JULKINEN

HEINÄVEDEN KUNNAN

TIETOTURVAPOLITIIKKA

Käsitelty: 30.3.2012 yhteistyötoimikunnassa
Hyväksytty: 16.4.2012 kunnanhallituksessa

SISÄLTÖ

1. ESIPUHE

Tähän dokumenttiin on koottu Heinäveden kunnassa noudatettavat tietoturvan tavoitteet, periaatteet ja toteuttamisen organisointitavat. Tuloksena syntynyt tietoturvapolitiikka toimii perustana kunnan tietoturvakäytäntöjen, -dokumenttien ja -ohjeistuksien laadinnassa/päivittämisessä.

2. TIETOTURVAPOLITIIKAN LÄHTÖKOHTA

Hyväksymällään tietoturvapolitiikalla kunnanhallitus määrittelee tietoturvan tavoitteet, periaatteet, toteutuskeinot ja vastuut. Tietoturva on kiinteä osa kunnan koko toiminnan varmistamista ja kehittämistä.

Tietoturvapolitiikan lainsäädännöllinen perusta nojautuu useisiin lakeihin. Näistä keskeisimpiä ovat valmius-, julkisuus- ja tietosuojalait. Lainsäädännön asettamien vaatimusten täyttäminen ja hallinta edellyttävät julkishallinnon toimintayksiköiltä vahvaa tietoturvan toteuttamista. Tietoturvaan liittyviä lakeja on listattu tämän dokumentin luvussa 10.

Tietoturvapolitiikka liittyy myös toiminnan kehittämiseen, jatkuvuuden varmistamiseen ja valvontaan. Tähän liittyen jatkuvuus- ja toipumissuunnitelmat sekä riskienhallintamenetelmät ja niihin liittyvät säännölliset riskikartoitukset sisällytetään osaksi kunnan normaalia toimintaa.

3. TIETOTURVA JA TIETOTURVALLISUUS

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi lainsäädännöllisillä, hallinnollisilla, teknisillä ja muilla toiminnoilla sekä normaali- että poikkeusoloissa.

Tietoturvallisuus kattaa kaikenlaiset tietojenkäsittelytehtävät sisältäen myös erityyppisten dokumenttien arkistoinnin. Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, luovutusta ja siirtoa.

Tietoturvallisuus rakentuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä lisäksi soveltuvilta osin pääsynvalvonnasta ja kiistämättömyydestä.

Luottamuksellisuus tarkoittaa, että tiedot ovat vain niiden käyttöön oikeutettujen käyttäjien saatavissa sovituilla tavoilla ja sovittuun aikaan sekä sovituista paikoista. Tietoja ei paljasteta tai muutoin saateta sivullisten tietoon.

Eheys tarkoittaa, että tiedot ja tietojärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ole muuttuneet tai vahingoittuneet laitteisto- tai ohjelmistovikojen, luonnontapahtumien taikka oikeudettoman inhimillisen toiminnan seurauksena.

Käytettävyys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat toiminnan kannalta hyväksyttävän ajan kuluessa käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille.

Pääsynvalvonta tarkoittaa, että tietoja tai tietojärjestelmiä ei voi käyttää ilman käyttäjälle myönnettyjä käyttö- ja pääsyoikeuksia.

Kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

4. TIETOTURVAN TAVOITTEET JA KATTAVUUS

Heinäveden kunnassa käsitellään sekä kunnan omia että asiakkaiden omistamia luottamuksellisia ja tärkeitä tietoja, kuten henkilötietoja, taloustietoja ja hallinnon asiakirjoja. Osa näistä tiedoista on salassa pidettävää, arkaluonteista tai muuten luottamuksellista tietoa. Tämän vuoksi on tärkeää, etteivät tiedot joudu tahattomasti tai tahallisesti asiattomien haltuun.

Lisäksi kunnassa käsitellään tietoa, joka ei ole salassa pidettävää vaan luonteeltaan julkista, mutta tällaisenkin tiedon oikeellisuudesta, muuttumattomuudesta, saatavuudesta, lainmukaisesta käsittelystä sekä oikeudesta ja velvollisuudesta luovuttaa tietoa on pystyttävä varmistumaan.

Kunnan palvelujen tuottaminen ja niiden tehokkuus ja luotettavuus riippuvat palveluketjusta, joka muodostuu toimivista työasemista, tietoliikenneverkoista, konesalipalveluista ja tietojärjestelmistä. Tämän vuoksi tietoturvatoimia tulee tarkastella kaikessa toiminnassa palvelujen varmistamisen ja jatkuvuuden näkökulmasta. Osa palveluketjun teknisistä alustoista on Istekki Oy:n ja PTTK Oy:n tuottamia ja ylläpidossa. Loput on kunnan itsensa huolehtimia

4.1. Tietoturvan tavoitteet

Kunnan tietoturvatyön tavoitteina on turvata omalle toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot.

Normaalitoiminnan jatkuvuuden turvaamisen lisäksi varaudutaan normaaliajan toiminnan keskeyttäviin erityistilanteisiin sekä poikkeusoloihin ja niistä toipumiseen hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Myös poikkeusolojen valmiuden luominen ja ylläpito on välttämätön osa kunnan/kaupungin tietojenkäsittelyn turvallisuutta.

Kunnan tietoturvan tason tulee olla sellainen, että:

- kunnan toimintaa koskevassa lainsäädännössä, sisäisissä määräyksissä ja ohjeissa asetetut turvallisuusvaatimukset täytetään

- tietojärjestelmätoiminnot on siten varmistettu, että niiden keskeytyksistä ja häiriöistä huolimatta toiminta ja palvelut voidaan hoitaa vähintään ennalta hyväksytyllä minimitasolla
- tiedot ja järjestelmät on suojattu siten, että niitä voivat käyttää vain ne, jotka työtehtäviensä takia ovat siihen oikeutettuja
- sidosryhmäyhteyksissä ylläpidetään sekä oman toiminnan että sidosryhmän toiminnan vaatimuksia vastaava tietoturvataso
- varmistetaan ulkopuolisten palveluntuottajien tietoturvan toteutuminen
- toimintojen vastuuhenkilöt tuntevat atk-riippuvuudet, niihin liittyvät riskit ja noudatettavat käytettävyyskriteerit
- tietojenkäsittelyn laatu määritellään ja on erityisen valvonnan kohteena toiminnoissa, joissa virheet niiden suuruusluokan, tietojen hyödyntämisen nopeuden/automaattisuuden vuoksi tai muista syistä saattavat aiheuttaa virheitä päätöksenteossa
- tietotekniikan käyttöympäristö ja resurssit on mitoitettu ja järjestetty siten, että ne tehokkuus- ja laatutavoitteiden täyttämisen ohella edistävät tietoturvan toteutumista
- tietojenkäsittelyn turvallisuuden ja vahinkojen seuranta sekä raportointi on määritelty toteutettavaksi toimialoittain.

Lisäksi yleisempänä päämääränä on saavuttaa ValtIT:n ICT-varautumisen määrittelemä tietoturvan kypsyyden ja varautumisen perustaso (2) kaikessa toiminnassaan sekä korotettu taso (3) kriittisiksi määritellyissä toimintaprosesseissa, tietojärjestelmissä ja palveluissa. Tietoturvan operatiivisessa toteutuksessa noudatetaan soveltuvin osin myös ISO 27002 – standardissa määriteltyjä menetelmiä.

4.2. Tietoturvapolitiikan kattavuus

Kunnanhallituksen vahvistama tietoturvapolitiikka kattaa kaiken toiminnan huomioiden tietoturvan kaikki osa-alueet. Tietoturvapolitiikkaan pohjautuvat tietoturvaan liittyvät suunnitelmat, ohjeet ja määräykset kattavat kaikki tietojenkäsittelytoiminnot sekä koskevat kaikkia kunnan viranhaltijoita ja työntekijöitä, työryhmiä, toimielimiä sekä kunnan toimeksiantoja tekeviä ulkopuolisia näiden hoitaessa julkisuuslainsäädännön mukaisesti julkisia tehtäviä.

Tietoturvapolitiikka kattaa myös toimistotyön kaikki tehtävät ja niihin sisältyvän arkistoinnin, tiedonsiirron sekä vaitiolovelvollisuuden piiriin kuuluvan ja muunkin puhutun, kirjoitetun ja graafisen tiedon.

Henkilöstön menettelytavoissa, tietoteknisissä ratkaisuissa sekä tietotekniikkaan liittyvissä laitehankinnoissa ja kehittämishankkeissa on otettava huomioon tässä tietoturvapolitiikassa määritellyt yhdenmukaiset linjaukset ja tietoturvan tasovaatimukset, joita täsmennetään erikseen ylläpidettävissä tietoturvasuunnitelmassa ja siihen liittyvissä ohjeistuksissa.

5. TIETOTURVAN VASTUUTUS JA ORGANISOINTI

Osana kokonaisvastuutaan **kunnanjohtaja** ja **kunnanhallitus** vastaavat tietoturvan toteutumisesta ja tarvittavien edellytyksien luomisesta tietoturvapolitiikan mukaisten tietoturvavaatimusten ja -tavoitteiden saavuttamiseksi.

Kunnan **johtoryhmä,** johon kuuluvat **kunnanjohtaja** ja **toimialapäälliköt**, vastaavat tietoturvapolitiikan toteutuksesta hallinnollisella tasolla sekä tietoturvan integroimisesta kokonaistoimintastrategiaan.

Johtoryhmän tehtäviin tietoturvan osalta lukeutuvat vakaviin tietoturvaongelmiin liittyvien ja nopeaa reagointia vaativien toimenpiteiden käynnistäminen. Johtoryhmän muihin tehtäviin kuuluu tietoturvallisuuteen liittyvien suunnitelmien ja ohjeistuksien katselmointi ja käytäntöön vienti.

Johtoryhmä valmistelee ja ohjaa kunnan tietoturvan käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa hallituksen hyväksymän tietoturvapolitiikan mukaisesti.

Toimialapäälliköt valvovat tietoturvan ja siihen liittyvien kehittämishankkeiden toteutusta omilla vastuualueillaan. Lisäksi he ovat mukana tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelussa ja varmistavat osaltaan toimintaan kuuluvien tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Kunnanjohtaja vastaa tietoturvan seurannasta, raportoinnista ja kehittämishankkeiden toteutuksesta sekä valmistelee niitä yhdessä muiden johtoryhmän jäsenien kanssa. Lisäksi kunnanjohtaja huolehtii mm. tietoturvaan liittyvien suunnitelmien ylläpidosta ja niiden perustana olevien lakien, säädöksien ja standardien seurannasta sekä selkeiden ohjeiden ja koulutusmateriaalin laadinnasta käyttäjille apunaan kunnansihteeri ja atk-suunnittelija.

Lisäksi jokainen kunnassa tietoja (sekä automaattisen tietojenkäsittelyn piiriin sisältyviä että paperimuotoisia) käsittelevä henkilö on vastuussa tietoturvan toteuttamisesta omalta osaltaan. **Jokaisen työntekijän** tulee erityisesti huolehtia siitä, että henkilötietoja käsiteltäessä noudatetaan tietosuojalain (523/1999) toisessa luvussa esitettyjä henkilötietojen käsittelyä koskevia yleisiä periaatteita.

Työntekijöille selvitetään tietoturvapolitiikan sisältö ja he sitoutuvat lakien ja asetusten määräysten lisäksi noudattamaan hyväksytyn tietoturvapolitiikan toteuttamiseen liittyviä määräyksiä, ohjeita ja toimintatapoja.

6. TIETOTURVAN TOTEUTUS

Tietojärjestelmätoimintojen tietoturvan keskeinen perusta on kunnan johdon antama, hallituksen vahvistama ja riskikartoitukseen perustuva **tietoturvasuunnitelma**, jossa kuvataan toimintatavat ja –menetelmät **tietoturvapolitiikassa** määriteltyihin tavoitteisiin pääsemiseksi. Tietoturvapolitiikka on ylin osa tietoturvaohjeistuksen hierarkiassa ja sitä päivitetään päälinjojen muuttuessa.

Tietoturvasuunnitelmaan nojautuvilla **ohjeistuksilla** viestitetään palvelujen käyttäjille hyväksyttävät käyttäytymissäännöt ja käytön rajoitukset tietoturvan toteutumiseksi sekä luodaan käytännön menettelytavat riittävän perusturvallisuustason saavuttamiseksi. Tietoturvasuunnitelmaan liittyy läheisesti **jatkuvuus- ja toipumissuunnitelmat**, joissa kuvataan toimenpiteet ja menetelmät toiminnan jatkuvuuden turvaamiseksi sekä toiminnan palauttamiseksi normaalitasolle häiriötilanteiden jälkeen. Tietoturvasuunnitelmaa ja siihen liittyvää ohjeistusta tarkastellaan säännöllisesti.

Tietoturvatoiminnan yksityiskohdissa noudatetaan hyväksyttyjä, olemassa olevia ja tämän tietoturvapolitiikan toteuttamisen yhteydessä syntyviä/päivitettäviä tietoturvaohjeita ja tietoturvan standardeja sekä ns. hyvän rekisterinpidon vaatimuksia. Nämä liitetään soveltuvin osin dokumentaatioon samoin kuin toimintayksiköiden erityisohjeet.

Tietoturvan kehittämistarpeiden ja -tavoitteiden määrittelemiseksi tietoturvariskit kartoitetaan säännöllisin väliajoin. Samalla kartoituksien antamien tuloksien perusteella suunnitellut kehitystoimenpiteet toimivat jatkuvuus- ja toipumissuunnitelmien sekä poikkeusolojen **valmiussuunnitelman** kehittämisen perustana.

Tietojärjestelmistä laaditaan **tietojärjestelmäselosteet** tarvittavin osin ja **tietojärjestelmäkuvaukset**, joissa järjestelmille määritetään niistä vastuussa olevat omistajat/haltijat ja joihin kytketään järjestelmäkohtaiset toipumissuunnitelmat. Selosteet kytketään osaksi muuta tietojärjestelmien dokumentaatiota, jonka ajantasaisuus edesauttaa tietoturvan toteutumista. Kunnan tietoaineistot ja tietojärjestelmät luokitellaan tietoaineistojen luottamuksellisuuden ja tietojärjestelmien tärkeyden mukaan. Tietoaineistojen luokittelu tehdään **arkistonmuodostussuunnitelman** yhteydessä. Kullekin turvallisuusluokalle määritellään vaadittava tietoturvataso ja sen mukaiset tietoturvatoimenpiteet. Tietojen käsittelyn yhteydessä noudatetaan hyvää tiedonhallintatapaa, jonka toteuttaminen liittyy keskeisesti säännösten puitteissa myös tietoturvan toteutumiseen.

Kunnan henkilökunnalle ja sidosryhmille viestitään tietoturvasta ja heitä koskevista säännöistä ja suosituksista. Henkilöstön tietoturvatietoisuutta lisätään tiedottein sekä järjestämällä asiaan liittyvää säännöllistä koulutusta. Tietoturvan toteuttamista ohjaavat asiakirjat ovat kunnan johdon vahvistamia ja asianomaisten kohderyhmien saatavissa.

7. TIETOTURVAN TOTEUTUMISEN SEURANTA JA VALVONTA

Tietoturvan toteutumisen seuranta on osa kunnan tietoturvan kehittämisen prosessia. Tätä osaa seurannasta ohjaa tämä tietoturvapolitiikka ja säätelee tarkemmin tietoturvasuunnitelma ohjeistuksineen.

Tietoturvajärjestelyjen ja seurantajärjestelmän kuvaus liitetään osaksi tietoturvadokumentointia. Seuranta toteutetaan jatkuvana prosessina koko organisaatiossa käyttäen sisäisiä ja ulkoisia auditointeja sekä muita vastaavia seurannan välineitä.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvapuutteista, tietoturvaan liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista toiminnallisessa vastuussa olevalle esimiehelle sekä kunnan tietoturvasta vastaavalle henkilölle.

8. TIEDOTTAMINEN

Kunnan tietoturva-asioista tiedottamisesta yleisellä tasolla vastaa kunnansihteeri ja sisäisestä tiedottamisesta huolehtii kunnan johtoryhmä tietoturvasuunnitelman mukaisesti.

9. TIETOTURVAPOLITIIKKAAN PERUSTUVAT DOKUMENTIT

Tietoturvapolitiikan määrittelemien tavoitteiden saavuttamiseksi ja prosessien kehittämisen turvaamiseksi laaditaan seuraavat tarkemmat suunnitteludokumentit:

- Tietoturvasuunnitelma
- Jatkuvuussuunnitelma
- Toipumissuunnitelmat (järjestelmäkohtaiset)
- Valmiussuunnitelma
- Arkistonmuodostussuunnitelma
- Pelastautumissuunnitelmat (yksikkökohtaiset).

Lisäksi on laaditaan henkilöstölle tarkoitettuja Tietoturvasuunnitelmaan perustuvia ohjeistuksia palvelujen ja resurssien käyttöön jokapäiväisessä työssä. Nämä ohjeet on mainittu tarkemmin Tietoturvasuunnitelmassa.

10. TIETOTURVAAN LIITTYVÄ LAINSÄÄDÄNTÖ

- Arkistolaki (831/1994)
- Asetus sähköisen viestinnän varautumisesta (1297/1997)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Hallintolaki (434/2003)
- Henkilötietolaki (523/1999)
- Kansanterveyslaki (66/1972)
- Kuntalaki (365/1995)
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki turvallisuusselvityksistä (177/2002)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki valmiuslain muuttamisesta (198/2000)
- Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (621/1999)
- Lukiolaki (629/1998), Perusopetuslaki (628/1998)
- Rikoslaki (39/1889)

- Sosiaalihuoltolaki (710/1982)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta ja niiden muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001)
- Sähköisen viestinnän tietosuojalaki (516/2004 muutossäädöksineen viim. 125/2009)
- Telemarkkinalaki (396/1997), Telemarkkina-asetus (424/1997)
- Valmiuslaki (1080/1991)
- Väestötietolaki (507/1993)