

# Vetelin kunnan tietoturvaohje

## 1. Yleistä ja avainkäsitteet

Vetelin kunnan tietoturvaohje koskee sekä henkilöstöä että luottamushenkilöitä. Tietoturvaohje on tärkeä osa kunnan riskienhallintaa ja kunnan toiminnan kehittämistä. Asiakirja määrittelee kunnan tietoturvatyön tavoitteet sekä tietoturvan ja tietosuojan toteuttamisen, seurannan ja vastuut. Tietoturvaohjeen nojalla annetaan käytännön määräyksiä tietoturvallisuuden toteuttamiseksi.

Tietoturvallisuuteen kuuluvat kaikki ne järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys, luottamuksellisuus ja turvallinen käsittely. Tietosuojalla tarkoitetaan henkilötietojen asianmukaista käsittelyä yksityisyyden suojan toteuttamiseksi. Tietosuoja rakentuu hyvälle tietoturvalle.

Tietoturvatyön päämääränä on taata kunnan tietojärjestelmien häiriötön toiminta siten, että tietojen käsittely pohjautuu luottamuksellisuudelle, eheydelle ja käytettävyydelle sekä turvalliselle käsittelylle.

**Käytettävyys** tarkoittaa, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Käytettävyyttä uhkaavat mm. ennakoimattomat tietokoneiden, tietoliikenneverkkojen ja tietokoneohjelmien rikkoutumiset. Ne voivat aiheutua esimerkiksi jonkin teknisen osan yllättävästä vikaantumisesta, käyttäjän inhimillisestä virheestä tai rikollisen tahon tekemästä haittaohjelmasta tai kyberhyökkäyksestä.

**Eheys** tarkoittaa, että tieto on yhtäpitävä alkuperäisen tiedon kanssa. Eheyttä uhkaavat mm. inhimilliset virheet tai väärinkäsitykset tietokoneohjelmien rakentamisessa tai tietojen tallennuksessa. Eheyttä uhkaavat myös rikollisten tahojen tarkoituksellisesti tekemät tietojen muuttamiset esimerkiksi rahaliikenteen käsittelyssä tai Internet-sivustojen sisällössä.

**Luottamuksellisuus** tarkoittaa, että kukaan sivullinen ei saa tietoa tai ei voi käsitellä sitä. Luottamuksellisuutta uhkaavat samat seikat kuin eheyttäkin. Lisäksi luottamuksellisuus on uhattuna, jos tiedon käsittelyn käyttöoikeushallinnan prosessit tai niiden toteutus on hoidettu huonosti.

Käyttöoikeuksien hallinnalla varmistetaan henkilöiden pääsy niihin tietoihin, joita he tarvitsevat työtehtäviensä suorittamiseen ja vastaavasti ulkopuolisten pääsy tietoihin. **Tietoturvallisuudessa ei ole kyse vain tekniikasta, vaan ihmisten työskentelytavoista.** Kyse ei ole myöskään vain yksittäisistä toimenpiteistä, vaan jatkuvasta ja suunnitelmallisesta toiminnasta. Henkilöstö perehdytetään tietoturvaohjeen mukaiseen tietoturvaan ja tietosuojaan palvelussuhteen alussa sekä osaamista ylläpitävällä koulutuksella sekä sitoutetaan noudattamaan tietoturva- ja

tietosuojaohjeita. Tärkeintä tietoturvapoliitiikan toteuttamista on jokaisen käyttäjän arkipäiväinen oikeanlainen toiminta.

## **2. Tietoturvatyön tavoitteet ja toimijat**

Vetelin kunnan tietoturvatyön tavoitteena on turvata kunnan tehtävissä tietojen käsittely, säilytys ja arkistointi tietoturvan ja tietosuojan järjestämistä koskevien säännösten ja lakien mukaisesti. Tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

### **Vetelin kunnan tietoturva- ja tietosuojatyön tavoitteet ovat seuraavat**

- \* tarjota ja kehittää kunnan palvelujen käyttäjille tietoturvallisia ja laadukkaita palveluita,
- \* tarjota kunnan henkilöstölle turvallinen käyttöympäristö työskentelyyn,
- \* turvata henkilöille yksityisyyden suoja lainsäädännön edellyttämällä tavalla,
- \* kehittää sekä teknistä että käyttäjästä lähtevää tietoturvaa ja siten turvata kunnan toiminnalle tärkeiden tietojärjestelmä- ja tietoverkkotoimintojen keskeytymätön toiminta ja estää niiden valtuudeton käyttö, tahaton tai tahallinen tuhoutuminen tai tiedon vääristäminen,
- \* kehittää kunnan sisäistä tietoturvakulttuuria ohjeistuksen ja koulutuksen avulla ja siten huolehtia siitä, että jokainen kunnassa työskentelevä ymmärtää velvollisuutensa tietoturvallisuuden toteutumisessa,
- \* tehdä tietoteknistä yhteistyötä seutukunnan kuntien ja KaseNet Oy:n kanssa tietoturvallisuuden seurannan, tietoturvariskitilanteisiin varautumisen ja niistä toipumisen osalta sekä hankittujen ja hankittavien tietojärjestelmien hallinnan osalta
- \* pitää yllä suunnitelmallista ja jatkuvaa kehittämistoimintaa uhkien ja riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. Normaaliajan tietojen käsittelyn turvaamisen kunta ja verkkopalveluoperaattori KaseNet Oy varautuu myös häiriö- ja poikkeusoloihin siten, että toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa ja normaalitilanteeseen päästään palaamaan mahdollisimman nopeasti.

## **3. Toteutus**

Vetelin kunnan tietoturvatyötä toteutetaan voimassaolevaa lainsäädäntöä ja tätä tietoturvaohjetta noudattamalla. Työtapoja ja osaamista kehitetään koulutuksen ja opastuksen avulla sekä henkilöstön oman aktiivisuuden ja palautteen avulla.

Työtehtävissä käytetään kunnan hankkimia laitteita ja ohjelmistoja, mikä huomioidaan myös etätyön suunnittelussa. Mikäli etätyötä ei voida tehdä työnantajan laitteilla, Office365-ympäristössä voi työskennellä myös omalta laitteelta käsin. Tietoturvasta etätyössä tulee tiedustella etukäteen it-asiantuntijalta. Kunnan tilojen käytössä noudatetaan annettuja ohjeita. Tietojärjestelmien ja tiedon keskeytymätön käyttö varmistetaan pääsyn- ja käytönvalvonnalla käyttöoikeuksin. Toiminnan jatkuvuus turvataan varautumalla poikkeustilanteisiin ja ymmärtämällä tietoturvallisuus yhdeksi kunnan varautumistoiminnan keskeisimmäksi kohteeksi.

#### **4. Tietoturvatyön organisointi ja vastuut**

**Hallinnollinen tietoturvallisuus** tarkoittaa organisaatiossa käytettäviä

tietoturvallisuuden toimintatapoja, toiminnan linjauksia, johtamista, organisointia, toimintojen sijoitusta organisaatioon, resursointia sekä vastuiden määrittelyä. Hallinnollisesta tietoturvasta vastaavat kunnan johto, jota edustaa kunnanhallitus, kunnanjohtaja ja toimialajohtajat. Kunnanhallitus hyväksyy tietoturvaohjeen ja päättää mahdollisista muutoksista ohjeeseen. Kunnanjohtaja ja toimialajohtajat huolehtivat toimialojen käytäntöjen tietoturvallisuudesta ja niiden yhdenmukaisuudesta. Kunnan tietoturvavastaavana toimii it-asiantuntija, jolla on oikeus antaa henkilöstölle sitovia tietoturvaohjeita. Hallinnollisen tietoturvan osana johdon ja esihenkilöstön tuki on tärkeää toimivan tietoturvakulttuurin olemassaololle.

**Henkilöstötietoturvallisuus** on tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation tietojen ja tietojenkäsittelyn suojaamista ihmisten aiheuttamilta tahallisilta sekä tahattomilta uhkilta ja ihmisten toimista tietoturvallisuuden varmistajina.

**Käyttöturvallisuus** tarkoittaa organisaation automaattisen ja manuaalisen tietojenkäsittelyn suojaamiseen liittyviä asioita.

**Tietoaineistoturvallisuus** tarkastelee eri talletusmuodoissa olevia organisaation päivittäessä toiminnassa tarvitsemia tietoja sekä niiden suojaamiseen liittyviä asioita. Tallennettavien tietojen, skannattavien ja säilytettävien asiakirjojen käsittelystä arkistonmuodostussuunnitelman mukaisesti huolehtivat osastoilla tietoaineistoja käsittelevät henkilöt. KaseNet Oy vastaa kunnan palvelimien varmuuskoopioiden ottamisesta. Pilvipohjaisten tietojärjestelmän kuten työajanseurannan ylläpidosta, toimintavarmuudesta ja varmuuskopioista vastaa palvelun tuottaja.

**Fyysinen tietoturvallisuus** tarkoittaa tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyviä asioita, joilla pyritään estämään organisaation tarvitsemien tietojen sekä fyysisen ja ei-fyysisen ominaisuuden tuhoutuminen, vahingoittuminen tai joutuminen väärin käsiin. Fyysinen tietoturvallisuus on myös tietojen käytettävyyden ylläpitoa, siltä osin kuin tilaratkaisut voivat sitä palvella tai mahdollisesti olla esteenä. Kulunvalvonnasta ja kiinteistöjen sekä laitteistojen suojaamisesta fyysisiä vahinkoja vastaan huolehtii tekninen toimiala huomioiden

toiminnassaan ohjeet omaisuuden hoidosta. Jokainen käyttäjä huolehtii laitteidensa ohjeiden mukaisesta käytöstä ja sijoittelusta työpisteessään. Etätyössä olevan tulee huolehtia, että etätyötila soveltuu työskentelyyn myös tietoturvan kannalta.

**Ohjelmistoturvallisuus** tarkoittaa organisaation käyttämien tietokoneohjelmien suojaamista sekä ohjelmien lisensointia ja rekisteröintiä. Ohjelmistoturvallisuudesta vastaavat it-asiantuntija ja pääkäyttäjät. Jokainen käyttäjä vastaa ohjelmistojen ohjeiden mukaisesta käytöstä ja on velvollinen ilmoittamaan havaitsemistaan tietoturvapoikkeamista tietosuojavastaavalle.

**Laitteistoturvallisuus** tarkoittaa organisaation käyttämien tietojenkäsittely- ja tietoliikennelaitteiden suojaamista. Siinä huolehditaan myös tietoteknisten laitteiden toimintavarmuudesta, asentamisesta sekä laitteiden käytössä tarvittavasta tietoturvasta. Kouluverkon laitteiden ylläpidosta vastaavat yläkoulussa ja lukiolla erikseen nimetty henkilö kunnan it-asiantuntijan johdolla.

**Tietoliikenneturvallisuus** tarkoittaa organisaation käyttämien tietoverkkojen ja niissä tapahtuvien tietoliikenteen suojaamiseen liittyviä asioita. Tietoliikenneturvallisuudesta huolehtii palvelun tarjoaja KaseNet yhdessä kunnan it-asiantuntijan kanssa.

### **Tietoturvan toteutumisen vastuunjako**

Tietoturvan toteutumisesta vastaa koko kunnan henkilöstö noudattamalla annettuja ohjeistuksia ja määräyksiä ja ilmoittamalla esihenkilölle ja/tai it-asiantuntijalle (tietoturvavastaavalle) havaitsemistaan epäkohdista tai tietoturvahuolta herättävästä toiminnasta. It-asiantuntija huolehtii lähiesihenkilöiden päätösten mukaisesti henkilöstön käyttöoikeuksien hallinnasta kunnan verkkoihin, työasemiin ja sähköpostiin. Lähiesihenkilöiden tulee yhdessä järjestelmän pääkäyttäjän kanssa harkita, mihin järjestelmään ja millä laajuudella työntekijä työssään tarvitsee käyttöoikeudet. Käyttöoikeuksien tulee olla työn kannalta tarkoituksenmukaisia eli työtehtävien kannalta riittäviä sekä perusteltuja. Työntekijän käyttöoikeuksia tulee aina päivittää tehtävien ja vastuiden muuttuessa.

Toimialojen ja työyksiköiden tietojärjestelmien käyttöoikeuksien määrittelystä huolehtivat järjestelmien pääkäyttäjät yhdessä it-asiantuntijan tai tehtävään erikseen nimetyn henkilön kanssa.

### **Kunnanhallitus**

- Hyväksyy tietoturvan ja tietosuojan yleisohjeet kuten tietoturvaohjeen ja päättää tarvittavista muutoksista johtavien viranhaltijoiden esittelystä.

### **Kunnanjohtaja, toimialajohtajat ja kunnan johtoryhmä**

-Vastaa annettujen tietoturvallisuutta koskevien määräysten ja ohjeiden noudattamisesta toimialallaan.

- Huolehtii siitä, että on nimetty tietoturvavastaava ja tietosuojavastaava

-Huolehtii it-asiantuntijan tarkempien ohjeiden tiedottamisesta toimialallaan, tarvittaessa ohjeita toimialakohtaisesti tarkentaen, tarvittaessa it-asiantuntijan osaamista tässä hyödyntäen

- Valvoo tietoturvamääräysten, ohjeiden ja suositusten noudattamista.
- Käsittelee ajankohtaisia tietoturvallisuutta koskevia kysymyksiä.

### **Tietoturvavastaava**

- Kehittää jatkuvasti ja aktiivisesti tietoturvallisuutta.
- Vastaa tietoturvallisuuteen liittyvien ohjeiden tiedottamisesta tietoturvan yhdyshenkilöille, esihenkilöille ja kaikille työntekijöille.
- Osallistuu esihenkilöiden tukena uusien työntekijöiden perehdyttämiseen tietoturvallisuutta koskevissa kysymyksissä.
- Ottaa vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi ne tarvittaessa johtoryhmälle
- Antaa yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä välttämättömän tietoturvamääräyksen, joka on voimassa enintään kaksi kuukautta
- Päättää edellä mainitun välttämättömän tietoturvamääräyksen päättämisestä sanottua aiemmin, mikäli arvioi sen mahdolliseksi.

### **Esihenkilö on velvollinen**

- välittämään tietoa tietoturvallisuuteen liittyvistä ohjeista omille työntekijöilleen ja järjestämään uusien työntekijöiden perehdytyksen tietoturvallisuuden
- huolehtimaan siitä, että työntekijät noudattavat annettuja määräyksiä ja ohjeita ja ilmoittamaan mahdollisista lisäkoulutustarpeista
- vastaamaan omien työntekijöidensä osalta siitä, että tietojärjestelmien käyttöoikeudet vastaavat työtehtävien tarpeita
- huolehtimaan henkilöstönsä käyttöoikeuksien päättämisestä palvelussuhteen päättyessä yhdessä pääkäyttäjien kanssa
- puuttumaan kaikkiin tietoturvaan koskeviin havaitsemiinsa epäkohtiin

### **Työntekijä on velvollinen**

- perehtymään häntä koskeviin tietoturvamääräyksiin ja ohjeisiin ja osallistumaan työnantajan järjestämään koulutukseen
- noudattamaan tietoturvaohjeistusta päivittäisessä työssään ja aktiivisesti hankkimaan itse työssään tarvitsemaa tietoturvatietoa
- raporttoimaan esihenkilölleen ja/tai tietoturvavastaavalle havaitsemansa tietoturvallisuuteen liittyvät epäkohdat ja poikkeamat

### **Tietojärjestelmän pääkäyttäjä**

- kouluttaa muita käyttäjiä ohjelman käytössä
- avaa ja sulkee käyttöoikeuksia it-asiantuntijalta saamansa ohjeen mukaisesti
- toimii ohjelmansa asiantuntijana ja kehittää käyttöoikeuspolitiikkaa yhdessä esihenkilöstön ja it-asiantuntijan kanssa

## **5. Koulutus ja ohjeistus**

Vetelin kunnan tietoturvallisuuspolitiikka pohjautuu siihen, että jokainen kunnassa työskentelevä tietää tietoturvaan ja tietosuojaan liittyvät vastuunsa ja on sitoutunut noudattamaan tietoturvasta ja tietojen käsittelystä annettuja ohjeita ja määräyksiä omassa työssään. Henkilöstön aiheuttamia tahattomia tietoturvauhkia ja -riskejä

voidaan minimoida ohjeistuksella ja koulutuksella ja virhetilanteissa avoimuuteen kannustamisella.

Tietoturvaohjeen nojalla annetaan tarvittaessa tarkempia ohjeita ja määräyksiä. Kunnan tietoturvaohjeistus sisältää ohjeistusta mm. omien tunnusten ja salasanojen käytöstä, henkilökohtaisen tietokoneen työtilan käytöstä sekä sähköpostin ja Internetin käytöstä ja tietojen turvallisesta käsittelystä.

Henkilöstölle järjestetään tietoturvakoulutusta joko sisäisenä koulutuksena tai ostopalveluna. Koulutusten tarkoituksena on sekä ylläpitää henkilöstön tietoturva- ja tietosuoja-asioiden osaamistasoa että muistuttaa säännöllisesti tietoturvan ja tietosuojan tärkeydestä. Osallistumisen dokumentointi on tärkeää koulutuksen suunnittelun ja riskien hallinnan (sisäinen valvonta) kannalta.

Johtoryhmän tehtävänä on huolehtia, että työntekijöillä on käytössään riittävästi ohjeistusta ja koulutusta tietojärjestelmien ja tietojen oikeanlaiseen käsittelyyn. Olemassa oleva tietoturvallisuusmateriaali jaetaan uusille työntekijöille ja sen läpikäyminen on osaksi uusien työntekijöiden perehdyttämistä.

## **6. Seuranta ja ongelmatilanteiden käsittely**

Kunnan tietoturvallisuus perustuu suunnitelmalliselle tietoturvatyölle, jota jokainen kunnan työntekijä toteuttaa työtehtävissään niin fyysisen turvallisuuden kuin tietoturvallisuuden osalta. Kunnanjohtaja, toimialajohtajat, it-asiantuntija ja tietosuojavaastaava seuraavat ja arvioivat tietoturvallisuuden tasoa ja tarvittavia toimenpiteitä.

Jokainen kunnan työntekijä on velvollinen ilmoittamaan havaitsemistaan ongelmatilanteista tai tietoturvapoikkeamista omalle esihenkilölleen ja it-asiantuntijalle tai tietosuojavaastaavalle. Ongelmatilanteissa minimoidaan ensin tietoturvapoikkeaman vaikutus, palaututaan normaalitilanteeseen, jonka jälkeen arvioidaan tietoturvan hallinnan tehokkuutta sekä muutetaan tarvittaessa toimintaa vastaavanlaisten tapahtumien estämiseksi.

### **Tarkastus ja arviointi**

Tietoturvaohjeen ja muiden tietoturvallisuusmääräysten ja -ohjeiden säännöllisestä tarkistamisesta ja arvioinnin järjestämisestä vastaa johtoryhmä ja kunnanhallitus. Arviointi suoritetaan aina, kun on tapahtunut sellaisia muutoksia, joilla on vaikutusta tietoturvallisuuteen.

Tietoturvaohjeen toimivuutta arvioidaan havaintojen ja tehtyjen turvallisuuspoikkeamatilanteiden perusteella.

## **7. Hyväksyminen**

*Vetelin kunnanhallitus on hyväksynyt tietoturvaohjeen 2.5.2022 § 57*