PADASJOKI

TIETOTURVA- JA TIETOSUOJA-POLITIIKKA

KUNNANHALLITUS § XX

SISÄLLYS

JOHDANTO

Padasjoen kunnan palvelutuotannon ja muun toiminnan keskeisimpiä resursseja ovat tietoaineistot. Kunnan tiloissa ja niiden ulkopuolella tietoa käsittelevät kunnan henkilöstön lisäksi ulkoiset sidosryhmät ja asiakkaat. Tietoa esiintyy muiden muassa paperille tulostettuna, tallennettuna tietojärjestelmiin, kannettaviin laitteisiin ja muistivälineille sekä käyttäjien muistiin tallentuneena. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys ovat tärkeitä toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Ensisijainen vastuu tietoturvan ja tietosuojan toteutumisesta on organisaation ylimmällä johdolla, joka varmistaa tietoturva- ja tietosuojatyön riittävän resursoinnin ja seurannan. Tietoturva- ja tietosuojapolitiikka koskee kuitenkin jokaista työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee tietoaineistoja riippumatta sen esitystavasta, muodosta, elinkaaren vaiheesta tai tallennusympäristöstä.

Tietoturva- ja tietosuojapolitiikka määrittelee periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, jotka ohjaavat tietoturvan toteuttamista ja kehittämistä. Lisäksi alakohtaisia ohjeita ja määräyksiä annetaan tarpeen mukaan, ja ne tiedotetaan kaikille työntekijöille ja tietojärjestelmän käyttäjille.

Tietoturvaperiaatteita noudatetaan kaikissa tiedon elinkaaren vaiheissa, ja henkilöstön perehdytyksessä ja koulutuksessa korostetaan tietoturva- ja tietosuojaperiaatteiden merkitystä. Teknisillä ratkaisuilla varmistetaan, että toiminnan ja työtehtävien kannalta tarpeellista tietoa käsitellään asianmukaisesti ja rajoitetaan tarpeettoman tiedon saatavuutta.

Kunnanhallitus on hyväksynyt kunnan johtoryhmän tässä tietoturva- ja tietosuojapolitiikassa kuvaamat, kunnan strategian mukaiset periaatteet, tavoitteet ja vastuut. Asiakirja on julkinen ja voimassa toistaiseksi. Sitä tarkastellaan säännöllisesti ja täydennetään sekä päivitetään tarpeen mukaan lain tai muun ohjeistuksen muuttuessa.

TIETOTURVA

Kunnassa tietoturvallisuudella tarkoitetaan tiedon, tietojärjestelmien, tietoliikenteen ja palveluiden, sekä niiden käyttöympäristöjen ja käyttäjän itsensä turvaamista siten, että niihin kohdistuvat uhat eivät aiheuta merkittävää riskiä tiedon elinkaaren missään vaiheessa. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä.

Tietoturva on olennainen osa organisaatioiden toimintaa, ja sen hallinnolliset periaatteet ovat keskeisiä tietoturvan varmistamisessa. Nämä kolme tavoitetta muodostavat kokonaisvaltaisen tietoturvan viitekehyksen, jotka tukevat toisiaan ja mahdollistaa toimivan ja tehokkaan tietoturvan:

- **Luottamuksellisuus** tarkoittaa, että erilaiset tiedot ja järjestelmät ovat vain niiden käytössä, joilla on oikeus niihin. Esimerkiksi salasanoja ei tule jakaa muiden kanssa
- **Eheys** varmistaa, että tiedot ovat luotettavia, oikeita ja ajantasaisia. Tietojen ei tule muuttua tai olla muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena. Säännöllinen tietojen päivittäminen ja varmuuskopioinneista huolehtiminen ovat osa eheyden periaatetta.

- **Käytettävyys** tarkoittaa, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen henkilöiden käytettävissä etukäteen määritellyssä vasteajassa. Esimerkiksi sähköpostijärjestelmän tulee vastata pyyntöihin, jotta käytettävyys säilyy.

HALLINNOLLINEN TIETOTURVA

Hallinnollinen tietoturva on kaiken tietoturvallisuuden perusta ja sen avulla määritellään eri tietoturvan osa-alueiden tavoitteet, toimintatavat ja suuntaviivat. Johto seuraa ja ohjaa näiden periaatteiden toteutusta, jotta tietoturva on tehokasta ja kokonaisvaltaista.

- Organisaation johto määrittelee tietoturvan pääperiaatteet ja vastuut koko kunnan toiminnan osalta.
- Operatiivinen vastuu mm. ilmoittaminen tietohallinnolle puutteista, rikkomuksista ym. toimenpiteistä on esihenkilöillä.
- Tietoturvallisuuden avainhenkilöille annetaan koulutusta turvallisuuden ylläpitämiseksi.

Lisäksi tietoon sen käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan. Kunnan tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kunnan hallintojärjestelmää ja se liittyy kiinteästi kunnan kokonaisturvallisuuteen, joka muodostuu useasta osa-alueesta.

TURVALLISUUSJOHTAMINEN

Turvallisuusjohtaminen on kokonaisvaltaista toimintaa, joka kattaa sekä lakisääteisen että omaehtoisen turvallisuuden hallinnan. Se yhdistää menetelmien ja toimintatapojen sekä ihmisten johtamisen. Turvallisuusjohtamisen keskeinen ajatus on, että työpaikka parantaa turvallisuuttaan ennakoivasti, jatkuvasti ja kokonaisvaltaisesti.

Turvallisuusjohtamisen osa-alueita ovat esimerkiksi työturvallisuus, ympäristöturvallisuus, pelastusturvallisuus ja tietoturvallisuus. Se on osa normaalia yrityksen johtamista, jonka tavoitteena on varmistaa yrityksen toiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus kaikissa tilanteissa. Tietoturvallisuuden riskienhallinta on osa koko kuntaan tehtävää riskienhallintaa.

Turvallisuusjohtamisen keskeisiä työkaluja ovat riskien arviointi ja riskienhallinta. Riskien arviointi on laaja-alaista ja järjestelmällistä työn vaarojen ja terveyshaittojen tunnistamista ja niiden merkityksen arvioimista työntekijän turvallisuudelle ja terveydelle. Riskienhallinta on järjestelmällistä työtä toiminnan jatkuvuuden ja henkilöstön turvallisuuden varmistamiseksi.

HENKILÖSTÖTURVALLISUUS

Henkilöstöturvallisuus on henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvavastuut ja tehtävät on selkeästi perehdytetty. Henkilöstöturvallisuuteen pyritään vaikuttamaan palvelussuhteen kaikissa vaiheissa – rekrytointivaiheessa, työsuhteen aikana ja työsuhteen päätyttyä tehtävillä toimenpiteillä.

Työtehtävän mukainen käyttöoikeus järjestelmiin ja ohjelmistoihin annetaan käyttölupahakemus ja vaitiolo-/salassapitositoumus täyttämällä ja kuittaamalla se sille osoitetulla sivulla (Liite 1). Esihenkilö on vastuussa käyttölupahakemuksen laatimisesta ja työtehtävän määrittelystä tehtäväkuvauksessa. Esihenkilö huolehtii siitä, että tarvittavat luvat haetaan tietohallinnolta ja työntekijän tehtävät ja vastuut on selkeästi kuvattu.

FYYSINEN TURVALLISUUS

Fyysinen turvallisuus käsittää toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja ja siellä olevia ihmisiä, tietoa ja muuta omaisuutta suojataan fyysisiltä vahingoilta, vahingoittamisyrityksiltä, oikeudettomilta henkilöiltä ja erilaisilta kiinteistövahingoilta. Fyysistä turvallisuutta toteutetaan mm. vartioinnilla, kameravalvonnalla, kulunvalvonnalla ja turvallisilla rakenteilla.

TIETOAINEISTOTURVALLISUUS

Tietoaineistoturvallisuus kattaa useita osa-alueita organisaatiossa. Tämä sisältää:

- **Käyttörajoitetut digiympäristöt**: Tietoaineistot on säilytettävä turvallisissa tiloissa, jotka täyttävät luottamuksellisuuden, eheyden ja saatavuuden vaatimukset.
- **Tietovarantojen varmuuskopioinnit:** Tietojen varmuuskopiointi on olennaista palveluiden jatkuvuuden kannalta.
- **Tietoliikenneturvallisuus:** Toteutetaan palomuurein, liikennesuodatuksin ja useiden rinnakkaisten tietoliikenneyhteyksien avulla.

Tietoaineistoturvallisuus on tärkeä osa kokonaisvaltaista tietoturvaa, joka huomioi sekä tekniset että hallinnolliset näkökulmat. Tavoitteena on estää tietojen tuhoutuminen tai tahaton muuttuminen sekä varmistaa tietoaineistojen luokitus, suojaaminen, oikeanlainen käsittely, säilyttäminen ja hävittäminen.

LAITTEISTOTURVALLISUUS

Laitteistoturvallisuudella turvataan organisaation laitteistojen elinkaarta ja turvallista käyttöä. Tähän kuuluu:

- **Asennus ja suojaus:** Laitteet asennetaan huolellisesti ja suojataan vahingoilta ja varkauksilta.
- **Takuu ja ylläpito:** Palvelusopimukset pidetään ajan tasalla.
- **Tietojen asianmukainen tuhoaminen:** Kun laitteiden elinkaari päättyy, tietojen poistaminen on otettava huomioon.
- **Vastuut ja sopimukset:** Tietojärjestelmätoimittajilla ja ylläpitäjillä on omat vastuunsa laitteistoturvallisuuden osalta.
- **Toiminnan jatkuvuus**: Teknisin toimin pyritään varmistamaan tietojen keskeytyksetön käyttö ja toiminnan jatkuvuus.
- **Kriittiset laitteistot:** Kriittisille laitteistoille toteutetaan erityistoimenpiteitä, kuten katkoton sähkönsyöttö ja korkeamman ylläpidon palvelutaso.

OHJELMISTOTURVALLISUUS

Tietoturvaan liittyen pääsynhallinta on keskeinen käsite. Se tarkoittaa toimenpiteitä, joilla estetään luvaton pääsy tietoaineistoon, ohjelmiin ja järjestelmiin. Tämä voidaan toteuttaa esimerkiksi käyttäjätunnuksilla, salasanoilla, kaksivaiheisella tunnistautumisella ja oikeuksien rajoittamisella.

Ohjelmistojen hankintavaiheessa tietoturva otetaan huomioon varmistamalla, että hankittavat ohjelmistot täyttävät tietoturvavaatimukset ja ovat yhteensopivia olemassa olevien ohjelmistojen ja arkkitehtuurin kanssa. EU:n yleisen tietosuoja-asetuksen vaatimukset on myös otettava huomioon.

Ohjelmiston valmistajan ja myyjän vastuu määräytyy hankinta- ja käyttöoikeussopimuksissa. Esihenkilön vastuulla on perehdyttää alaiset ohjelmistojen tietoturvalliseen käyttöön. Ohjelmistojen hankinta on keskitetysti tietohallinnolla. Lisäksi ohjelmien asentaminen, suojaus, päivitykset ja varmuuskopiointi on sovittava tietohallinnon kanssa erikseen.

Perustana kunnan tietoturvatyössä käytetään ensi sijassa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) suosituksia ja Tietoturvatasojen kuvaaman perustason vaatimuksia (Tiedonhallintalaki (906/2019)).

TIETOTURVALLISUUSTAVOITTEET

Tietoturvatyön tavoitteena on kehittää Padasjoen kunnan toimintaympäristön digitaalisen turvallisuuden hallintaa ja siten varmistaa palvelutoiminnan luotettavuus ja jatkuvuus. Tietoturvatyö on keskeinen osa kunnan johtamista ja riskienhallintaa ja sen avulla luodaan yhdenmukaiset tietoturvakäytänteet hallintosäännöstä johdettuja periaatteita noudattaen.

Kunnan tietoturvallisuustavoitteet ovat

- Kokonaisvalainen tietoturvan johtaminen.
    - riskienhallinta
    - henkilöturvallisuus
    - henkilöstön kouluttaminen
- Uhkatekijöiden tunnistaminen.
- Ennaltaehkäisy sekä tiedon suojaaminen.
- Tekniset ja hallinnolliset tietoturvajärjestelyt täyttävät keskeisiltä osin Perustason vaatimukset.

Tietojen oikeaoppinen ja tarkoituksenmukainen käsittely turvataan yhdenmukaisilla tietoturva- ja tietosuojakäytänteillä, jotka ovat tiedonhallintalain edellyttämiä. Tietoturvatyössä kansallisen tason verkostoitumisella edistetään kunnan sekä yhteiskunnan tavoitteiden ja strategioiden toteuttamista. Tietoturvallisilla palveluilla ja tietosuoja huomioiden varmistetaan kuntalaisten luottamus kunnan palvelutuotantoon.

TIETOJÄRJESTELMIEN KÄYTTÖ

Kunnan käytössä olevat ICT-palvelut, -järjestelmät, -laitteet ja -ohjelmistot, on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmiä ei tule käyttää toimintaan mikä saattaa, välittömästi tai välillisesti, vaarantaa kunnan vastuulla olevan tiedon ja/tai järjestelmien turvallisuuden ja aiheuttaa haittaa kunnalle, sen toiminnalle tai käyttäjälle itselleen.

Tietojärjestelmien vähäinen käyttö henkilökohtaisiin tarkoituksiin on sallittu omalla ajalla. Henkilökohtainen käyttö ei kuitenkaan saa aiheuttaa ylimääräisiä kustannuksia kunnalle, eikä vaarantaa kunnan tietoa tai tietojärjestelmiä.

Tietojärjestelmiä, laitteita ja ohjelmistoja kunnan hallinnon käytössä olevaan tietoverkkoon saa asentaa vain kunnan it-palvelut tai kunnan valtuuttama taho.

Käyttöoikeudet kunnan tietojärjestelmiin ja tietoon myönnetään vain kunnan tehtävien hoitoon liittyen. Pääsääntöisesti tarvittavat oikeudet määrittelee esihenkilö.

Tietojärjestelmien turvallinen käyttäminen etätyötä tehtäessä vaati etätyöntekijältä erityistä huolellisuutta ja sitoutumista tietoturvaohjeiden noudattamiseen.

Tietoturvarikkomukset ovat vakavia rikkeitä, joita säätelevät sekä työsopimuslaki että viranhaltijalaki. Lisäksi henkilötietoihin kohdistuvat rikkomukset kuuluvat EU:n yleisen tietosuoja-asetuksen sekä kansallisten lakien ja asetusten, kuten rikoslain, piiriin.

Organisaation tietoturva- ja tietosuojapolitiikan sekä näiden pohjalta annettujen ohjeiden vastaiset rikkomukset tulee aina raportoida tietosuojavastaavalle tai esihenkilölle. Tietosuojavastaava ja vastaava viranhaltija johtavat valvontaprosessia ja päättävät seuraamuksista seuraamustaulukon mukaisesti.

Rikkomusten seuraukset voivat vaihdella tapauskohtaisesti. Ne voivat sisältää käyttöoikeuden rajoituksia, palvelussuhteeseen liittyviä seuraamuksia sekä rikoslaissa määriteltyjä seuraamuksia.

TIETOSUOJA

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuoja koskee kaikkia tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tietosuoja varmistaa, että organisaatiot käsittelevät henkilötietoja lainmukaisesti ja vain silloin, kun niiden käsittelyyn on lainmukainen peruste. Tietosuojan ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus. Tietosuojaan kuuluu myös oikeus tarkastaa ja tarvittaessa korjata henkilötietoja.

Tietosuoja on erityisen tärkeä nykypäivän digitaalisessa ympäristössä, jossa tietoturvauhat ovat jatkuvasti läsnä. Tietosuoja ja tietoturva ovat läheisesti yhteydessä toisiinsa: tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät.

HENKILÖTIETOJEN KÄSITTELYN PERIAATTEET

EU:n yleisen tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn periaatteet ovat seuraavat:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys: Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.
- Käyttötarkoitussidonnaisuus: Henkilötiedot on kerättävä tiettyä laillista tarkoitusta varten ja niitä saa käsitellä vain niin kauan kuin se on tarpeen kyseisen tarkoituksen kannalta.
- Tietojen minimointi: Henkilötietojen käsittelyn tulee olla tarpeellista ja rajoittua vain niihin tietoihin, jotka ovat välttämättömiä käsittelyn tarkoituksen kannalta.
- Täsmällisyys: Henkilötiedot on pidettävä ajan tasalla, ja virheelliset tiedot on poistettava tai korjattava ilman aiheetonta viivytystä.
- Säilytysajan rajoittaminen: Henkilötietoja saa säilyttää muodossa, josta rekisteröity on tunnistettavissa, vain niin kauan kuin se on tarpeen henkilötietojen käsittelyn tarkoituksen kannalta.
- Eheys ja luottamuksellisuus: Henkilötietoja on käsiteltävä tavalla, joka takaa niiden asianmukaisen turvallisuuden, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Periaatteiden noudattaminen on tärkeässä osassa kunnan toimintaa, sillä ne varmistavat, että henkilötietoja käsitellään oikeudenmukaisesti, läpinäkyvästi ja turvallisesti, mikä puolestaan auttaa suojaamaan yksilöiden yksityisyyttä.

SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Tietoturvan ja tietosuojan seuranta, ylläpito ja kehittäminen ovat keskeisiä tehtäviä organisaatiossa. Ne tulee sovittaa yhteen palveluiden, toimintatapojen ja teknisten ratkaisujen kehittämisen kanssa. Lisäksi säännöllinen tiedottaminen, osaamisen ylläpito ja koulutus ovat olennaisessa roolissa tietoturvallisuuden kehittämisessä.

Tietoturva ja tietosuoja vaativat jatkuvaa seurantaa sekä tarpeenmukaista raportointia kunnan johdolle. Seurannan ja raportoinnin vastuu kuuluu pääosin IT-palveluille sekä tietosuojavastaavalle, mutta jokaisella on velvollisuus raportoida havaituista poikkeamista esihenkilölleen. Esihenkilön vastuulla on dokumentoida havaitut poikkeamat ja ilmoittaa näistä eteenpäin tietosuojavastaavalle.

RISKIENHALLINTA

Tietoturva ja tietosuoja on kiinteä osa kunnan riskienhallintakäytäntöjä ja kuuluu jokaisen työntekijän vastuulle. Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä kartoitetaan, analysoidaan ja hallitaan järjestelmällisesti. Henkilöstön osaaminen ja tietoisuus ovat merkittäviä tekijöitä uhkien pienentämisessä.

Riskienhallintakäytäntöjen tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että käytetyt keinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen.

- **Riskien tunnistaminen:** Tulee tunnistaa mahdolliset tietoturva- ja tietosuojauhat. Tämä sisältää teknisiä, organisatorisia ja inhimillisiä riskejä.
- **Riskien arviointi:** Täytyy arvioida riskien vakavuus ja todennäköisyys. Tämä sisältää arvioinnin siitä, mitä vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Vahingot voivat olla fyysisiä, aineellisia tai aineettomia.
- **Riskien hallinta:** Riskien hallintaan kuuluu toimenpiteiden suunnittelu ja toteuttaminen riskien vähentämiseksi. Tämä sisältää teknisiä ja organisatorisia toimenpiteitä, kuten tietojärjestelmien tietoturvaa, tietojen salausta ja muita suojatoimenpiteitä.
- **Seuranta ja tarkistus:** Riskienarviointia on tarkistettava säännöllisesti ja päivitettävä tarvittaessa. Tämä varmistaa, että riskienhallinta on ajan tasalla ja vastaa organisaation nykyisiä tarpeita.
- **Dokumentointi:** Riskienarviointi ja siihen liittyvät toimenpiteet on dokumentoitava säännöllisesti. Tällä tavoin organisaatio osoittaa noudattavansa tietosuojasääntelyä.

JATKUVUUDENHALLINTA JA VARAUTUMINEN

Kunnan toiminnassa on tärkeää tunnistaa ja ennakoida riskit, jotka saattavat uhata toiminnan jatkuvuutta. Tämä sisältää valmistautumisen mahdollisiin riskeihin laatimalla valmiussuunnitelman sekä toteuttamalla niihin liittyviä varajärjestelyjä.

Jatkuvuuden varmistamiseksi painopiste on ongelmien ja riskien ennaltaehkäisyssä sekä kyvyssä nopeaan palautumiseen poikkeamatilanteista. Tämä sisältää myös valmistautumisen kyberuhkiin ja kyberturvallisuuden suojauskäytäntöjen riittävyyden arvioinnin.

Lisäksi kunnan sopimuskumppaneilta odotetaan säännöllistä toiminnan jatkuvuutta uhkaavien riskien tunnistamista sekä ajantasaisia jatkuvuus- ja toipumissuunnitelmia. Tämä varmistaa, että kaikki osapuolet ovat valmiita vastaamaan mahdollisiin haasteisiin ja takaamaan toiminnan jatkuvuuden.

ROOLIT JA VASTUUT

Kunnan tietoturvallisuuteen liittyvät roolit ja vastuut ovat seuraavat:

KUNNANHALLITUS

- Tietoturvapolitiikan hyväksyminen.
- Kantaa ylimmän vastuun tietoturvan toteutumisesta.

KUNNANJOHTAJA

- Tietoturvan ja tietosuojan järjestäminen ja toimintaedellytysten luominen.
- Poikkeusolojen viestinnän johtaminen.
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa.
- Tietoturvaohjeiden ja muiden vastaavien ohjeiden vahvistaminen.

TOIMIALAJOHTAJAT

- Vastuullisen nimeäminen tietojärjestelmille.
- Tietoturvallisuuden toteutuminen omalla toimialallaan.

HALLINTOJOHTAJA

- Kunnan tietouden ylläpitäminen koskien tietoturvallisuuteen vaikuttavia lakeja, säädöksiä ja määräyksiä, sekä huolehtiminen niiden huomioimisesta tietoturvallisuustoiminnassa.
- Henkilöstöturvallisuuden ja henkilöstötietojen käytön ohjaus ja koordinointi työntekijän palvelussuhteen kaikissa vaiheissa.

ASIANHALLINTARYHMÄ

- Myös tietoturvaryhmä
    - Tietoturvallisuuden suunnittelu, ohjaus, seuranta ja kehittäminen.
    - Teknisen tietoturvallisuuden minimivaatimusten määrittely, toteutus, ohjaus ja valvonta kunnan tietojärjestelmäympäristössä.
    - Tietoturvallisuuden teknisen valvonnan toteutuminen tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.
    - Tietoturvariskien ja -poikkeamien hallinnan koordinointi.
    - Tietoturvallisuuden tilan raportointi kunnan johdolle.
- Yksiköiden arkistonmuodostuksen ohjaaminen ja neuvonta.

- Laatii tiedonhallinnan ohjeet ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti.
- Huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta.
- Kunnanarkistoon siirretyistä asiakirjoista huolehtiminen ja niistä tietojen antaminen.

TIETOSUOJAVASTAAVA

- Auttaa johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä.
- Auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja mahdollisten erityislakien edellyttämän tietosuojan tason.
- Seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuoda esiin havaitsemiaan puutteita.
- On rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa.
- Tietosuojavastaava toimii yhteyshenkilönä valtakunnalliseen tietosuojavaltuutettuun ja tekee tarvittaessa ilmoitukset tietosuojaloukkauksista.
- Tietosuojavastaavalla on nimetty varahenkilö.

PÄÄKÄYTTÄJÄ

- Tietoturvan toteutumisen valvonta omalla vastuualueellaan.
- Sovelluksen ylläpitotoiminnoista huolehtiminen ja varmistaminen, että järjestelmää käytetään lakien, säädösten ja ohjeiden mukaisesti.
- Tietosuojavastaavien avustaminen, henkilöstön neuvonta ja kouluttaminen.
- Käyttäjien ja käyttöoikeuksien toteuttaminen.

ESIHENKILÖ

- Oman vastuualueensa henkilöstön perehdyttäminen työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin.
- Henkilöstön tietoturva- ja tietosuojapolitiikan 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 IT-palveluille käyttöoikeuksien päättämisestä tai muuttamisesta.
- Raportointi näistä asioista toimialajohdon lisäksi tietoturvavastaavalle.

HENKILÖSTÖ JA LUOTTAMUSHENKILÖT

- Määräysten ja ohjeiden noudattaminen.
- Tietoturvaan tai tietosuojaan liittyvien poikkeuksien, uhkien ja riskien välitön ilmoittaminen joko esihenkilölle, tietohallintoon tai tietosuojavastaaville.

KÄYTTÖOIKEUSHAKEMUS JA SITOUMUS 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 työsuhteen alkaessa, sijaisten, opiskelijoiden ja harjoittelijoiden kanssa ensimmäisen palvelusuhteen alkaessa tai palvelusuhteen luonteen muuttuessa.
- Jokainen työntekijä vastaa oman toimintansa tietoturvallisuudesta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.
- Työnantajan tietoturva- ja tietosuojaohjeet sekä muut täydentävät tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Esihenkilön velvollisuus on uuden työntekijän perehdytyksen yhteydessä läpikäydä henkilöstön tietoturva- ja tietosuojaohjeet.

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 yhteydessä. Tietojen luovutuksen tulee perustua aina 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, taloudellista asemaa tai sosiaalisia etuuksia koskevat tiedot sekä turvallisuuteen, tietojärjestelmiin ja kiinteistöön liittyvät tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja. En käsittele esim. työkavereiden, lähiomaisten, naapureiden tai julkisuuden henkilöiden tietoja, mikäli työtehtäväni eivät sitä sillä hetkellä edellytä.
- Vastaan käyttäjätunnuksillani ja/tai varmennekortin tunnuksillani tapahtuvasta tietojen käytöstä. Tunnuksia ei saa luovuttaa 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 esihenkilölleni 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 henkilörekisteritoiminnassa 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.

Paikka ja aika: _____ ____/____20___

_____ _____

Työntekijän nimi Työyksikkö

_____ _____

Liite 1

Työntekijän allekirjoitus

Esihenkilön allekirjoitus

TIETOJÄRJESTELMIEN VÄÄRINKÄYTÖN SEURAAMUKSET

Tietotekniikkarikkomuksia ovat kunnan tietojärjestelmien käyttö niiden käytöstä annettujen sääntöjen tai määräysten vastaisesti tai niiden käyttö Suomen lakien vastaisesti.

Tämä toimintaohje kuvaa toimenpiteitä, joita henkilöön kohdistetaan, kun tietotekniikkarikkomus on havaittu tai sitä on perustellusti syytä epäillä. Toimenpiteet on jaettu käyttövaltuuksien rajoituksiin rikkomuksen selvitystyön ajaksi sekä mahdollisiin rikkomuksesta määriteltyihin seuraamuksiin.

Tämän ohjeen ensisijainen tarkoitus on kuvata millaisiin toimenpiteisiin ja seuraamuksiin tietojärjestelmien väärinkäyttö voi johtaa. Mahdolliset seuraamukset käsitellään kunnassa tietoturvaperiaatteiden mukaisesti soveltaen tapauskohtaista harkintaa. Mikäli kunta katsoo tietotekniikkarikkomuksen täyttävän myös rikoksen tunnusmerkit, saatetaan asia viranomaisten käsiteltäväksi, jolloin mahdollisista seuraamuksista päättää viimekädessä toimivaltainen tuomioistuin.

KÄYTTÖVALTUUKSIEN RAJOITUS

Padasjoen kunta voi rajoittaa käyttövaltuuksia selvitystyön ajaksi. Rajoituksista päätetään, kun tietotekniikkarikkomus on havaittu tai sitä epäillään. Valtuuksia rajoitetaan aina, kun perustelluista syistä epäillään, että käyttäjä on syyllistynyt väärinkäytökseen, ja on mahdollista, että käyttövaltuudesta on haittaa rikkomuksen selvittämiselle tai vahinkojen minimoimiselle. Tarvittaessa käyttäjä kutsutaan kuultavaksi ja käyttäjällä on aina oikeus tulla kuulluksi asiassa.

Käyttövaltuuksien rajoittamisesta päättää toimialajohtaja tai hänen määräämänsä henkilö. Rajoittamisen toteuttaa palvelun ylläpitäjä.

Kiireellisissä tapauksissa ylläpitäjä voi omalla päätöksellään rajoittaa käyttövaltuuksia enintään kolmeksi työpäiväksi, mistä hänen tulee välittömästi ilmoittaa lähiesihenkilölle, toimialajohtajalle sekä kunnan tietosuojavastaavalle.

Tarvittaessa käyttäjän työasema tai muu laite voidaan kytkeä irti verkosta.

Rajoitukset voidaan purkaa selvitystyön päätyttyä, jos käyttövaltuuksien palauttamisesta ei ole ilmeistä haittaa.

Käyttäjään kohdistuvista seuraamuksista voi valittaa seuraamuksesta päättäneen henkilön esihenkilölle.

SEURAAMUKSET

Lievissä tapauksissa lähiesihenkilö puhuttelee asianosaista asiattomasta toiminnasta.

Tietotekniikkarikkomuksen seurauksena käyttäjä voi olla korvausvastuussa väärinkäyttämistään resursseista (esimerkiksi palvelimet tai tietoverkko), välittömistä vahingoista ja väärinkäytön selvitystyön aiheuttamista kustannuksista.

Seuraamuksiin vaikuttaa rikkomuksen vakavuuden lisäksi teon tahallisuuden aste.

SEURAAMUKSET OPISKELIJALLE

Opiskelijalle kohdistettavia seuraamuksia voivat olla rehtorin tekemä puhuttelu, käyttäjätunnukseen perustuva toiminnan seuraaminen, käyttövaltuuksien rajoitus tai koulun hallinnolliset toimet (kirjallinen varoitus, määräaikainen erottaminen) ja rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Kirjallisen varoituksen antamisesta opiskelijalle päättää rehtori ja määräaikaisesta erottamisesta monialainen toimielin. Henkilön käyttövaltuudet perutaan erottamisen ajaksi.

Mahdollisten rikosilmoitusten tekemisestä päättää sivistysjohtaja lakimiehen valmistelun perusteella.

SEURAAMUKSET HENKILÖKUNTAAN KUULUVALLE

Henkilökuntaa koskevia seuraamuksia voivat olla kunnan työoikeudelliset toimet (puhuttelu, kirjallinen varoitus, irtisanominen, palvelussuhteen purku) sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä väärinkäytöksen vuoksi evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista päättää IT-asiantuntija yhdessä toimialajohtajan kanssa. Henkilökuntaa koskevista työoikeudellisista toimista päättää esihenkilö. Mahdollisten rikosilmoitusten tekemisestä päättää toimialajohtaja lakimiehen valmistelun perusteella.

SEURAAMUKSET MUILLE KÄYTTÄJILLE

Kunnan henkilökuntaan tai opiskelijoihin kuulumattomia käyttäjiä koskevat seuraamukset voivat olla käyttövaltuuksien poistaminen tai rajoittaminen sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksen vuoksi evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista luottamushenkilön tilanteessa päättää kunnanhallituksen puheenjohtaja yhdessä IT-asiantuntijan kanssa. Mahdollisten rikosilmoitusten tekemisestä päättää kunnanhallituksen puheenjohtaja ja kunnanjohtaja lakimiehen valmistelun perusteella.

KÄYTTÖSÄÄNTÖJEN RIKKOMISEN SEURAAMUSTAULUKKO

Taulukossa esitellään mahdollisia käyttösääntöjen vastaisen toiminnan seuraamuksia. Taulukko ei ole ehdoton sääntö vaan antaa pohjaa seuraamusten harkinnalle.

Kaikissa tapauksissa voidaan harkita yksittäisten järjestelmien käyttövaltuuden menettämistä väärinkäytöksen vuoksi määräajaksi tai pysyvästi.

Vakavia rikkomuksia ovat esimerkiksi salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen, hakkerointi ja tunkeutuminen tietojärjestelmiin, vahingonteko kuten tietoliikenteen häirintä tai haittaohjelmien levittäminen.

Esimerkkejä rikkomuksista ovat ohjeiden vastainen laitteistojen käyttö, käyttäjätunnuksen luovuttaminen esimerkiksi kertomalla salasana toiselle käyttäjälle, tiedon luottamuksellisuuden vaarantaminen esimerkiksi

luovuttamalla henkilötietoja oikeudettomasti, tekijänoikeudella suojatun materiaalin luvaton kopiointi tai jakelu ja tietoliikennettä ohjaavien laitteiden tai ohjelmien luvaton asentaminen verkkoon.

Esimerkkejä lievistä rikkomuksia ovat henkilökohtaisen tietoturvan tai tietosuojan laiminlyönti esimerkiksi käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin, luvaton kaupallinen tai poliittinen toiminta kuten sähköpostin käyttäminen henkilökohtaiseen markkinointiin, kulunvalvontaohjeiden rikkominen kuten avainten luovuttaminen toisen käyttöön.

Rikkomuksen vakavuus	**Tahallisuuden aste**			
	Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus		Piittaamattomuus, tahallisuus, toistuvuus	
	Opiskelijat	**Henkilökunta**	**Opiskelijat**	**Henkilökunta**
Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)	Puhuttelu, käyttövaltuuksien rajoitus	Käyttövaltuuksien rajoitus, rikosilmoitus, puhuttelu, kirjallinen varoitus	Rikosilmoitus, määräaikainen erottaminen, käyttövaltuuksien rajoitus	Rikosilmoitus, kirjallinen varoitus, palvelussuhteen päättämismenettely
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen)	Puhuttelu, opastus	Puhuttelu, opastus	Rikosilmoituksen harkinta, kirjallinen varoitus, käyttövaltuuksien rajoitus	Rikosilmoituksen harkinta, puhuttelu, kirjallinen varoitus, palvelussuhteen päättämismenettelyn harkinta
Lievä rikkomus (asiaton toiminta tai väärinkäytös)	Puheeksi ottaminen ja opastus	Puheeksi ottaminen ja opastus	Puhuttelu, toiminnan seuraaminen	Puhuttelu, kirjallinen varoitus