

**TEUVAN KUNNAN
TIETOTURVAPOLITIikka JA -OHJEET
1.4.2015 ALKAEN**

Sisältö

1.	TIETOTURVAPOLITIikka.....	3
1.1.	Tietoturvatyö	3
1.2.	Tietoturvallisuuden osa-alueet.....	4
1.3.	Vastuut ja valvonta	4
2.	TIETOTURVAOHJE	5
2.1.	Tavoitteet	5
2.2.	Toteutumisen varmistaminen	5
2.2.1.	Fyysinen turvallisuus	5
2.2.2.	Hallinnollinen tietoturvallisuus.....	6
2.2.3.	Henkilöstöturvallisuus	6
2.2.4.	Käyttöturvallisuus	6
2.2.5.	Laitteistoturvallisuus	6
2.2.6.	Ohjelmistoturvallisuus.....	7
2.2.7.	Tietoaineistoturvallisuus	7
2.2.8.	Tietoliikenneturvallisuus	7

1. TIETOTURVAPOLITIikka

Tietoturvapoliittikan avulla turvataan omalta osaltaan Teuvan kunnan palveluiden laadukas ja turvallinen toteuttaminen. Se määrittelee yleisellä tasolla pitkäjänteisesti kunnan tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Se on kaikkia toimialoja sitova ja sitä tarkennetaan tarvittaessa vastuualueiden omilla tietoturvamääräyksillä.

Tietoturvapoliittikkaa toteuttavassa tietoturvaohjeessa määritellään yksityiskohtaisemmin tietoturvallisuuden toteuttamisen linjaukset. Tietoturvaohjeet, jotka tarkistetaan tarvittaessa, tarkentavat ja täydentävät omalta osaltaan tietoturvapoliittikkaa ja tietoturvallisuuden osa-alueita.

Kunnan yhteistyö- ja sopimuskumppaneiden edellytetään noudattavan Teuvan kunnan tietoturvalinjauksia. Jos yhteistyön puitteissa käsitellään luottamuksellisia tietoja, tietoturva on kirjattava yhteistyökumppanin kanssa tehtäviin sopimuksiin.

Tämä ohje korvaa kunnanhallituksen 16.12.2002 hyväksymän Tietoturvasuunnitelman toimitaohjeineen.

1.1. Tietoturvatyö

Tietoturvatyö on jatkuvaa toimintaa päivittäisessä työssä ja se on tärkeä osa kunnan toiminnan ja palveluiden laatua. Jokaisen kunnan henkilökuntaan kuuluvan velvollisuus on noudattaa tietoturvasta annettuja määräyksiä ja raportoitava esimiehelleen havaitsemistaan ongelmista.

Tietoturvatyö tarkoittaa tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tämä kattaa tietojen turvaamisen menetelmät, välineet, toimenpiteet, määräykset, ohjeistuksen, koulutuksen, viestinnän, varautumista erilaisiin uhkatilanteisiin sekä sovitujen toimintatapojen noudattamista.

Tietoturvallisuus tarkoittaa tietojenkäsittelyn turvaamista sekä tietojen turvallista käsittelyä. Tietoturvallisuuden tehtävänä on varmistaa palvelutoiminnassa ja päätöksenteossa tarvittavien tietojen eheys sekä estää luottamuksellisten tietojen pääsy ulkopuolisten käsiin.

Tietoturvatyön päämääränä on

1. turvata kunnan toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymättömän toiminta sekä tietojen ja palveluiden saatavuus (toiminta normaalioloissa)
2. varautuminen toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen (toiminta poikkeustilanteissa)
3. estää tietojen ja tietojärjestelmien oikeudeton käyttö
4. estää tiedon tahaton tuhoutuminen
5. estää tiedon tahallinen tuhoaminen
6. estää tiedon vääristyminen
7. minimoida aiheutuvat vahingot.
8. turvata kunnan jäsenten yksityisyyden suoja

1.2. Tietoturvallisuuden osa-alueet

Tietoturvallisuuden osa-alueita ovat hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, käyttö- ja tietoaineistoturvallisuus. Osa-alueet kattavat kaikki kunnan tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon sekä arkistoinnin ottaen huomioon vastuualueiden perusluonteen ja tietoturvatarpeet.

Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, luovutusta, säilyttämistä ja siirtämistä.

Kunnan tiedot sekä tietojenkäsittelyjärjestelmät ja -palvelut on pidettävä asianmukaisesti suojattuna sekä normaalioloissa että poikkeusoloissa hallinnollisten, teknisten, rakenteellisten ja muiden toimenpiteiden avulla.

Tietoturvallisuus rakentuu

- tiedon luottamuksellisuudesta
luottamukselliset tiedot (ei - julkiset ja salassa pidettävät) ovat vain niiden käyttöön oikeutettujen saatavissa sovituilla tavoilla ja sovittuun aikaan eikä niitä paljasteta tai muutoin saateta sivullisten tietoon. Niiden käsittelyssä noudatetaan julkisuuslakia sekä erikseen toiminnoittain/järjestelmittäin hyväksyttyjä tietojen turvaluokituksia.
- tiedon eheydestä
tiedot ja tietojärjestelmät sekä paperiasiakirjojen arkistot ovat luotettavia, oikeellisia ja ajantasaisia, eivätkä ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai vahingoittuneet
- tiedon käytettävyydestä
tiedot ja tietojenkäsittelyjärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille, toiminnan kannalta hyväksyttävän ajan kuluessa
- pääsynvalvonnasta
tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman valvontaa
- kiistämättömyydestä
todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen
- henkilöstön ja luottamushenkilöiden toimintatavoista ja asenteesta
henkilöstö ja luottamushenkilöt ymmärtää tietoturvan merkityksen ja on motivoitunut noudattamaan tietoturvaohjeita ja tietoturvamääräyksiä.

1.3. Vastuut ja valvonta

Kunnanhallitus hyväksyy kunnan tietoturvapolitiikan ja tietoturvaohjeen.

Johtoryhmä vastaa tietoturvallisuuden kuntatason toteuttamisesta.

Esimiehet vastaavat vastuualueillaan, että tietoturvaohjeita noudatetaan.

Jokaisen kunnan luottamushenkilön ja työntekijän on noudatettava tietoturvaohjeita omalla toiminta-alueellaan. Lisäksi jokaisen kunnan palveluksessa olevan on raportoitava esimiehelleen havaitsemistaan ongelmista, uhkista tai ohjeiden vastaisesta menettelystä.

2. TIETOTURVAOHJE

2.1. Tavoitteet

Tietoturvallisuutta ylläpidetään noudattaen hyviä kansallisia ja kansainvälisiä käytäntöjä. Palvelut ja järjestelmät toteutetaan niin toimintavarmoina ja hyvin suojatuiksi, että ne sellaisinaan kestävät kohtuudella odotettavissa olevat uhkat.

Hyvä tietoturvallisuuden hallinta on prosessinomaista toimintaa. Valittujen tietoturvakontrollien tulee olla kustannustehokkaita ja kohdistua oikeisiin prosesseihin.

Teuvan kunnassa

- varmistetaan lakien ja muiden sitovien normien sekä sopimusvelvoitteiden noudattaminen
- ylläpidetään laadukasta ja tietoturvallista työympäristöä
- vaalitaan kunnan mainetta ja luottamusta kunnan toimintaan ja tuotoksiin
- noudatetaan käyttäjien vastuullisuuteen nojautuvaa hyvää tietoturvapoliittikkaa.

2.2. Toteutumisen varmistaminen

2.2.1. Fyysinen turvallisuus

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

Päävastuualueilla huolehditaan siitä, että tietojen käsittelyyn liittyviä kohteita suojellaan mahdollisimman hyvin fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä. Laitteet ja tietovarastot pyritään suojaamaan asiaankuulumattomilta henkilöiltä ja erilaisilta palo-, vesi- ja kiinteistövahingoilta. Vahinkojen rajaamiseksi tärkeimpiin tietoaineistojen sisältäviin kunnan toimitiloihin on asennettu murto- ja palohälyttimet.

Käyttäjät vastaavat siitä,

- että kunnan tiloissa ei liiku asiattomia henkilöitä
- että ovet pidetään lukittuina poistuttaessa tiloista
- että salasanoja ei jätetä näkyville eikä saataville
- että laitteet liitetään asianmukaisesti sähköverkkoon (ei maadoittamattomia jatkojohtoja)
- IT:lle varattuihin pistorasioihin ei kytketä muita kuin IT-laitteita.

Teuvan kunnan tietoliikenneyhteyksistä ja palvelimien ylläpidosta vastaa palvelusopimuksen mukaisesti Suupohjan Seutupalvelukeskus. Lähtökohtana on, että

- tietoliikenneyhteydet on pyrittävä turvaamaan sekä normaaleissa että poikkeusoloissa
- palvelimet ovat asennettu tiloihin, joissa niiden toiminnallisuus on turvattu.

2.2.2. Hallinnollinen tietoturvallisuus

Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Päävastuualueella vastataan käyttäjätason tietoturvallisuudesta. Päävastuualueen päällikkö päättää kirjallisesti kenelle, mihin ja missä laajuudessa käyttöoikeuksia annetaan ja poistetaan.

- Käyttöoikeuksista päättää päävastuualueen päällikkö
- Rajoitukset ja oikeudet toteuttaa pääkäyttäjä

2.2.3. Henkilöstöturvallisuus

Henkilöstöön liittyvien tietoturvariskien hallinta soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta

- Toiminnallisista oikeuksista ja yleisistä lukuoikeuksista päättää päävastuualueen päällikkö
- Rajoitukset ja oikeudet toteuttaa pääkäyttäjä.

2.2.4. Käyttöturvallisuus

Tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi

- Laitteiden ja ohjelmien käyttäjien on perehdyttävä Teuvan kunnan tietoturvapoliittikkaan ja -ohjeeseen sekä noudatettava sitä
- Esimiesten ja pääkäyttäjien tulee neuvoa, opastaa ja kouluttaa henkilöstöä tietotekniikan käyttöön ja tietoturvallisuuteen liittyvissä asioissa
- Johtoryhmän tulee tarvittaessa tarkistaa tietoturvaohjeiden ajantasaisuuden.

2.2.5. Laitteistoturvallisuus

Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi

- Päävastuualueiden päälliköt hyväksyvät vastuualueidensa laitehankinnat
- IT-laitteiden hankinnasta vastaa keskitetysti Suupohjan Seutupalvelukeskus
- Kannettaviin tietokoneisiin (sis. iPad) kirjautuminen edellyttää salasanaa
- Tietoliikenneyhteydet ja työasemat ovat varustettu virustentorjuntaohjelmilla.

2.2.6. Ohjelmistoturvallisuus

Käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämisen-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi

- Ohjelmien asentamisesta työasemille vastaa Suupohjan Seutupalvelukeskus
- Tärkeimpiin ohjelmiin pääsee sisään vain käyttäjätunnuksen ja salasanan avulla. Salasana on vaihdettava riittävän usein.
- Ohjelman pääkäyttäjä myöntää käyttäjätunnuksen ja salasanan ohjelman käyttöä varten
- Kaikista ohjelmista pidetään varmuuskopiota
- Ohjelmien käytöstä tallentuu lokitiedot palvelimille.

2.2.7. Tietoaineistoturvallisuus

Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen hallinta arkistonmuodostussuunnitelmalla, luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen

- Ohjelmien käyttäjätunnukset ja salasanat annetaan vain niille, jotka käyttävät ohjelmia työssään
- Tiedostoista otetaan varmuuskopio vuorokausittain yöajossa
- Palvelimien toiminta varmistetaan päivittäin
- Irrotettavilla muistikorteilla/muistitikuilla on oltava salasana silloin, kun ne sisältävät arkaluonteista tietoa
- Luottamuksellista tietoa sisältävät paperiset asiakirjat on arkistoitava tai tuhottava asianmukaisesti
- Kaikki käyttäjät ovat velvollisia noudattamaan kulloinkin voimassa olevaa tekijänoikeuslakia.

2.2.8. Tietoliikenneturvallisuus

Tavoitetila, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta.

Lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Tietoliikenneturvallisuuteen tähtäviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

- Kunnan tietoliikenneyhteysistä vastaa Suupohjan Seutupalvelukeskus
- Kunnan toimipisteissä pääasiallisena tietoliikenneyhteytenä on Suupohjan Seutuverkon rakentama valokuituyhteys
- Langattoman tietoliikenneyhteyden operaattorina toimii kilpailutettu operaattori
- Tietoliikenneyhteydet ovat suojattu palomuuureilla
- Työasemilla on virustentorjuntaohjelma, joka päivittyy automaattisesti.