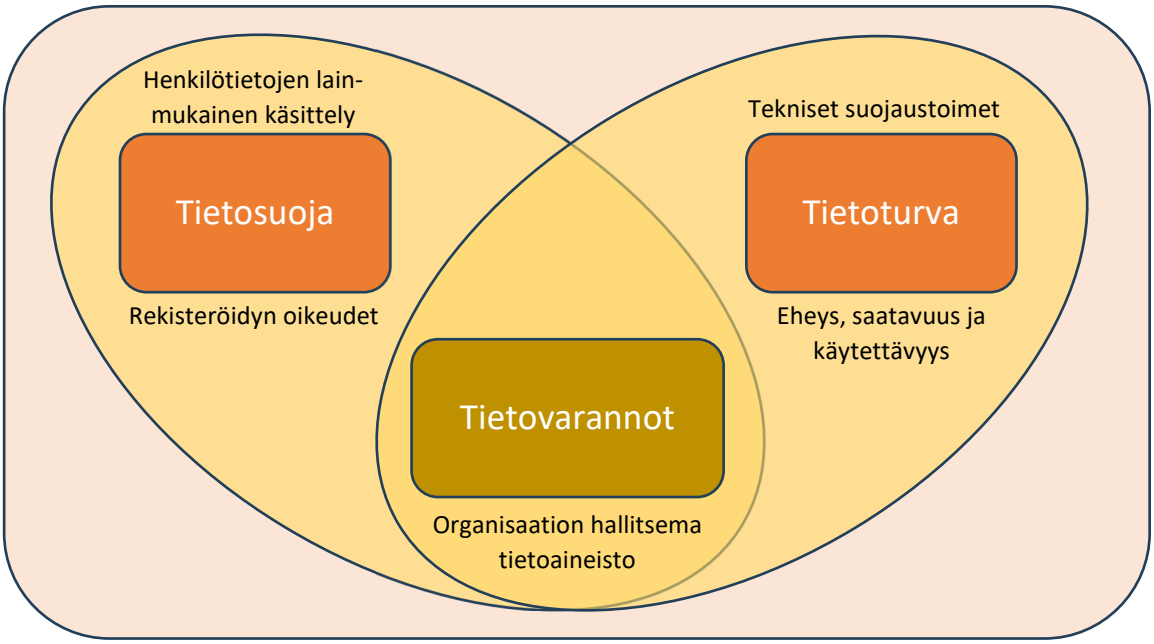
Kuva 1 Tietoturvan tavoitteet

Tietoturvan ja tietosuojan toteuttaminen ovat keskiössä tietoaineistojen käsittelyssä.

Tietosuoja kattaa henkilötietojen käsittelyn sekä henkilötietojen suojaamisen periaatteet sekä rekisteröityjen oikeuksien toteuttamisen.

Tietoturva tarkoittaa järjestelmien, tilojen ja tietoaineistojen teknisiä suojaustoimenpiteitä, joita ilman myöskään tietosuoja ei toteudu.

Tietoturvan ja tietosuojan keskinäinen suhde on kuvattu oheisessa kuviossa.



Kuva 2: Tietoturvan ja tietosuojan suhde toisiinsa

2.1. Tietoturvan hallinnolliset periaatteet

Hallinnollinen tietoturva on tietoturvatyön johtamista ja organisointia, ja sillä tarkoitetaan tietoturvatoimintojen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta.

Hallinnollisen tietoturvan keinoin pyritään ennakoimaan riskejä sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia. Tavoitteena ovat sekä tietoturvan tekninen toteutuminen että johdon ja henkilöstön sitoutuminen tietoturvallisuuden suunnitelmalliseen toteuttamiseen ja kehittämiseen.

Palveluiden hankinnoissa edellytetään tiedon käsittelyyn liittyvien suojatoimien, vastuiden ja teknisten tietoturvavastuiden sisältyvän sopimuksiin. Lisäksi henkilötietojen käsittelystä sovitaan EU:n yleisen tietosuoja-asetuksen mukaisesti ja huomioidaan tietosuoja-asetuksen vaatimukset organisaatiolle.

Tietoturvatehtävillä on omat vastuuhenkilöt. Vastuuhenkilöille järjestetään resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät. Tarkemmin tästä luvussa Vastuut ja organisointi.

Tietoturvarikkomukset ja tietoturvapoikkeamat käsitellään tietoturvan vaarantumisepäilyn selvitysprosessin (Liite 3) mukaisesti. Tietoturvarikkomusten ja väärinkäytösten rangaistusta määritettäessä sovelletaan tietosuojarikkomusten seuraamustaulukkoa (Liite 4).

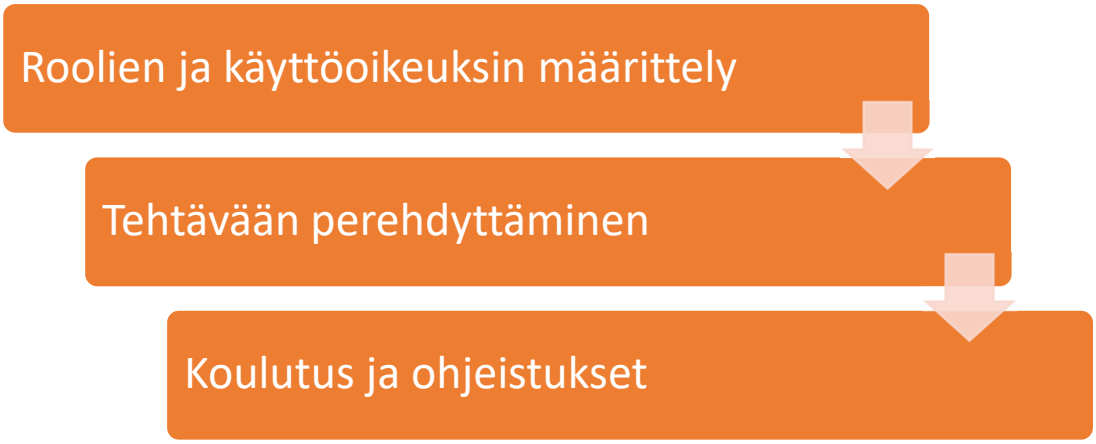
Kuva 3 Hallinnollinen tietoturva

2.2. Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöiden toimista johtuvia ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti asetetut tietoturvavaatimukset.

Henkilökunnan koulutus ja perehdyttäminen ovat tärkeä osa henkilökunnan tietoturvatietoisuuden ylläpidossa. Henkilöstö perehdytetään tehtäväänsä, perehdytyksessä tietoturva- ja tietosuojaohjeet annetaan tiedoksi. Koulutuksella pyritään antamaan henkilökunnalle riittävä tieto erilaisista tietoturvallisuuden uhista ja niiden estämisestä, jossa henkilöstön osaamisella on erityisen suuri merkitys.

Henkilöstö, opiskelijat, harjoittelijat ja organisaatiolle toimeksiannosta palveluita tuottavat henkilöt ja toimijat velvoitetaan noudattamaan tietoturvallisia toimintatapoja tehtävässään.



Kuva 4 Henkilöstöturvallisuus

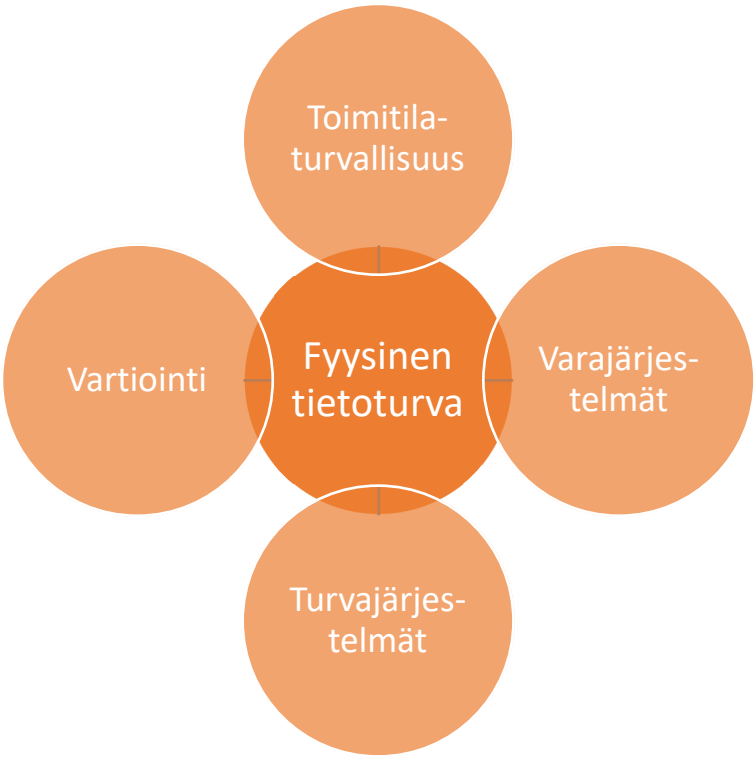
2.3. Fyysinen tietoturva

Fyysinen tietoturva tarkoittaa toimitilojen suojaamista erilaisin teknisin keinoin, joita ovat mm. turvajärjestelmät, kuten valvontakamera-, paloilmoitin- tai kulunvalvontajärjestelmät.

Fyysisen tietoturvan keinoin suojataan organisaation hallussa olevia tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien toimien seurauksilta. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta.

Tekninen toimiala ja Suupohjan Seutupalvelukeskus Oy vastaavat omien vastuualueidensa mukaisesti fyysisen tietoturvan ylläpidosta.

Henkilöstöä ohjeistetaan fyysisen tietoturvan käytänteistä ja toimintavoista.



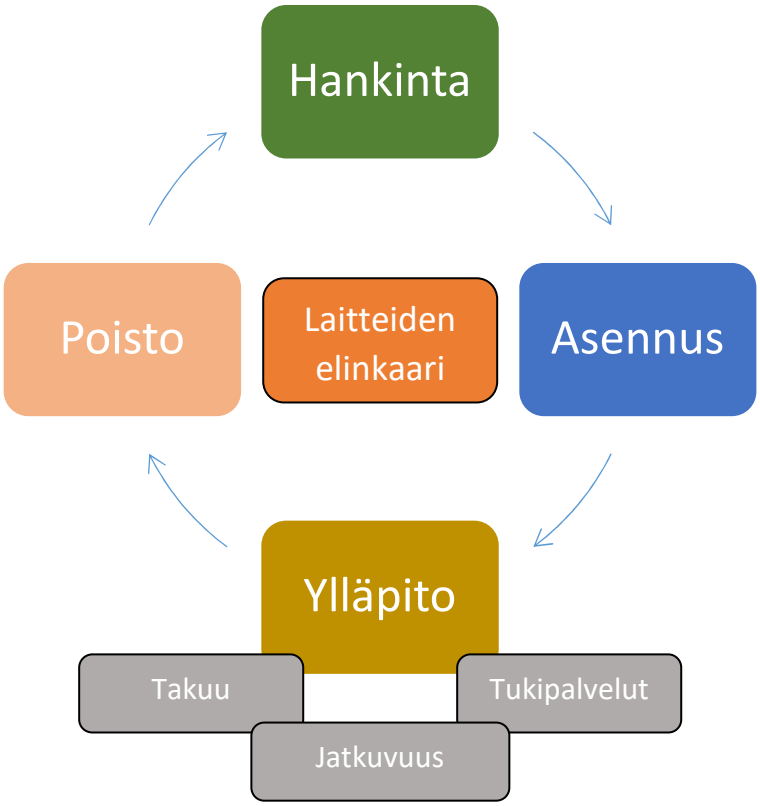
Kuva 5 Fyysinen tietoturva eli toimitilaturvallisuus

2.4. Laitteistoturvallisuus

Laitteistoturvallisuudella turvataan organisaation laitteistojen elinkaarta ja turvallista käyttöä, siihen kuuluvat laitteiston asennuksen, suojauksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja sopimukset sekä laitteistojen turvallinen poisto niiden elinkaaren lopussa.

Teknisin toimin pyritään varmistamaan laitteiden keskeytyksetön käyttö ja toiminnan jatkuvuus sekä varaudutaan mahdollisista häiriöistä toipumiseen.

ICT-laitteiden hankinnasta, ohjelmistoasennuksista, suojauksesta ja ylläpidosta vastaa keskitetysti Suupohjan Seutupalvelukeskus Oy palvelusopimuksen mukaisesti.



Kuva 6 Laitteiden elinkaari

2.5. Ohjelmistoturvallisuus

Ohjelmiston hankinnan lähtökohta on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja arkkitehtuurin kanssa. Ohjelmistojen tietoturva huomioidaan jo hankintavaiheessa, jolloin varmistutaan ohjelmistojen vaatimustenmukaisuudesta. Ohjelmiston valmistajan ja myyjän vastuu ohjelmistotuotteista määräytyy hankinta- ja käyttöoikeussopimuksissa.

Esihenkilö vastaa siitä, että hänen alaisuudessaan olevat käyttäjät perehdytetään ohjelmistojen käyttöön ja määrittelee henkilöstölle tarvittavat käyttöoikeudet.

Ohjelmien hankinta, asentaminen, suojaus, päivitykset ja varmuuskopiointi on osin keskitetty Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti. SaaS-palveluiden tuottajat vastaavat näistä sopimusten mukaisesti.

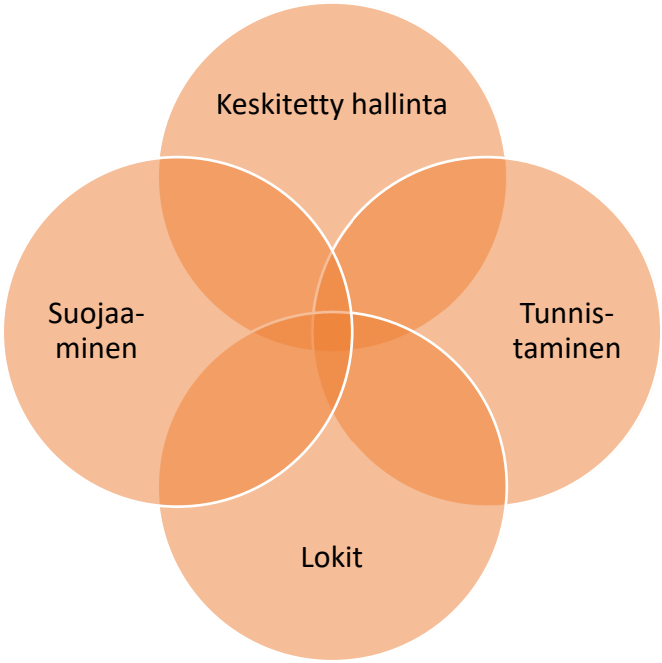
Kuva 7 Ohjelmistoturvallisuus

2.6. Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden toimenpitein pyritään turvaamaan viestinnän häiriöttömyys, tiedonsiirtoyhteyksien käytettävyys, tiedonsiirron suojaaminen sekä käyttäjien tunnistaminen. Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet.

Tietoliikenneverkkojen toiminnasta kerätään järjestelmälokia, jonka perusteella voidaan ehkäistä väärinkäyttöä ja voidaan torjua ulkoisia uhkia. Järjestelmälokit keräävät tietoa mm. järjestelmien käyttöasteesta, käyttökatkoksista, kirjautumisista ja mahdollisista tietomurtojen yrityksistä.

Tietoliikenneturvallisuuden ylläpito on keskitetty Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti.



Kuva 8 Tietoliikenneturvallisuuden keinoja

2.7. Käyttöturvallisuus

Käyttöturvallisuus tarkoittaa turvallisen käytön toimintaolosuhteita, tekniikan toimivuuden valvontaa, käytön ja lokien valvontaa, ohjelmistotukea, ylläpitoa ja huollon turvallisuustoimenpiteitä, varmuuskopiointia sekä häiriöraportointia.

Esihenkilöt ja ohjelmien pääkäyttäjät opastavat henkilöstöä ohjelmistojen käyttöön ja tietoturvallisuuteen liittyvissä asioissa. Laitteiden ja ohjelmien käyttäjien tulee perehtyä annettuihin ohjeisiin ja noudattaa niitä. Tietojen käyttöoikeuksia rajataan tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla.

Käyttöturvallisuuden tekninen ylläpito on osin keskitetty Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti. SaaS-palveluiden tuottajat vastaavat käyttöturvallisuudesta sopimusten mukaisesti.

Kuva 9 Käyttöturvallisuuden periaatteet

2.8. Tietoaineistojen käsittely

Tietojen käsittely, luokittelu ja säilyttäminen perustuvat tiedonhallintaa ohjaavaan lainsäädäntöön ja ohjeisiin. Perusteena henkilötietojen käsittelylle on lakisääteisyys tai suostumus, sekä käyttäjän työtehtävästä johtuva asiayhteys asiakkaaseen ja häntä koskeviin tietoihin. Muun salassa pidettävän tiedon käyttöön tulee myös olla työtehtävästä johtuva peruste.

Pääsynhallinnalla ja sen suunnittelulla pyritään estämään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Pääsynhallinta sisältää käyttäjätunnusten ja työtehtävässä tarvittavien oikeuksien määrittelyn.

Tietojen saatavuus, käytettävyys ja eheys pyritään varmistamaan sekä estämään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen.

Teknisillä toimilla pyritään varmistamaan toiminnan jatkuvuus häiriöttä, sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys sekä varaudutaan mahdollisista häiriöistä toipumiseen.

Tietoturvatoimia sovelletaan tietoaineiston koko elinkaaren ajan, tiedon syntymisestä sen hävittämiseen.

Kuva 10 Tietoaineistojen käytön periaatteet

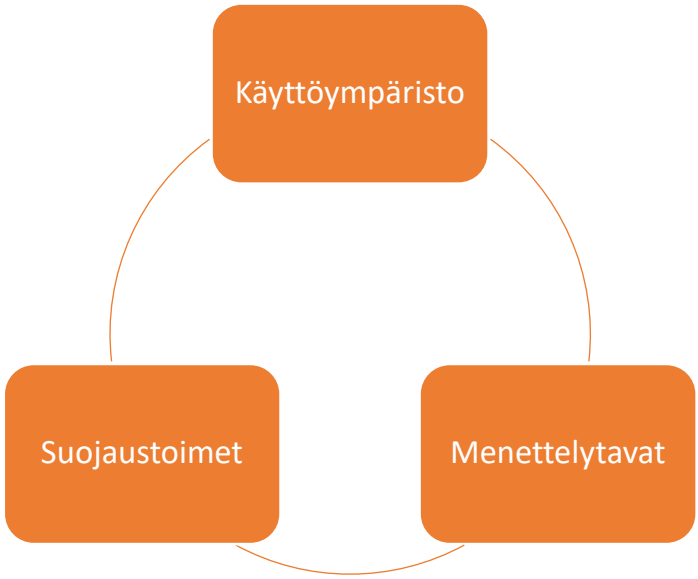
2.9. Etätyö ja matkatyö

Etä- ja matkatyö ovat muualla kuin vakituisessa toimipisteessä tehtävää työtä, jolloin käyttöympäristöt vaihtelevat, eikä ympäristön turvallisuuteen voida aina vaikuttaa. Etätyöntekijän toimenpiteillä ja menettelytavoilla on tällöin erityisen suuri merkitys ja etätyöntekijän on kyettävä tekemään itsenäinen arvio etätyöympäristön turvallisuudesta sekä toimittava sen mukaisesti.

Puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassapidon toteutumisesta tulee huolehtia, kunkin käyttöpaikan erityisolosuhteet huomioiden.

Etätyössä korostuu henkilökohtainen vastuu tietoturvallisista toimintatavoista.

Annettuja ohjeita tulee noudattaa kaikessa organisaation toimitilojen ulkopuolella tehtävässä työssä.



Kuva 11 Etätyön turvallisuuteen vaikuttavat tekijät

2.10. Tekoäly, eli AI

Tekoäly, eli AI tai keinoäly, on ohjelma, joka tekee älykkäinä pidettäviä toimintoja, kuten puheentunnistusta, päättelyä, suunnittelua tai ongelmanratkaisua ja pystyy myös sopeuttamaan toimintaansa olosuhteiden tai ohjeiden mukaan. Usein tekoälyn ymmärretään tarkoittavan yleisesti tarjolla olevia tekoälypalveluja, kuten ChatGPT tai Gemini, mutta tekoäly on tätä huomattavasti laajempi kokonaisuus.

Tekoälyn käyttö ja ohjeistukset perustuvat EU:n tekoälysäädökseen ja kansallisiin suosituksiin. Tämän politiikan kirjoitushetkellä tekoälyn käyttöä laajemmin vasta pohditaan organisaation tasolla. Käytössä on joitakin tekoälyä sisältäviä ohjelmistoratkaisuja, kuten haku- tai lajittelutoimintoja sekä mahdollisia tekoälyavustajia, joiden avulla esim. julkisen dokumentin oikoluku tai sisällön tiivistäminen on mahdollista.

Tekoälyä tullaan tulevaisuudessa hyödyntämään laajemmin, mutta missä ja millä tavoin, ei vielä ole kokonaan selvää. Tekoälyä käyttöönotettaessa tehdään asiaan liittyvänä mm. tietosuojan vaikutustenarviointi tarvittaessa sekä kartoitetaan tekoälyn riskit ja mahdollisuudet. Näiden lisäksi tehdään, mikäli on tarpeen, erillinen tekoälypolitiikka.

2.11. Kehittäminen ja ylläpito

Tietoturvan kehittäminen ja ylläpito ovat osa jatkuvaa prosessia, johon kuuluvat tietoturva- ja tietosuojatoimenpiteiden arviointi ja valvonta sekä poikkeamien raportointi ja tilastointi.

Esihenkilöiden velvollisuus on dokumentoida havaitut tietoturvaan ja tietosuojaan liittyvät poikkeamat ja ilmoittaa näistä eteenpäin tietoturvan tai tietosuojan vastuuhenkilöille.

Sisäisen valvonnan ja riskienhallinnan ohjeen mukainen jatkuva seuranta ja valvonta kuuluu nimettyjen henkilöiden lisäksi kaikille esihenkilöille. Valvontaa tehdään myös rekisteröidyn pyynnöstä tai muun ilmoituksen perusteella.

Jokaisen henkilöstöön tai muuhun sidosryhmään kuuluvan tulee raportoida havaitsemistaan poikkeamista.

Tietoturvan kehittämistoimenpiteissä otetaan huomioon yllä mainitut tekijät ja ajankohtaiset vaatimukset. Kehittämisessä tarkoituksena on parantaa tietojärjestelmien, tietoverkkojen ja käytön turvallisuutta sekä vikasietoisuutta. Kehittämistoimenpiteissä hyödynnetään myös viranomaisten välisiä verkostoja ja verkostojen jäsenien jo hyväksi havaittuja käytänteitä.

Kuva 12 Tietoturvan kehittämisen toimenpiteitä

3. TIETOSUOJA

Tietosuoja kattaa henkilötietojen käsittelyn ja se määrittää henkilöiden yksityisyyden suojaamista ja sillä turvataan luonnollisten henkilöiden oikeuksia, tietoja ja luottamusta.

Tietosuojan vaatimukset määrittävät EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, jotka velvoittavat rekisterinpitäjän suunnittelemaan henkilötietojen käsittelyn ja osoittamaan käsittelyn lainmukaisuuden sekä suojaamaan tiedot asiattomalta käsittelyltä. Nämä lait määrittävät myös henkilötiedon määritelmän.

Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta tiedon tallennusmuodosta. Henkilötietojen turvallinen käsittely korostuu alueellisten ja kansallisten yhteisjärjestelmien käytössä.

Tietosuojan toteutumista seurataan ja havaittuun asiattomaan käyttöön puututaan.

Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta. Näitä toimenpiteitä kuvataan liitteissä kaksi ja kolme.

Työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietosuojaan kohdistuvista ongelmista.

Kuva 13 Henkilötietojen käsittelyn vaatimukset

3.1. Henkilötietojen kerääminen ja käsittely

Henkilötietoja käsitellään siinä laajuudessa kuin se on tarpeen palvelun tai työtehtävän kannalta. Käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön tai henkilön suostumuksen perusteella.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi.

Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen ja perustua lakiin tai rekisteröidyn suostumukseen.

Suostumuksella ei voida ohittaa lakien ja asetusten vaatimuksia henkilötietojen käsittelylle.

Rekisteröidyllä on EU:n yleisen tietosuoja-asetuksen mukaiset oikeudet itseään koskeviin tietoihin.

4. TIETOTURVARISKEIHIN VARAUTUMINEN

Tietoturvallisuutta voi uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat tilanteet sekä järjestelmiin kohdistuvat tahalliset sähköiset tai fyysiset hyökkäykset. Näiden seurauksena voivat olla mm. tiedon saatavuuden heikentyminen, tiedon muuttuminen tai tiedon päätyminen ulkopuolisen tietoon.

Sähköiset tietojärjestelmät ja näitä yhdistävät tietoverkot muodostavat järjestelmäkokonaisuuksia, joiden häiriöt, ja niiden vaikutukset, voivat laajentua yksittäistä työasemaa koskevista koko järjestelmän laajuisiksi. Tietojärjestelmäkokonaisuuteen kuuluvat mm. työasemat, puhelimet, palvelimet ja muu verkon infrastruktuuri.

Tietoturvariskejä arvioidaan ja niihin varaudutaan ennalta, toimenpiteiden toteuttaminen perustuu uhkien arviointiin ja järjestelmien kartoitukseen. Toteutettujen toimenpiteiden vaikutuksia seurataan aktiivisesti. Uhkien pienentämiseksi henkilöstön kouluttaminen sekä tietoisuuden lisääminen tietoturvallisuudesta ovat keskeisiä toimenpiteitä.

ICT-palvelut ja verkon ylläpito ostetaan suurelta osin Suupohjan seutupalvelukeskukselta, jonka valmiussuunnittelua ja varautumista ohjataan perussopimuksen mukaisesti. Lisäksi käytössä on sisäisesti hankittuja ohjelmistokokonaisuuksia, joiden ylläpidosta vastataan sisäisesti tai yhteistyössä ohjelmatoimittajan kanssa. Useat näistä ohjelmistoista toimivat ns. saas-palveluina, jolloin ylläpito tapahtuu järjestelmän toimittajan toimesta ja käyttö soveltuvan käyttöliittymän kautta etäyhteydellä. Näihin palveluihin sovelletaan yleisiä tietoturvaperiaatteita ja käsittelyssä noudatetaan annettuja ohjeita.

Kuva 14 Tietoturvariskeihin varautuminen

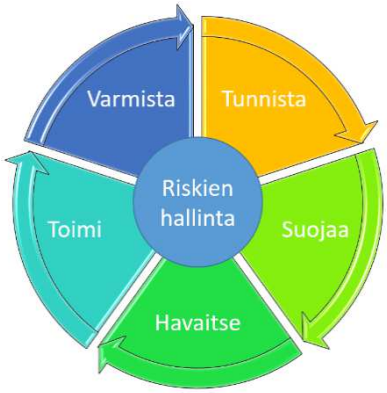
4.1. Riskien arviointi ja hallinta

Tietoturvariskejä arvioitaessa huomio kiinnitetään erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietojen oikeudeton käyttö.

Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. Järjestelmien turvajärjestelyt tarkastetaan säännöllisesti ja tarvittaessa niiden toimivuus testataan.

Tietoturvariskejä arvioidaan ja hallitaan riskienhallinnan ohjeistuksen mukaisesti ja tietoturvallisuuden suurimmat riskit sisällytetään organisaation riskienhallintasuunnitelmaan.

Tiivistetysti riskienhallintaa toteutetaan oheisen kuvion mukaisesti. Riskienhallinnassa tunnistetaan riskit, suojataan tiedot, havaitaan rikkomukset, toimitaan tilanteen vaatimalla tavalla ja varmistetaan toiminnan vaikutukset.



Kuva 15: Riskienhallintaprosessi

4.2. Häiriön tai uhkatilanteen tunnistaminen ja reagointi

Järjestelmän puutteiden ja haavoittuvuuksien tai inhimillisen toiminnan seurauksena voi olla tietojärjestelmään tai tietoaineistoon kohdistuva uhka tai poikkeama.

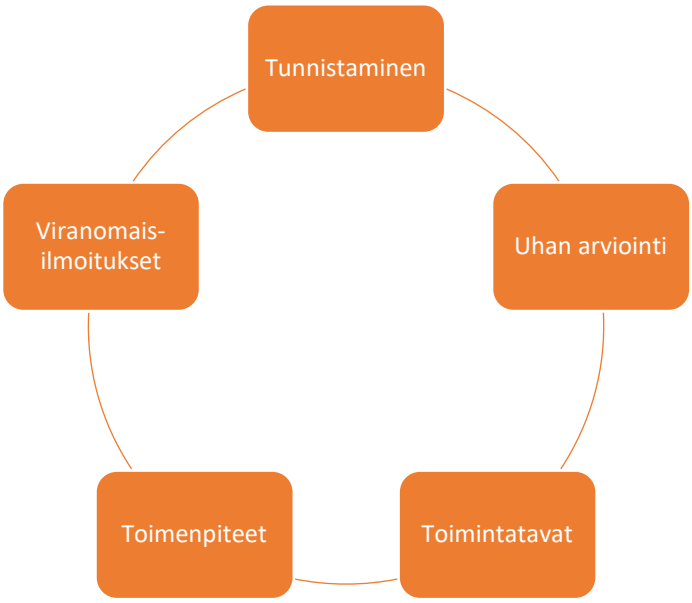
Jokaisella työntekijällä ja luottamushenkilöllä on velvollisuus ilmoittaa havaitsemistaan tai tietoonsa tulleista tietosuojan tai tietoturvan puutteista, haavoittuvuuksista ja häiriötilanteista esimiehelle, ICT-tuelle tai tietosuojavastaavalle.

Häiriötilanteen tai uhan toteutuessa ei välttämättä alkuvaiheessa ole tietoa siitä, onko häiriö tahallinen vai tahaton. Näiden käsittelyssä on merkittäviä eroja, joten tilannetta arvioidaan jatkuvasti tilannekuvan täydentyessä.

Mikäli kyseessä on tahallinen häiriö, toimintatavat sovitetaan sellaisiksi, että mahdolliselle hyökkääjälle ei anneta harkitsemattomilla toimenpiteillä etua. Keskeistä on arvioida häiriön tyyppi ja sen aiheuttama uhka toiminnalle tai tietoturvallisuudelle.

Mikäli kyse on henkilötietoihin kohdistuneesta tapahtumasta, arvioidaan tapahtuneen vakavuus ja se, tuleeko tapahtuneesta tehdä ilmoitus tietosuojavaltuutetun toimistolle ja rekisteröidyille. Tilanteen arvioinnin ja päätöksen ilmoituksesta tekevät tietoturvatyöryhmä ja tietosuojavastaava.

Tiedonkulku ICT-palveluntuottajan ja rekisterinpitäjän välillä on oleellista. Tiedottaminen havaituista häiriöistä ja niiden selvittämisen etenemisestä sekä muista toimenpiteistä pidetään molempien osapuolten saatavilla.



Kuva 16 Uhan tunnistaminen ja toimenpiteet

4.3. Viestintä häiriötilanteessa

Häiriötilanne, jonka vaikutukset ovat laajat, vaatii yleensä viestintää organisaatiosta asiakkaille ja muille sidosryhmille.

Viestinnässä noudatetaan kriisiviestinnän ohjeistuksia ja vastuita.

Viestintä toteutetaan siten, että tapahtuneen selvitys ei häiriinny, eikä viestinnällä anneta tietoa, josta voi olla hyötyä mahdolliselle ulkopuoliselle hyökkääjälle. Alkuvaiheen viestintä on näin ollen niukkaa ja rajoittuu tilanteen kannalta tarpeelliseen tietoon, yksityiskohtia tarkennetaan tilanteen ja selvitystyön edetessä.

4.4. Tietoturvarikkomusten seuraamukset

Tietoturvarikkomuksista säädetään mm. työsopimuslaissa ja viranhaltijalaissa. Henkilötietoihin kohdistuvien rikkomusten osalta EU:n yleinen tietosuoja-asetus sekä kansalliset lait ja asetukset määrittelevät toimintaperiaatteita.

Tietoturvalainsäädäntöä ja organisaation tietoturva- ja tietosuojapolitiikkaa sekä näiden perusteella annettuja ohjeita vastaan rikkominen tulee aina ilmoittaa esihenkilölle tai muulle vastuulliselle sekä tarvittaessa tietosuojavastaavalle. Valvontaprosessi etenee vastaavan viranhaltijan johdolla, joka kutsuu koolle tarvittavat henkilöt (liite 2). Seuraamuksista päättää rekisterinpidosta vastaava viranhaltija, seuraamustaulukon (liite 3) mukaisesti.

Seurauksena rikkomuksista, niiden tapauskohtaisen vakavuuden mukaisesti, voi olla käyttöoikeuteen kohdistuvia rajoituksia, palvelusuhteeseen vaikuttavia seuraamuksia sekä rikoslaissa määriteltyjä seuraamuksia.

Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.

5. SOPIMUKSIIN PERUSTUVA VARAUTUMINEN (SOPIVA)

Sopimuksiin perustuva varautuminen ja jatkuvuudenhallinta parantaa toimintaedellytyksiä ja toimintakyvyn ylläpitämistä yhteistyökumppaneiden ja muiden sidosryhmien kanssa tehtävien sopimusten avulla. Näillä varmistetaan myös tietoturvan ja tietosuojan toteutuminen yhteistyökumppaneiden kanssa tehtävissä sopimuksissa.

Jatkuvuudenhallinta on olennainen perustehtävä, jota ilman ei voida toimia tehokkaasti häiriötilanteissa. On tärkeää kehittää häiriöiden ehkäisyä, vähentää mahdollisten häiriöiden vaikutuksia toimintaan ja nopeuttaa palautumista. Nämä tavoitteet saavutetaan strategialla, joka huomioi häiriötilanteet. Tällainen strategia varmistaa valmiuden kohdata ja selviytyä erilaisista häiriöistä tehokkaasti ja nopeasti.

Toimintavarmuutta kehitetään varmistamalla, että uusissa hankinta- ja yhteistyösopimuksissa vaaditaan verkoston kaikilta kumppaneilta toiminnan jatkuvuuden hallintaa koskevien suositusten noudattamista. Tämä koskee sekä sopimuskumppaneita että niiden alihankkijoita ja muita verkostokumppaneita. Mallisopimuslausekkeiden avulla suositukset voidaan helposti ottaa käyttöön sopimuksissa, ja ne liitetään varsinaisen sopimuksen liitteeksi.

https://www.huoltovarmuuskeskus.fi/files/c6ae96c3124b891df65a25a65540ce11b3a88cf7/sopiva-mallilausekkeet.pdf

Organisaation toiminnassa ja varautumissuunnitelmassa tämä tulee huomioida seuraavilla tavoilla:

Sopimusten sisällöt:
Varmistetaan sopimusten olevan selkeitä ja kattavan mahdolliset häiriötilanteet. Niissä tulee määritellä vastuut, velvollisuudet ja toimintatavat eri tilanteissa.

Yhteistyökumppanien valinta:
Valitaan luotettavat ja osaavat yhteistyökumppanit, joilla on kokemusta ja kykyä toimia häiriötilanteissa. Taustaselvityksin arvioidaan kumppanien toimintakyky.

Tiedon jakaminen ja viestintä:
Sopimuksissa tulee määritellä, miten tieto ja viestintä jaetaan eri osapuolten välillä. Tämä on erityisen tärkeää kriisitilanteissa, jotta kaikki osapuolet ovat ajan tasalla ja toimivat yhteisen suunnitelman mukaisesti.

Sopimusten säännöllinen tarkastelu ja päivittäminen:
Sopimukset tarkistetaan ja päivitetään säännöllisesti, jotta ne pysyvät ajan tasalla ja vastaavat muuttuvia olosuhteita ja riskejä.

Koulutus ja harjoitukset:
Säännölliset koulutukset ja mahdolliset harjoitukset yhteistyökumppaneiden kanssa, jotta kaikki osapuolet ovat valmiita toimimaan häiriötilanteissa ja tietävät, miten sopimuksia sovelletaan käytännössä.

Riskienhallinta ja jatkuvuussuunnittelu:
Sopimuksiin sisällytetään riskienhallinta- ja jatkuvuussuunnitelmat, jotka auttavat ennakoimaan ja hallitsemaan mahdollisia häiriöitä sekä palautumaan niistä nopeasti.

6. VASTUUT JA ORGANISOINTI

Tietoturva on yhteinen asia ja se koskettaa koko henkilöstöä. Vastuiden määrittelyssä otetaan huomioon eri toimijoiden vastuualueet ja velvollisuudet.

Seuraavissa kappaleissa on kuvattu tarkemmin vastuualueita, lisäksi liitteenä on kaavio, jossa eri toimijoiden suhde toisiinsa on kuvattu.

6.1. Vastuu organisoinnista

Ylintä vastuuta tietoturvasta ja tietosuojasta kantaa kunnanhallitus ja sitä johtaa kunnanjohtaja. Ylimmän johdon tehtävänä on valvoa kokonaisuutta sekä riskienhallinnan ja sisäisen valvonnan toteutusta, lisäksi tehtävänä on vastata ja antaa tarkemmat ohjeet sopimusten hallinnasta sekä määrätä sopimusten vastuuhenkilöt, jotka vastaavat kulloinkin voimassa olevien sopimusten ajantasaisuudesta.

Tietoturva- ja tietosuojatyöhön huolehditaan riittävä resursointi ja tietosuojavastaavan työ mahdollistetaan organisaation toimenpitein.

Hallintojohtaja vastaa teknisen ja hallinnollisen tietoturvan yleisestä järjestämisestä, kehittämisestä ja seurannasta.

6.2. Tietosuojavastaava

Tietosuojavastaava avustaa rekisterinpitäjää velvoitteidensa toteuttamisessa ja osallistuu asiantuntijana rekisterinpitäjän vastuulla olevien tietosuojan velvoitteiden täyttämiseen.

Tietosuojavastaava osallistuu tietosuojan suunnittelutoimintaan, valmistelee ohjeita ja ylläpitää niitä sekä kouluttaa henkilöstöä tietosuojan toimintatavoista.

Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä sekä seuraa ja valvoo henkilötietojen käsittelyä ja suojausmenettelyä.

Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä sekä ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa kunnanhallituksen hyväksymän toimintatavan mukaisesti.

Organisaation lainmukainen velvollisuus on ottaa tietosuojavastaava riittävän aikaisessa vaiheessa mukaan henkilötietojen käsittelyä koskevaan suunnittelutoimintaan sekä henkilötietoja sisältävien tietojärjestelmien hankintojen suunnitteluun. Lisäksi tietosuojavastaava kutsutaan säännöllisesti mukaan organisaation työryhmiin ja johdon tapaamisiin.

6.3. Tietoturvan toteuttaminen ja suunnittelu

Tietoturvatyöryhmä toimii yhteistyössä tietosuojavastaavan kanssa tietoturvan toteuttamisessa ja suunnittelussa. Työryhmään kuuluvat tietosuojavastaava, kunnanjohtaja ja toimialajohtajat.

Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet sekä valmistelee asiat tarpeen mukaan johdon käsittelyyn. Ryhmä seuraa ja toteuttaa tietoturvan eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin ja seuraa yleisesti tietoturvatilannetta.

Toimialajohtajat vastaavat palvelualueensa tietoturvatoimenpiteistä ja tietoturvatyön organisoinnista ja kehittämistoimista sekä tietoturvaa koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Tehtävänä on vastata palvelualueen henkilötietojärjestelmien rekistereistä, rekisteröityjen ajantasaisesta informoinnista ja rekistereiden vastuuhenkilöiden nimeämisestä sekä vaikutustenarvioinnin tekemisestä omalla palvelualueellaan, käsittelytoimista tehtävän selosteen, ja muiden tietosuoja-asetuksen vaatimien dokumenttien, ajantasaisuudesta sekä sopimusten ajantasaisuudesta.

Toimialajohtajat antavat henkilötietojen ja tietoaineiston käsittelystä ja menettelytavoista ohjeita, jotka esimerkiksi tarkentavat kansallisia määräyksiä ja alueellisesti sovittuja toimintamalleja. Ohjeiden luontiin osallistuvat rekisterin vastuuhenkilöt ja tietosuojavastaava sekä tarpeen mukaisesti määriteltävät henkilöt.

Asiakirjahallinnon johtava viranhaltija laatii tiedonhallinnan ohjeet sekä huolehtii asiakirjahallintoon liittyvästä koulutuksesta, neuvonnasta ja valvonnasta. Asiakirjahallinnon johtavan viranhaltijan ja toimialojen arkistovastaavien vastuulla on asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen tiedonhallintaohjeistuksen mukaisesti.

Esihenkilöiden vastuulla on tietoturvan ja tietosuojan toteutuminen vastuualueellaan. Keskeisimmät tehtävät tietoturvan ja tietosuojan kannalta ovat:

- Oman vastuualueensa henkilöstön perehdyttäminen työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin
- Henkilöstön tietoturva- ja tietosuojaoppaan sekä muiden tietoturva- ja tietosuojaohjeiden antaminen tiedoksi henkilöstölleen
- Oikeus velvoittaa henkilöstönsä lisäkoulutukseen tai -perehdytykseen
- Tietoturvan ja tietosuojan toteutumisen seuranta
- Palvelusuhteen päättyessä tai työtehtävän vaihtuessa ilmoitus ICT-palveluille käyttöoikeuksien päättämisestä tai muuttamisesta ja kulkuoikeuksien poistamisesta

Pääkäyttäjät vastaavat käyttöoikeuksiensa mukaisesti järjestelmän tai sovelluksen tietoturvan ja tietosuojan toteutumisesta sekä ohjeistavat ja kouluttavat muita käyttäjiä järjestelmän tai sovelluksen käytössä.

Jokainen työntekijä ja luottamushenkilö on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista, uhista tai menettelyvirheistä esihenkilölle, ICT-tuelle tai tietosuojavastaavalle. Lisäksi havaituista haavoittuvuuksista yms. puutteista laitteiden suojauksessa tulee ilmoittaa ICT-palveluille. Jokainen työntekijä ja luottamushenkilö on omalta osaltaan vastuussa tietoturvan ja tietosuojan ohjeiden noudattamisesta sekä niiden toteuttamisesta toiminta-alueellaan.

Suupohjan seutupalvelukeskus ylläpitää alueella verkkopalveluita sekä leasing yms. laitteita sekä toteuttaa teknisiä tietoturvan ratkaisuja. ICT-palvelujen tehtävä on osaltaan edistää tietoturvan ja tietosuojan toteutumista sekä toimia käyttäjien tukena erilaisissa tilanteissa sopimusten mukaisesti.

7. KOLMANNET OSAPUOLET

Palveluja tuottavat kolmannet osapuolet ovat velvollisia noudattamaan ostajan antamia ohjeita sekä laissa määriteltyjä tietoturva- ja tietosuojavaatimuksia.

Kolmannet osapuolet ovat velvollisia ilmoittamaan tietoturvapoikkeamista, joilla voi olla vaikutusta tietoturvan toteutumiselle. Ilmoitusvelvollisuus ja muut vastuut määritellään myös sopimuksin.

Kolmannet osapuolet velvoitetaan tarpeen mukaisesti nimeämään tietoturva- ja tietosuoja-asioihin yhteyshenkilö, joka vastaa ohjeiden sekä tietoturva- ja tietosuojatason noudattamisesta.

8. LISÄTIETOA

Tämä tietoturva- ja tietosuojapolitiikka pohjautuu kansalliseen lainsäädäntöön ja EU:n yleiseen tietosuoja-asetukseen. Lisätietoa löydät mm. seuraavista:

- Organisaation intranet
  - https://seutupalvelukeskusfi.sharepoint.com/sites/Teuvankunta-Intranet
- Lainsäädäntö
  - www.finlex.fi
  - https://eur-lex.europa.eu/homepage.html?locale=fi
- Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI-ohjeet
  - www.vahtiohje.fi
- Viestintäviraston kyberturvallisuuskeskuksen sivut
  - https://www.viestintävirasto.fi/kyberturvallisuus.html
- Tietosuojavaltuutetun toimisto
  - www.tietosuoja.fi
- Sopimuksiin perustuva varautuminen
  - Sopimuksiin perustuva varautuminen - SOPIVA - Huoltovarmuuskeskus

LIITE 1

SITOUMUS SALASSAPIDOSTA JA VAITIOLOVELVOLLISUUDESTA

Me allekirjoittaneet osapuolet olemme sopineet salassapito- ja vaitiolovelvollisuudesta seuraavaa:
Asiakirjojen, tietoaineiston ja tietojärjestelmien käsittely- ja käyttöoikeudet annetaan vain tämän sitoumuksen allekirjoittaneelle. Sitoumus tehdään työsuhteen alkaessa. Sijaisten, opiskelijoiden ja harjoittelijoiden kanssa sitoumus tehdään ensimmäisen palvelusuhteen alkaessa tai palvelusuhteen luonteen muuttuessa.

Työntekijä vastaa oman toimintansa tietoturvallisuudesta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa. Työntekijän tulee seurata työnantajan antamia ohjeita ja tarvittaessa on kysyttävä lisäohjeita.

Esihenkilö antaa uuden työntekijän perehdytyksen yhteydessä tiedoksi henkilöstön tietoturva- ja tietosuojapas sekä muut ohjeet. Ohjeet tulee antaa jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.

Vaitiolo- ja salassapitositoumus:
Työntekijänä sitoudun olemaan käyttämättä, ilmaisematta tai luovuttamatta palvelusuhteen aikana asiakkaisiin, henkilötietoihin sekä liike- ja ammattisalaisuuksiin liittyviä salassa pidettäviä tietoja, riippumatta siitä, miten tai mihin tieto on tallennettu tai millä tavalla tieto on saatu (kirjallisesti, suullisesti tai havainnoimalla) muutoin kuin työtehtävien vaatimassa laajuudessa ja työtehtävien yhteydessä. Tietojen luovutuksen tulee perustua asiakkaan kirjalliseen suostumukseen, asiayhteydestä ilmenevään suostumukseen tai lainsäädäntöön.

Sitoudun noudattamaan seuraavia tietosuojaperiaatteita:

- Salassapito- ja vaitiolovelvollisuus koskee minua palvelusuhteeni aikana ja myös sen jälkeen
- Noudatan erityistä huolellisuutta käsitellessäni salassa pidettäviä tietoja
- Pidän salassa kaikki tietooni saamani arkaluonteiset tiedot esim. henkilön sairautta, tutkimusta, hoitoa, taloudellista asemaa tai sosiaalisia etuuksia koskevat tiedot sekä yleiseen turvallisuuteen, tietojärjestelmiin ja kiinteistöturvallisuuteen liittyvät tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja. Työkavereiden, lähiomaisten, naapureiden tai julkisuuden henkilöiden tietoja en käsittele, mikäli työtehtäväni eivät sitä edellytä.
- Vastaan käyttäjätunnuksillani ja/tai varmennekortin tunnuksillani tapahtuvasta tietojen käytöstä.
- En luovuta tunnuksiani toisen henkilön käyttöön.
- Vastaan käytössäni olevasta kannettavasta tietokoneesta tai muusta laitteesta niin, ettei laite ja siinä olevat tiedot joudu vääriin käsiin.
- Olen tietoinen, että tietojärjestelmissä käyntini ja siellä tehdyt tapahtumat kirjautuvat lokitiedostoihin ja epäillystä väärinkäytöstä raportoidaan esihenkilölle ja tarvittaessa myös viranomaisille sekä henkilölle, jonka tiedoista on kyse.
- Olen tietoinen, että tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta on lainsäädännössä rangaistava teko. Rangaistavaa menettelyä henkilötietojen käsittelyssä koskevat säännökset sisältyvät EU:n yleiseen tietosuoja-asetukseen, tietosuojalakiin ja rikoslakiin. Tietojen oikeudettomasta käytöstä voi seurata rikos-, työ- ja vahingonkorvausoikeudellisia seuraamuksia.

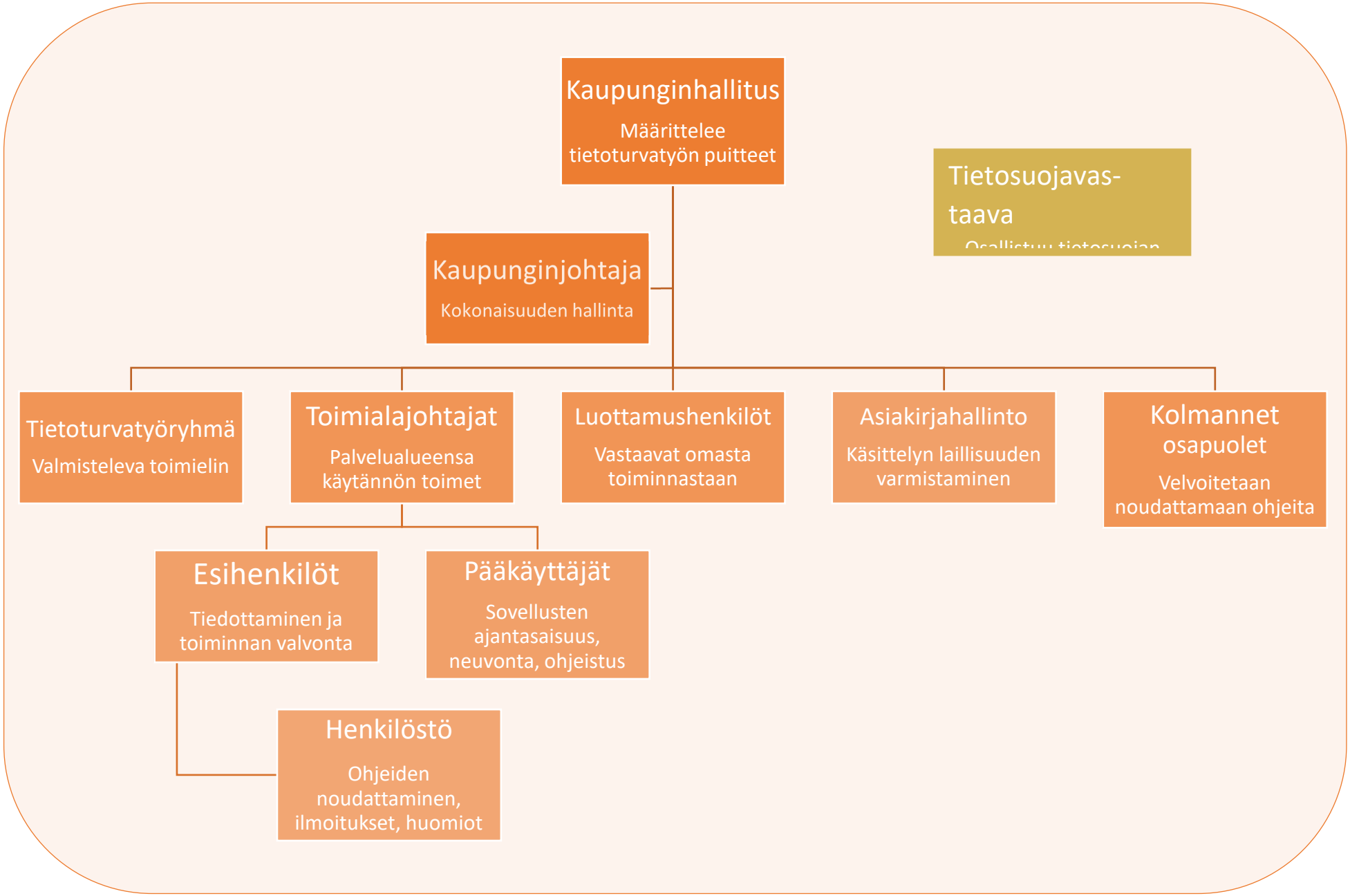
Olen lukenut tämän sitoumuksen ja ymmärrän sen sisällön ja merkityksen.
Olen saanut tiedokseni henkilöstön tietoturva- ja tietosuojaoppaan sekä ohjeet työtehtävääni koskien.

Paikka ja aika:_____ _____ / _____ 20_____

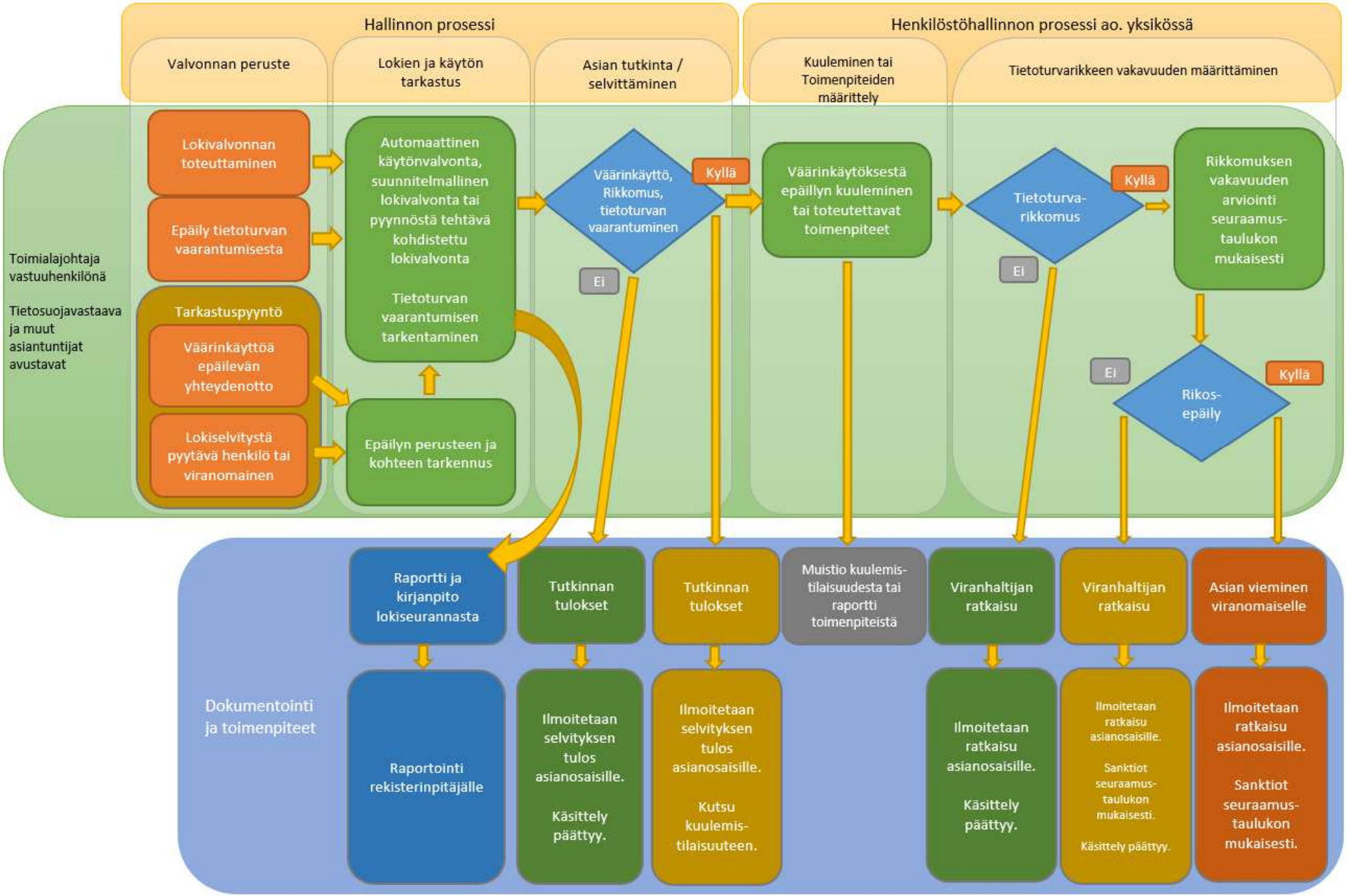
_____ _____
Työntekijän nimi Työyksikkö

_____ _____
Työntekijän allekirjoitus Esimiehen allekirjoitus

Liite 2. Tietoturvan ja tietosuojan vastuiden organisointi



LIITE 3. Tietoturvan tai tietosuojan vaarantumisepäilyn selvitysprosessi.



LIITE 4. Tietosuojarikkomusten seuraamustaulukko