SUUPOHJAN KOULUTUSKUNTAYHTYMÄ

TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Käsittely:	Johtoryhmä	08.05.2019
Hyväksytty:	Yhtymähallitus	YH 6/23.05.2019 §59
	Yhtymävaltuusto	YV 1/11.06.2019 §10

Muutos-/tarkastushistoria:

Suupohjan koulutuskuntayhtymä
Oppitie 4 /PL 6, 61801 KAUHAJOKI
hallinto@saiedu.fi

Sisällys

1. JOHDANTO

Tieto on keskeisessä roolissa organisaatioiden toiminnassa ja palvelutuotannossa. Tiedon tulee olla hyödynnettävissä tarpeen mukaisesti ja tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys ovat tärkeitä toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Tietosuoja suojaa ihmisten yksityisyyttä. Inhimillisenä toimintana tietojenkäsittelyyn liittyy aina riskejä, joita pyritään minimoimaan ohjeistuksilla, koulutuksella ja teknisillä ratkaisuilla. Tietoturvariskeistä pystytään minimoimaan teknisin ratkaisuin vain osa, tärkeintä ovat päivittäisessä tietojenkäsittelyssä tehdyt ratkaisut ja toimenpiteet.

Tietoturva suojaa henkilötietoja ja muita tietoja luvattomalta käytöltä, se käsittää keskeisiin toimintoihin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti uhkia ja tarvittaessa sietää niiden vaikutuksia. Riskien tunnistamisen ja hallinnan sekä vaikutusten minimointi on osa organisaation aktiivista tietoturvan toteuttamista.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla, jonka on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös organisaation toimintakykyyn. Lisäksi lainsäädäntö edellyttää tietoturvan asianmukaista hoitamista. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen. Tietoturvan ja tietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvon antajina.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi ja sitä voidaan tarvittaessa täydentää tai päivittää, kuten lainsäädännön tai muiden ohjeistusten muuttuessa.

Tietoturva- ja tietosuojapolitiikka on julkinen asiakirja.

2. TIETOTURVA- JA TIETOSUOJAPERIAATTEET

Tietoturvatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain tietoturvaorganisaation raportoinnilla johdolle.

Tietoturva- ja tietosuojapolitiikka määrittää periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan tietoturvan toteuttamiseksi ja kehittämiseksi, sitä sovelletaan kaikessa toiminnassa ja koko henkilöstöön sekä sidosryhmiin.

Yksityiskohtaisemmat toimintaohjeet löytyvät Henkilöstön tietoturvaoppaasta ja toimialuekohtaisista lisäohjeista ja määräyksistä. Nämä asiakirjat tulee antaa tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.

Tietoturvaperiaatteita noudatetaan kaikissa tiedon elinkaaren vaiheissa ja tämän edistämiseksi tietoturva- ja tietosuojaperiaatteet ovat osa henkilöstön perehdytystä ja koulutusta. Teknisin ratkaisuin varmistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely.

3. TIETOTURVA

Tietoturvasta huolehditaan asianmukaisesti, joka tarkoittaa tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä. Tietoturvalliseen toimintatapaan ohjeistetaan ja sen tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella.

Tietoturva koostuu:

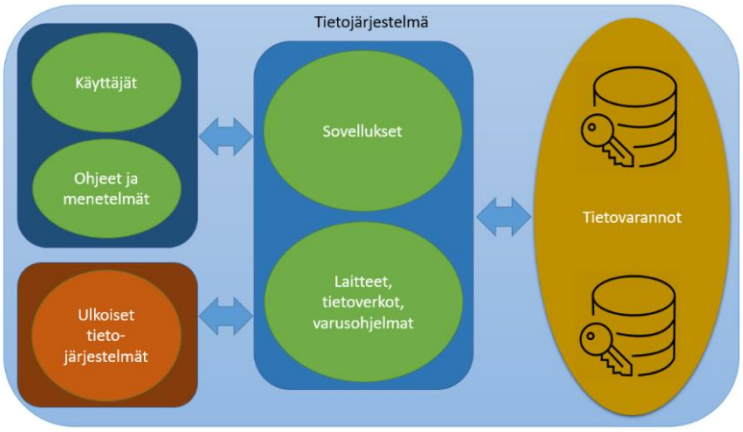
- **Tiedon luottamuksellisuudesta**, eli siitä, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla eivätkä ne päädy ulkopuolisten tietoon
- **Tiedon eheydestä,** joka tarkoittaa tietojen muuttumattomuutta tai muutoksen havaitsemista ja säilyvyyttä laitteisto- tai järjestelmävian tai inhimillisen toiminnan vuoksi
- **Tiedon saatavuudesta,** jolloin tieto on oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun niitä tarvitaan.
- **Todentamisesta ja kiistämättömyydestä**, joilla tarkoitetaan käyttäjän todentamista ja käyttäjien tietojen käytön kiistämätöntä todistamista

Kuva 1: Tietoturva ja tietosuoja

Tietojärjestelmien teknisen ympäristön ja ohjelmistojen sekä laitteiden ylläpito on ulkoistettu Suupohjan seutupalvelukeskus Oy:lle, joka vastaa sopimuksen mukaisesti tietoturvan toteutumisesta lain ja asetusten sekä rekisterinpitäjän ohjeiden mukaisesti. Johdon vastuulla on huolehtia sopimuksen ajantasaisuudesta ja vaatimustenmukaisuudesta, etenkin lainsäädännön tai viranomaismääräysten muuttuessa on tarkistettava vastaako sopimus muuttuneeseen tilanteeseen.

3.1. Tietojärjestelmä

Tietojärjestelmä on kokonaisuus, joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmään kuuluu oleellisena osana käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta. Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.



Kuva 2: Tietojärjestelmä

3.2. Tietoturvan hallinnolliset periaatteet

Hallinnollinen tietoturva on tietoturvatoimintojen johtamista ja organisointia, sillä tarkoitetaan tietoturvatoimintojen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Hallinnollinen tietoturva pyrkii ennakoimaan riskit sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia. Tavoitteena on sekä tietoturvan toteutuminen että johdon ja henkilöstön sitoutuminen sen suunnitelmalliseen hoitamiseen ja kehittämiseen.

Palveluiden hankinnoissa edellytetään tiedon käsittelyyn liittyvien suojatoimien, vastuiden ja teknisten tietoturvavastuiden sisältyvän palvelusopimuksiin, lisäksi henkilötietojen käsittelystä tulee sopia EU:n yleisen tietosuoja-asetuksen mukaisesti.

Tietoturvaan liittyvillä tehtävillä on omat vastuuhenkilöt. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät. Tarkemmin tästä on kerrottu luvussa **Vastuut ja organisointi**

Tietoturvaperiaatteet viedään käytäntöön ohjeistuksin, koulutuksin ja tiedottein.

3.3. Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöiden toimista johtuvia ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti hänelle asetetut tietoturvavaatimukset. Henkilöstön ja organisaatiolle ostopalveluita tuottavien henkilöiden ja toimijoiden tulee noudattaa tietoturvallisia toimintatapoja tehtävässään.

Henkilökunnan koulutus, valmennus ja perehdyttäminen ovat tärkeä osa henkilökunnan tietoturvatietoisuuden ylläpidossa. Uusi henkilöstö perehdytetään ja koulutetaan tehtäväänsä, samalla käydään läpi tietoturvaohjeet. Osallistumista koulutuksiin ja tietoturvaosaamista seurataan yleisellä tasolla.

Työtehtävän mukainen käyttöoikeus järjestelmiin ja ohjelmistoihin annetaan käyttölupahakemus täyttämällä ja salassapitositoumus hyväksymällä. Tämä edellyttää henkilöllisyyden luotettavaa varmistamista. Esimies huolehtii käyttölupahakemuksen tekemisestä ja työtehtävän määrittelystä.

Tietoturvaohjeiden noudattamisen seuranta on säännöllistä. Tietoturvarikkomukset käsitellään Liitteen 2 ja Liitteen 3 mukaisesti. Väärinkäytösten varalle on laadittu yhtymävaltuuston hyväksymä seuraamustaulukko (Liite 2).

3.4. Fyysinen tietoturva

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

3.5. Tietoaineiston turvallisuus

Tietojen käsittely sekä luokittelu ja säilyttäminen perustuvat tiedonhallintaa ohjaavaan lainsäädäntöön ja ohjeisiin. Perusteena henkilötietojen käsittelylle on lakisääteisyys tai käyttäjän tehtävästä johtuva asiayhteys asiakkaaseen ja häntä koskeviin tietoihin.

Tietojen saatavuus ja käytettävyys varmistetaan teknisin toimin ja estetään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen. Teknisillä toimilla pyritään varmistamaan toiminnan jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Samalla varmistetaan mahdollisen sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys, joka tarkoittaa sähköisen asioinnin toimintaprosessin huolellista suunnittelua.

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

3.6. Laitteistoturvallisuus

Laitteistoturvallisuudella suojataan 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.

Laitteiden elinkaareen liittyvät palvelusopimukset pidetään ajan tasalla ja laitteiston elinkaaren päättyessä huolehditaan tietojen asianmukaisesta tuhoamisesta. Tietojärjestelmätoimittajilla ja tietoinfrastruktuurin ylläpitäjällä on omat vastuunsa laitteistoturvallisuuden osalta ja nämä huomioidaan hankinnoissa ja sopimuksissa.

Teknisin toimin pyritään varmistamaan tietojen keskeytyksetön käyttö ja toiminnan jatkuvuus sekä varaudutaan mahdollisista häiriöistä toipumiseen. Kriittisille laitteistoille taataan katkoton sähkönsyöttö ja ylläpidon korkea palvelutaso.

3.7. Ohjelmistoturvallisuuden periaatteet

Pääsynhallinnalla ja sen suunnittelulla estetään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Ohjelmistojen tietoturvallisuuteen kiinnitetään huomiota jo niiden hankintavaiheessa, jolloin varmistutaan ohjelmistojen tietoturvallisuudesta ja vaatimustenmukaisuudesta. Käyttäjät perehdytetään ohjelmistojen käyttöön.

Ohjelmistohankinnat ja kehittäminen perustuvat toiminnan tarpeisiin. Uuden ohjelman hankinnan lähtökohta on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja arkkitehtuurin kanssa. Lisäksi huomioidaan EU:n yleisen tietosuoja-asetuksen asettamat vaatimukset.

3.8. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus pyrkii varmistamaan viestinnän häiriöttömyyden, tiedonsiirtoyhteyksien käytettävyyden, tiedonsiirron suojaamisen ja salauksen sekä käyttäjien tunnistamisen. Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet.

3.9. Käyttöturvallisuus

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

Tietoturva on suuressa määrin käyttäjien toiminnasta riippuvaista. Käyttöturvallisuuden perustana on osaava ja sitoutunut henkilöstö sekä ajantasaiset ohjeistukset, joita toiminnassa noudatetaan. Tietojen oikeudeton käyttö estetään tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla.

3.10. Liikkuva työ

Liikkuva työ tarkoittaa kaikkea organisaation toimitilojen ulkopuolella tehtävää työtä. Etätyötä tehtäessä huolehditaan puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassa pidon toteutumisesta. Kaikessa organisaation toimitilojen ulkopuolella tehtävässä työssä on noudatettava tietoturvavaatimuksia.

Liikkuvan työn käytäntöjä on selvitetty tarkemmin henkilöstön tietoturvaoppaassa.

3.11. Seuranta, valvonta ja raportointi

Tietoturvan kehittäminen ja ylläpito vaativat jatkuvaa seurantaa. Tähän kuuluvat tietoturvan valvonta sekä poikkeamien raportointi ja tilastointi. Seurannan toteuttaminen on esimiesten ja nimettyjen henkilöiden toteuttamaa valvontaa, lisäksi valvontaa tehdään rekisteröidyn pyynnöstä tai työntekijän ilmoituksen perusteella.

4. TIETOSUOJA

Tietosuoja on olennainen osa tietoturvaa. Tietosuoja määrittelee henkilön yksityisyyden suojaamista ja sillä turvataan oikeuksia, tietoja ja luottamusta. Tietosuojan lähtökohtana on suojata henkilöiden perusoikeudet ja -vapaudet sekä erityisesti henkilötiedot ja varmistaa yksityisyyden suoja.

Tietosuojaa ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan ja osoittamaan henkilötietojen käsittelyn lainmukaisuuden.

Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta niiden tallennusmuodosta tai niihin kohdistuvan uhan luonteesta. Uhat voivat olla tahallisia tai tahattomia, kuten tietojen urkinta, huolimattomuus, järjestelmäviat, tapaturmat tai luonnonkatastrofit.

Rekisterinpitäjä seuraa tietosuojan toteutumista ja puuttuu havaitsemaansa asiattomaan käyttöön, myös työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvaongelmista. Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta. Näitä toimenpiteitä kuvataan liitteissä kaksi ja kolme sekä riskienhallintasuunnitelmassa.

Henkilötietojen turvallinen käsittely korostuu alueellisten ja kansallisten yhteisjärjestelmien käytössä.

4.1. 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 nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö toteutetaan siten, ettei ulkopuolisten ole mahdollista saada niitä tietoonsa.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella. Rekisteröidyllä on EU:n yleisen tietosuoja-asetuksen mukainen oikeus tarkistaa itseään koskevat tiedot.

Suomessa henkilötietojen käsittelyä ohjaa ja valvoo tietosuojavaltuutettu, joka käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröidyn oikeuksien toteutumisesta. Yhteyshenkilönä organisaation ja tietosuojavaltuutetun välillä toimii tietosuojavastaava.

Henkilötietojen käsittelystä on saatavissa tarkempaa tietoa nettisivuilta tai tietosuojavastaavalta.

5. TIETOTURVARISKEIHIN VARAUTUMINEN

Tieturvariskejä arvioidaan ja niihin varaudutaan ennalta. Suurimmat tietoturvariskit tulee sisällyttää organisaation riskienhallintasuunnitelmaan. Tietoturvaan kohdistuvat uhat voivat aiheuttaa riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Laitetason ratkaisuilla voidaan vaikuttaa tietoturvan toteutumiseen vain rajallisesti, henkilöstön osaaminen ja tietoisuus ovat suuressa roolissa tietoturvan toteutumisessa ja kouluttaminen sekä tietoisuuden lisääminen tietoturvasta, ovat merkittävä tekijä uhkien pienentämisessä. Esimiesten vastuulla on huolehtia henkilöstön perehdyttämisestä.

Uhkia aiheuttavat myös mahdolliset tietoisesti tehdyt väärinkäytökset, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset ja haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat.

5.1. Riskien arviointi

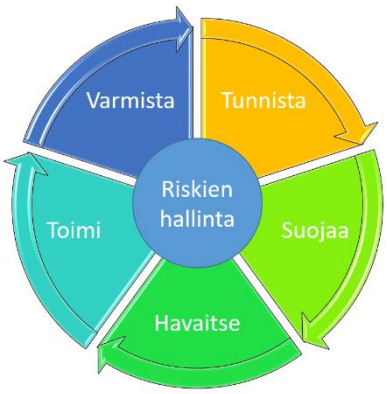
Tietoturvariskejä arvioitaessa on huomio kiinnitettävä erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen,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

Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. SPK vastaa järjestelmien turvajärjestelmien säännöllisestä tarkastuksesta ja toimivuuden testaamisesta.

5.2. Riskienhallintasuunnitelma

Tietoturvariskejä tulee arvioida ja hallita riskienhallinnan ohjeistuksen mukaisesti ja tietoturvan suurimmat riskit tulee sisällyttää organisaation riskienhallintasuunnitelmaan.

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



Kuva 3: Riskienhallintaprosessi

5.3. Tietoturvapoikkeamat

Jokaisella on velvollisuus ilmoittaa havaitsemistaan tietoturvaan kohdistuvista uhista tai rikkeistä. Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation tietovarantoihin ja palveluihin kohdistuu uhka, joka vaarantaa tiedon ja palvelun eheyden, luottamuksellisuuden tai saatavuuden.

Havainnon tietoturvapoikkeamasta voi tehdä kuka tahansa, kuten organisaation työntekijä, tietojärjestelmän ylläpitäjä tai ulkopuolinen henkilö. Tällöin on tilanne huomioiden otettava yhteys tietosuojavastaavaan, tietohallintoon, esimieheen tai muuhun vastuuhenkilöön. Työntekijän velvollisuus on viedä asia eteenpäin, mikäli esimerkiksi asiakas siitä hänelle ilmoittaa.

Mikäli kyse on henkilötietoihin kohdistuneesta tapahtumasta, tulee arvioida tapahtuneen vakavuus ja se, tuleeko tapahtuneesta tehdä ilmoitus tietosuojavaltuutetun toimistolle ja rekisteröidyille. Kyseinen ilmoitus edellyttää aina tilanteen arvioinnin, jonka tekee tietoturvatyöryhmä ja tietosuojavastaava.

Tarkemmat toimintaohjeet löytyvät Henkilöstön tietoturvaoppaasta.

5.4. Tietoturvarikkomusten seuraamukset

Tietoturvarikkomuksista säädetään työsopimuslaissa sekä viranhaltijalaissa. Henkilötietoihin kohdistuvien rikkomusten osalta asiaa säätää lisäksi EU:n yleinen tietosuoja-asetus sekä kansalliset lait ja asetukset.

Tietoturvalainsäädäntöä ja organisaation tietoturva- ja tietosuojapolitiikkaa sekä näiden perusteella annettuja ohjeita vastaan rikkominen tiedotetaan aina esimiehelle. Seurauksena rikkomuksista, niiden 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.

Seuraamuksia arvioitaessa on toimintaa tarkasteltava kokonaisuutena, jonka yhtenä osana tietoturvarikkomus on, ja jonka vaikutukset ja seuraukset arvioidaan aina tapauskohtaisesti. Arvioinnissa käytetään apuna liitteen 2 mukaista taulukkoa.

6. VASTUUT JA ORGANISOINTI

Tietoturva on organisaation yhteinen asia ja se koskettaa koko henkilöstöä.

Ylintä vastuuta tietoturvasta kantaa **yhtymähallitus**, jonka tehtävänä on valvoa kokonaisuutta sekä riskienhallinnan ja sisäisen valvonnan toteutusta. Tietoturva- ja tietosuojatyöhön huolehditaan riittävä resursointi ja tietosuojavastaavan työ mahdollistetaan organisaation toimenpitein.

Yhtymähallitus vastaa sopimusten hallinnan ja sopimusvalvonnan järjestämisestä, antaa tarkemmat ohjeet sopimushallinnasta sekä määrää sopimusten vastuuhenkilöt.

Talous- ja henkilöstöjohtaja vastaa kokonaisuudessaan teknisen ja hallinnollisen tietoturvan järjestämisestä, kehittämisestä ja seurannasta. Toimialoittain vastuuta kantavat kunkin tulosyksikön johtajat, he myös päättävät vastuualueeseensa kuuluvista kehittämistoimista ja organisoinnista.

Kuntayhtymän johtaja johtaa tietoturvallisuutta.

Johtoryhmä tekee esitykset yhtymähallitukselle tietoturvan eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista. Yhtymävaltuuston hyväksymä tietoturva- ja tietosuojapolitiikka on tietoturvallisuuden toteuttamisen perusta.

Tietosuojavastaava auttaa johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, valmistelee ohjeita ja ylläpitää niitä sekä kouluttaa tietosuoja-asioita henkilöstölle. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa ja seuraa sekä valvoo henkilötietojen käsittelyä ja suojausmenettelyä. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Lisäksi tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä sekä ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa hallituksen hyväksymän toimintatavan mukaisesti. Organisaation velvollisuus on ottaa tietosuojavastaava riittävän aikaisessa vaiheessa mukaan henkilötietojen käsittelyä koskevaan suunnittelutoimintaan sekä henkilötietoja sisältävien tietojärjestelmien hankintojen suunnitteluun.

Tietoturvatyöryhmä toimii yhteistyössä tietosuojavastaavan kanssa tietoturvan toteuttamisessa ja suunnittelussa. Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet sekä huolehtii tietoturvan toteuttamisen vastuuttamisesta. Ryhmä seuraa ja toteuttaa tietoturvan eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin ja seuraa yleisesti tietoturvatilannetta.

Tulosyksiköiden johtajat huolehtivat vastuualueensa tietoturvasta sekä tietoturvaa koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Tulosyksiköiden johtajat vastaavat vastuualueensa henkilötietojärjestelmien rekistereistä, rekisteröityjen ajantasaisesta informoinnista ja rekistereiden vastuuhenkilöiden nimeämisestä. Tulosyksiköiden johtajat huolehtivat vaikutustenarvioinnin tekemisestä omalla vastuualueellaan sekä selosteen käsittelytoimista ajantasaisuudesta ja sopimusten ajantasaisuudesta. Tulosyksiköiden johtajat antavat henkilötietojen ja asiakirjojen käsittelystä ja menettelytavoista

vastuualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja. Ohjeiden laatimiseen osallistuvat asiantuntijoina tietosuojavastaava sekä tarpeen mukaisesti rekisteriasioista vastaavat henkilöt.

Asiakirjahallinnosta laaditaan tiedonhallinnan ohjeet ja valvotaan, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä huolehditaan asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta. Asiakirjahallinnon ja arkistovastaavien vastuulla on asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen tiedonhallintaohjeistuksen mukaisesti.

Tietojärjestelmistä ylläpidetään tietojärjestelmäluetteloa, joka toimii tietojärjestelmäselosteena.

Esimiehet vastaavat tulosalueittain sekä toimintayksiköittäin tietoturvan toteutumisesta ja siihen liittyvästä tiedottamisesta sekä valvonnasta. Esimiesten vastuulla on perehdyttää tietoturva- ja tietosuojamääräykset henkilöstölle ja valvoa näiden noudattamista.

Jokainen työntekijä on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista, uhista tai menettelyvirheistä tietosuojavastaavalle. Samoin jokainen työntekijä on omalta osaltaan vastuussa tietoturvan toteuttamisesta.

Organisaatiolle palveluja tuottava kolmannet osapuolet velvoitetaan noudattamaan organisaation ja lakien määrittelemiä tietoturvaperiaatteita.

7. LISÄTIETOA

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

- Organisaation intranet
  - www.intra.net
- 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

LIITE 1

SOPIMUS SALASSAPIDOSTA JA VAITIOLOVELVOLLISUUDESTA

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

Jokainen työntekijä vastaa oman toimintansa tietoturvasta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

Henkilöstön tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Esimiehen velvollisuus on uuden työntekijän perehdytyksen yhteydessä läpikäydä henkilöstön tietoturva- ja tietosuojaohjeet.

Vaitiolo- ja salassapitositoumus:
Työntekijänä sitoudun olemaan käyttämättä, ilmaisematta tai luovuttamatta 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 yhteydessä. Tietojen luovutuksen tulee perustua aina asiakkaan 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 taloudellista asemaa koskevat tiedot sekä turvallisuuteen, tietojärjestelmiin ja kiinteistöturvallisuuteen liittyvät tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja.
- Vastaan käyttäjätunnuksillani ja/tai varmennekortin tunnuksillani tapahtuvasta tietojen käytöstä.
- Vastaan käytössäni olevasta kannettavasta tietokoneesta tai muusta laitteesta ja huolehdin, ettei laite ja siinä olevat tiedot joudu vääriin käsiin.
- Olen tietoinen, että tietojärjestelmissä käyntini ja siellä tehdyt tapahtumat kirjautuvat lokitiedostoihin ja epäillystä väärinkäytöstä raportoidaan esimiehelleni 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 koskevat säännökset sisältyvät EU:n yleiseen tietosuoja-asetukseen, kansalliseen lainsäädäntöön ja viranomaismääräyksiin. Tietojen oikeudettomasta käytöstä voi seurata rikos-, työ- ja vahingonkorvausoikeudellisia seuraamuksia.

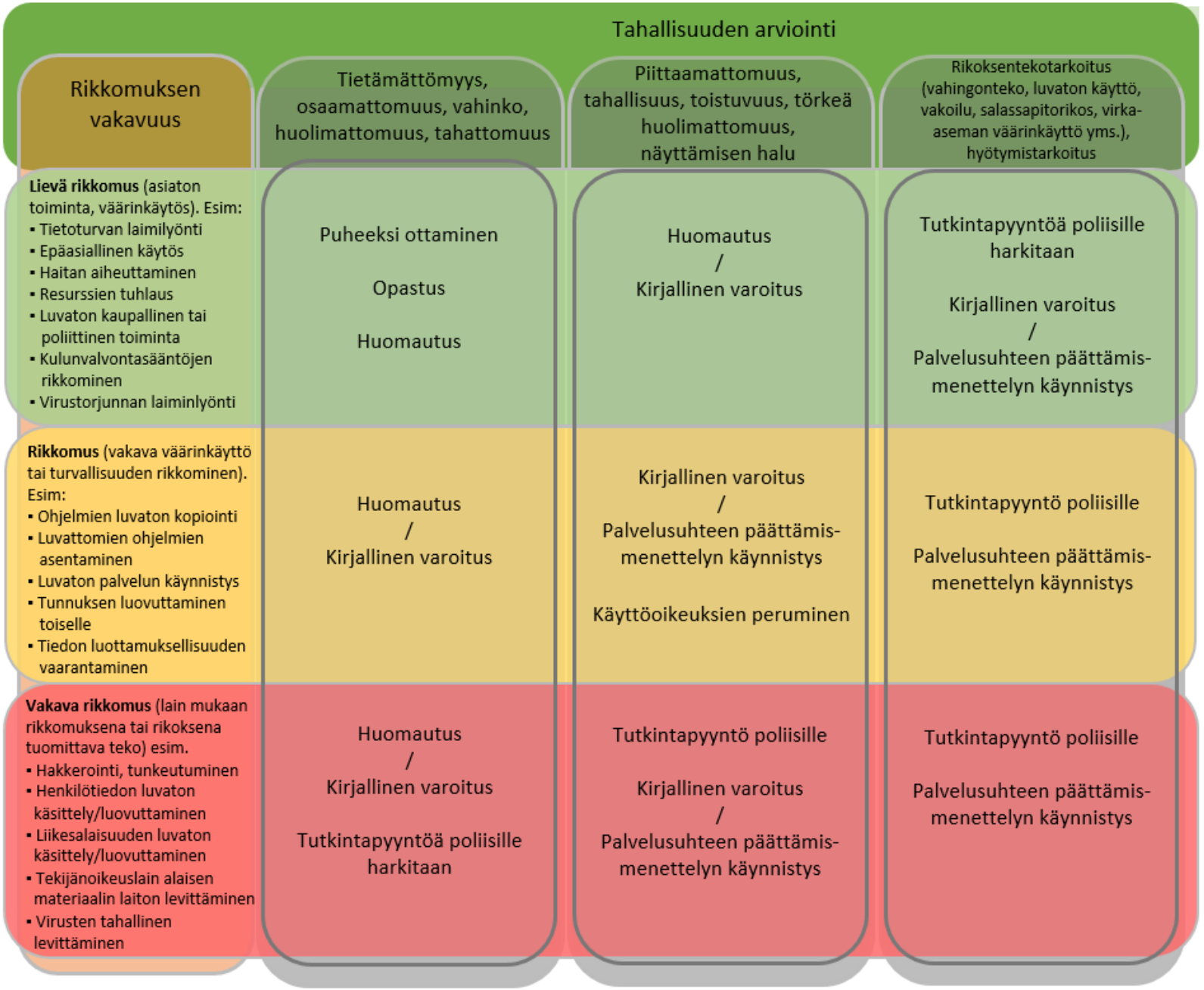
Olen lukenut tämän sitoumuksen ja ymmärrän sen sisällön ja merkityksen.

Paikka ja aika:_____ _____ / _____ 20_____

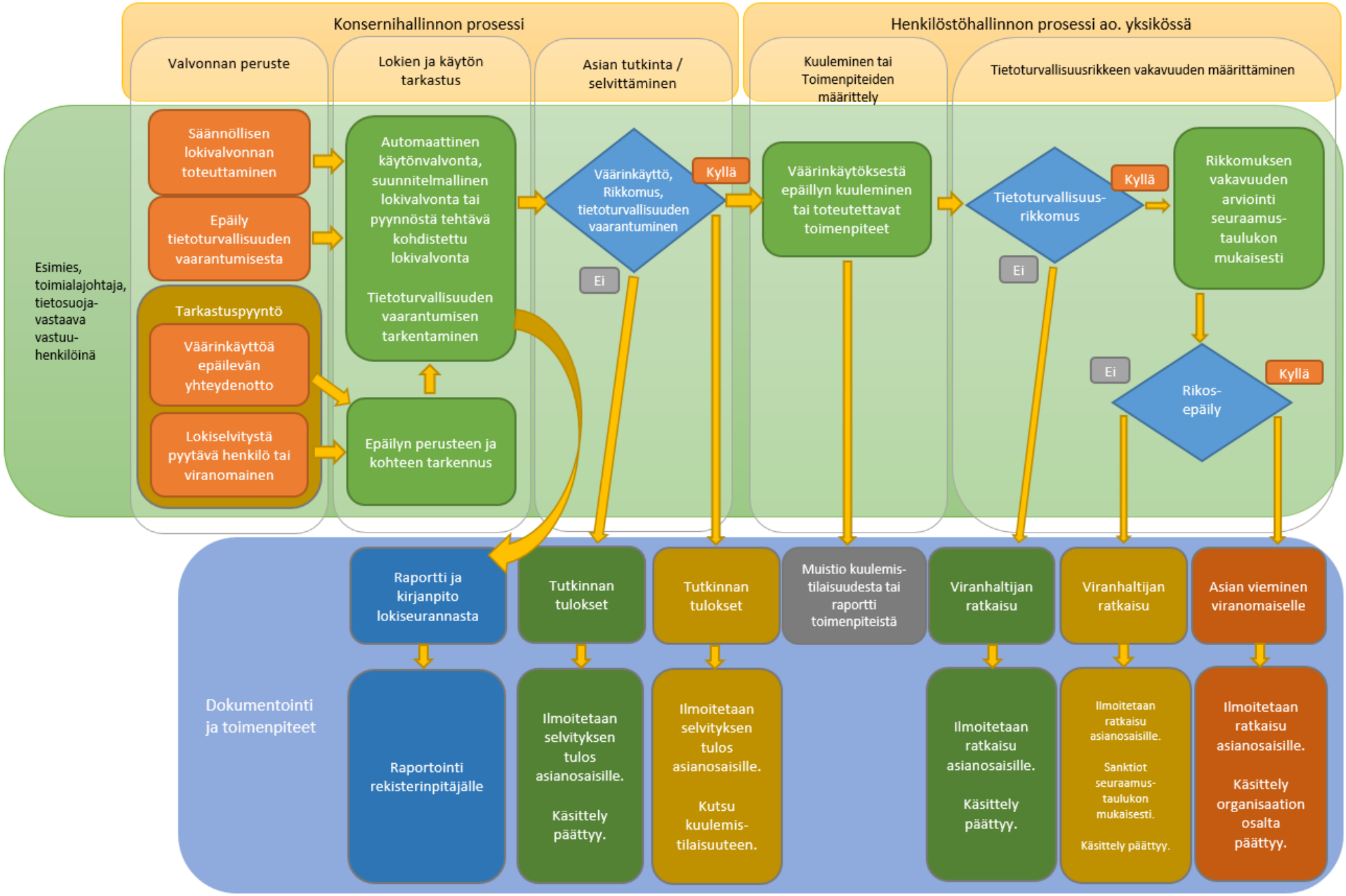
_____
Työntekijän nimi

_____ _____
Työntekijän allekirjoitus Esimiehen allekirjoitus

LIITE 2. Seuraamustaulukko henkilökunnalle / Versio 2 (**Vahti-ohjeen mukainen**)



LIITE 3. Lokivalvonnan ja tietoturvallisuuden vaarantumisepäilyn selvitysprosessi.



Tietoturva kuuluu jokaiselle

Käyttäjätunnukset

- Tunnukset ja salasanat ovat henkilökohtaisia, niitä ei saa luovuttaa muiden käyttöön ja säilytä salasanat, PIN-koodit, toimikortit ja muut kirjautumistunnisteet huolellisesti.
    - Käsittele näitä samoin kuin pankkikorttiasi ja tunnuslukuasi.
- Lukitse tietokoneesi, kun poistut sen läheisyydestä, nopeinta on käyttää näppäinyhdistelmää Win + L 

Luottamukselliset tiedot

- Muista keskustellessasi työkaverin tai asianosaisen kanssa, ettet paljasta luottamuksellisia tietoja sivullisille. Huomioi tämä myös puhelinkeskusteluissa.
- Mikäli käsittelet työsi vuoksi luottamuksellisia tietoja kotonasi tai matkoilla, muista huolehtia niiden salassapidosta.
- Kunnioita asiakkaiden ja työkaverien yksityisyyttä.

Tietosuoja-aineisto

- Huolehdi paperien, muistitikkujen ja muiden tallennusvälineiden, puhelinten, avainten, toimikorttien yms. asianmukaisesta käsittelystä ja säilytyksestä. Älä luovuta niitä sivullisten käyttöön.
- Säilytä salassa pidettävät tiedot asianmukaisesti, noudata ns. puhtaan pöydän periaatetta.
- Hävitä salassa pidettävät tiedot asianmukaisesti siten, etteivät sivulliset pääse näkemään niitä.
- Tieto tulee suojata sen kaikissa käsittelyvaiheissa.
    - Luominen, käyttäminen, muuttaminen, tallentaminen, siirtäminen Kerääminen, käsittely, tuhoaminen

Mobiililaitteet ja kannettavat tietokoneet

- Huolehdi etätyössä ja matkoilla mobiililaitteiden ja niiden kautta käytettävien salassa pidettävien tietojen suojaamisesta ulkopuolisten katseilta.
- Puhelin ja muut mobiililaitteet, joista on pääsy tietosuojan alaisiin tietoihin tai esim. sähköpostiin, tulee suojata PIN-koodilla tai salasanalla, kuvion piirtäminen ei ole riittävä suojaus.
- Huolehdi laitteiden valvonnasta, älä jätä niitä näkyville esim. autoon tai hotelliin.

Muuta huomioitavaa

- Anna ICT-tuen asentaa ohjelmistot ja tehdä niihin tarvittavat muutokset.
- Kerro tietosuojavastaavalle tai esimiehellesi, mikäli havaitset ongelmia tai rikkomuksia tietosuojan tai tietoturvan toteutumisessa tai tapahtuu jotain normaalista poikkeavaa.
- Työtiloihin ei tule tarpeettomasti päästää ulkopuolisia eikä jättää näihin ulkopuolisia yksinään.
    - Ovia ei saa kiilata auki esim. harjanvarrella tms.
    - Ulkopuolisia ei saa päästää lukittuihin tiloihin. Tapaamisen järjestänyt työntekijä huolehtii ovien avaamisen.
    - Kysy kuka ja millä asialla henkilö on, mikäli näet lukituissa tiloissa ulko-puolisia yksinään.
    - Lukitse toimiston ovi lähtiessäsi, ellei tiloihin jää toista työntekijää.
- Mikäli olet epävarma jostain, kysy.