POMARKKU

TIETOTURVA – JA TIETOSUOJAPOLITIIKKA

Kunnanhallitus 24.4.2018 §74

1. Johdanto

Yhteiskunta ja kuntien toiminnot ovat jatkuvasti entistä riippuvaisempia ICT-teknologiasta ja - palveluista sekä niiden toimintavarmuudesta. Tietojen käsittelyyn ja tietotekniikkaan liittyviä riskejä pitää tunnistaa ja hallita aktiivisesti. Riskien negatiivisia vaikutuksia pitää minimoida teknisillä ja hallinnollisilla keinoilla.

Tietoturvan tärkeyttä lisäävät myös kansalaisille suunnattujen sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäytön lisääntyminen, kuntien yhteistyö palvelujen järjestämisessä, laaja palveluntuottajien verkosto (monituottajamallissa myös ostopalvelu- ja palvelusetelituottajat käyttävät kuntien järjestelmiä) sekä palvelutuotannon uudet menetelmät (erityisesti pilvipalvelut, jotka hämärtävät maiden rajat ja tietojen sijainnin).

Tietoturvapolitiikka on laadittu ja tarkoitettu Pomarkun kunnan henkilöstölle, luottamusmiehille sekä kunnan tietoja ja tietojärjestelmiä tai toimitiloja käyttäville muille henkilöille.

Tietoturvapolitiikka on sisäinen määräys, joka jaetaan tiedoksi ja noudatettavaksi. Tietoturvapolitiikkaan sisältyvät erikseen hyväksytyt tietoturvaan ja tietosuojaan liittyvät määräykset ja ohjeet.

2. Tietoturvapolitiikan tavoite

Tietoturvallisuuden ensisijaisena päämääränä on organisaatioiden vastuulla olevien palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa eli tietotekniikkanäkökulmasta mahdollistaa organisaation palveluihin liittyvien ICT-ratkaisujen käytettävyys sekä prosesseissa, rekistereissä ja palveluissa käytettävien tietojen eheys ja luottamuksellisuus kaikissa olosuhteissa.

Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja-asioiden hoidolla tuetaan oman organisaation toiminnalle asetettuja vaatimuksia ja varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely varmistaen samalla kansalaisten yksityisyyden suoja.

2.1 Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Se edellyttää tietojen, järjestelmien, palvelujen ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuus on toimintatapa, jonka tavoitteena on tietojärjestelmien ja toiminnan jatkuvuutta uhkaavien riskien hallinta. Se on edellytys toiminnan luotettavalle hoitamiselle.

2.2 Tietosuojan käsite ja merkitys

Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityisyyden ja oikeusturvan varmistamiseksi. Tietosuojan tarkoituksena on näin ollen turvata tiedon kohteen yksityisyys sekä edut ja oikeusturva. Tietosuoja on Suomessa yksilön perustuslaillinen oikeus ja osa palvelujen laatua.

2.3 Määritelmät

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa (lyhyt ja tarkempi kuvaus):

Luottamuksellisuus; kukaan sivullinen ei saa tietoa

- tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn sekä tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.

Eheys; tiedon yhtäpitävyys alkuperäisen tiedon kanssa

- tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus sekä ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys; tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana

- ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Todentaminen (autentikointi); varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.

Kiistämättömyys; tietoverkossa eri menetelmin saatava näyttö siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi.

Tietosuojaan liittyvät käsitteet **henkilötieto**, **henkilötietojen käsittely**, **henkilörekisteri**, **rekisterinpitäjä**, **rekisteröity**, **sivullinen** ja **suostumus** määritellään henkilötietolaissa.

3 Tietoturvatoimintaa ohjaavat tekijät

- Euroopan unionin yleinen tietosuoja-asetus (velvoittaa 5/2018-)
- Suomen perustuslaki (731/1999) 2. luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
- Suomen perustuslaki (731/1999) 2. luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö

- Turvallisuusselvityslaki (726/2014)
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
- Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
- Rikoslaki (39/1889) 34. luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
- Rikoslaki (39/1889) 38. luku 8 §: Tietomurto
- Rikoslaki (39/1889) 38. luku 9 § 1. kohta: Henkilötietorikos
- Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
- Vahingonkorvauslaki (41/1974)

Lainsäädännön lisäksi tulee noudattaa muita omalle organisaatiolle hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason määräysten kanssa siten, että tietoturva tai tietosuoja heikkenee.

4 Tietoturvallisuuteen kohdistuvat uhat

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Henkilöiden mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys aiheuttavat merkittävimmän uhan organisaation tietoturvallisuudelle. Lisäksi uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset, haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Merkittäviä uhkia voi liittyä myös ulkopuolisten palvelujen tuottamiseen, mikäli palveluntuottajien kanssa ei ole tehty sopimuksia, joissa huomioidaan tietoturvaan, tietosuojaan ja varautumiseen liittyvät asiat sekä rikkomuksiin liittyvät sanktiot.

Organisaatiossa, prosesseissa, projekteissa ja tietojärjestelmissä tulee huolehtia tietoturvaan ja tietosuojaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta.

5 Tietoturvallisuuden merkitys ja toteuttaminen

5.1 Turvattavat kohteet

Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan. Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietoverkon toiminnan turvaaminen sekä palvelujen tuottaminen normaali- ja poikkeusoloissa.

5.2 Tietoturvaperiaatteet

1. Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaisesti osa organisaation päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
2. Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta. Tarkoituksena on varmistaa (liike)toiminnan jatkuvuus, minimoida (liike)toiminnalliset riskit sekä maksimoida investoinneista ja (liike)toiminnan mahdollisuuksista saatu tuotto.
3. Tietoturvaan liittyvät ongelmat tulee mieluummin ennaltaehkäistä kuin hoitaa jälkikäteen.
4. Tietoturva- ja tietosuoja-asiat pitää huomioida välineestä riippumatta eli ne eivät liity vain tietotekniikkaan.
5. Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.
6. Tietoturvallisuuden saavuttamiseksi pitää toteuttaa sopivia turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
7. On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
8. Jokaisen esimiehen on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle.
9. Tietoturvaan liittyvä ohjaus, valvonta ja seuranta tulee organisoida.
10. Tietoturvan toteutumista tulee seurata ja kehittää.

5.3 Tietoturvallisuuden toteutumista tukevia käytäntöjä

EU 2016/679 (tietosuoja-asetus) 37 artikla edellyttää, että reksiterin pitäjä nimeää tietosuojavastaavan aina kun tietojen käsittelyä suorittaa jonkin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin. Pomarkun kunnan tulee nimetä tietosuojavastaava.

Uusien tietojärjestelmien, prosessien sekä tilojen tietoturva-asiat tulee huomioida ja testata jo ennen niiden käyttöön ottamista. Tietojärjestelmien toimintaa ja käyttöä tulee valvoa.

Sisäisten tietojärjestelmien tietojen käyttö tulee pääsääntöisesti sallia vain työtehtävien tai niihin rinnastettavien tehtävien hoitamiseen sekä yhteistyökumppaneilla vastaavasti sopimusten ja lupien mukaisten tehtävien hoitamiseen.

Tietoturvan ja tietosuojan toteuttamisessa tulee käyttää tarvittaessa ulkopuolisten asiantuntijoiden apua.

Palvelujen hankintaan ja ulkoistuksiin liittyvissä sopimuksissa pitää huomioida turvallisuuteen ja varautumiseen liittyvät asiat.

Tietojärjestelmiin ja tietojen käsittelyyn liittyvissä suunnitelmissa, järjestelyissä sekä ohjeissa varaudutaan tietoturvallisuutta ja tietosuojaa koskevien laiminlyöntien, vahinkojen tai virheiden

jälkikäteisselvittämiseen. Tässä on hyvä pitää periaatteena kustannusten kohtuullisuus saatuun hyötyyn nähden.

6 Turvatoimien priorisointi

Turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

- henkilön hengen tai terveyden turvaaminen
- arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen

- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen

7 Tietoturvallisuuden hallintajärjestelmä

Hallintajärjestelmän avulla toteutetaan tietoturvan hallintaa ja seurantaa sekä arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa valmiuksia hallita tietoturvallisuutta järjestelmällisesti. Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, joka koostuu mm. seuraavista toimintamalleista ja dokumenteista:

Toimintamallit

- tietoturvan ja tietosuojan vastuuhenkilöiden ja ryhmien toiminta
- ICT-palveluiden toimittajien tietoturvaan liittyvät toimintamallit ja raportointi
- tietoturvaraportointi johdolle
- tietoturvapoikkeamien käsittely
- tietosuojapoikkeamien ja –selvitysten käsittely
- tietoturvan ja tietosuojan huomioiminen prosesseissa ja projekteissa
- tietoturva- ja tietosuojakoulutus
- tietoturvaan ja tietosuojaan liittyvä riskienhallinta
- tietojen, tietojärjestelmien ja henkilörekisterien omistajuus

Dokumentit:

- kunnan tietoturvapolitiikka (tämä dokumentti)
- muut tietoturvaan ja tietosuojaan liittyvät määräykset
- tietoturvallisuuteen liittyvä ohjeistus

8 Tietoturvavastuut

8.1 Organisaation tietoturvavastuut

Vastuu tietoturvan ja tietosuojan toteuttamisesta sekä tietoturvapolitiikan noudattamisesta on jokaisella, vaikka tietohallinto vastaa yleisestä tietoturvan ja tietosuojan hallinnan kehittämisestä sekä koordinoinnista. Tietoturvaan ja tietosuojaan liittyvissä asioissa jokainen henkilö on vastuussa riskeistä, jotka liittyvät hänen päätöksentekovaltaan tai päätöksiin.

Tietoturvallisuuden ja tietosuojan kehittäminen on jatkuvaa laaja-alaista toimintaa, jossa eri viranomaisilla, vastuuhenkilöillä ja ryhmillä on omat tehtävänsä. Kunta vastaa tämän tietoturvapolitiikan mukaisesta tietoturvan ja tietosuojan toteuttamisesta. Organisaation eri osat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan.

Jokaisen henkilörekisterin rekisterinpitäjä vastaa kyseisen henkilörekisterin osalta hyvän henkilötietojen käsittelytavan ja lainsäädännön edellyttämän korkean tietoturvan ja tietosuojan tasosta sekä rekisterin tietojen käsittelyyn liittyvistä linjauksista. Erityisesti palvelu- ja alihankintasopimuksissa on rekisterinpitoon, tietosuojaan ja tietoturvaan liittyvät asiat huomioitava. Yksityisyyden suoja on kansalaisten perusoikeus, jonka varmistaminen on vastuuhenkilöiden lisäksi myös kaikkien esimiesten vastuulla.

Rekisterinpitäjän, toimialojen ja prosessien omistajien vastuulla on rekistereissä, toiminnassa ja prosesseissa tuotettavien sekä käsiteltävien tietojen ajantasaisuuden, oikeellisuuden, käytettävyyden ja eheyden varmistaminen sekä tietoihin liittyvien käyttövaltuuksien määrittely. Tietohallinto vastaa yleisestä käyttövaltuuspolitiikasta.

Tietojärjestelmien omistajalla on vastuu tietojärjestelmän toimintavarmuudesta ja dokumentoinnista sekä riskien hallinnasta. Jokainen sovellusta tai ICT-palvelua käyttävä rekisterinpitäjä tai prosessin omistaja on kuitenkin itse vastuussa toimintansa riskien

hallinnasta ja varautumisesta muun muassa sen varalta, että sovelluksen tai ICT-palvelun toiminnassa on häiriöitä. Riskienhallinta ja varautuminen tulee tehdä kunnan sekä oman (liike)toiminnan lähtökohdista ja laatia suunnitelmat siitä, miten toimitaan häiriöiden aikana ja miten toiminta palautetaan normaaliksi häiriöiden jälkeen. Tietohallinto turvaa ja priorisoi omistamansa järjestelmät asiakkaidensa toiminnan prioriteettien ja riskien pohjalta. Tietojärjestelmien ylläpitoon liittyvät tietoturva-asiat määritellään tarkemmin sitä asiaa käsittelevissä erillisissä määräyksissä ja ohjeissa.

Tietoturvatoiminnan ja tietoturvallisuuden hallintajärjestelmän kehittämisestä vastaa hallintopalvelut hallintojohtajan johdolla.

Kunnan tietoturvasta vastaavalla henkilöllä sekä kunnan tietosuojavastaavalla on oikeus suorittaa käytönvalvontaa sekä tarkastaa ja auditoida toimintatapoja, tietojärjestelmiä ja tietoja liittyen kunnan tietoturvan tai tietosuojan sääntöjen ja ohjeiden noudattamiseen ja toteuttamiseen.

Tietoturvapolitiikka päivitetään tarvittaessa. Päivitystarvetta seuraa hallintojohtaja ja tietosuojavastaava. Organisaatiomuutoksista, laeista tai muista määräyksistä johtuvia teknisiä korjauksia tähän dokumenttiin voidaan tehdä ilman erillistä hyväksyntäkäsittelyä.

9 Organisaation yhteistyökumppaneiden vastuut

Organisaatiolle palveluja tuottavat tahot tulee velvoittaa nimeämään tietoturva- sekä tietosuoja-asioihin yhteyshenkilö, joka heillä vastaa sovitun tietoturva- ja tietosuojatason noudattamisesta. Kumppanien tulee viipymättä ilmoittaa omista kuntaan vaikuttavista tietoturvapoikkeamistaan kunnan tietosuojavastaavalle. Kumppaneille asetettavat vaatimukset tulee kuvata kunkin sopimuksessa tai sen erillisessä liitteessä.

10 Tietoturva- ja tietosuojakoulutus ja –ohjeet

Tietoturvallisuus tulee olla sisällytettynä perehdytysprosessiin. Koulutusta järjestetään ja mahdollistetaan kaikille työntekijöille määräajoin. Henkilöstön tietoturvaopas pidetään ajan tasalla ja siitä kerrotaan työntekijöille sekä kaikille organisaation tietoja ja tietojärjestelmiä käyttäville muille henkilöille.

Tietoturvaan ja tietosuojaan liittyvien ohjeiden sisällöstä ja ajantasaisuudesta vastaavat nimetyt tietoturvan ja tietosuojan vastuuhenkilöt.

Esimiesten tulee varmistaa, että henkilöstö hallitsee tietoturvan ja tietosuojan perusteet. Varmistaminen onnistuu esim. tarkastamalla kehityskeskusteluissa, että jokainen tietojärjestelmiä käyttävä henkilö on tutustunut henkilöstön tietoturvaoppaaseen ja mahdollisesti suorittanut tietoturvaan liittyviä kursseja.

Yhteistyökumppanit tulee velvoittaa noudattamaan tilaajan tietoturva- ja tietosuojaohjeistusta.

11 Tietoturvallisuudesta tiedottaminen

Tietoturva- ja tietosuoja-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaavat tietoturvan ja tietosuojan vastuuhenkilöt yhdessä viestinnästä vastaavan tahon kanssa.

Tietoturva- ja tietosuoja-asioista ei aktiivisesti tiedoteta ulkopuolisille, mutta jos tiedottamistarvetta ilmenee, sen hoitavat tietoturvasta tai tietosuojasta vastaavat henkilöt.

12 Tietoturvallisuuden toteutumisen valvonta

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä kunnan tietosuojavastaavalle tai omalle esimiehelleen.

Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin toimintayksikkö tai organisaatiolle palveluja tuottava yritys omalla vastuualueellaan. Esimiesten tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita. Esimiesten tulee raportoida tietosuojavastaavalle valvonnan tuloksista.

Tietoturvapolitiikan ja siihen liittyvien ohjeistuksien toteutumista ja noudattamista seuraavat nimetyt tietoturvan ja tietosuojan vastuuhenkilöt, joiden velvollisuus on raportoida oman organisaationsa johdolle.

13 Toiminta häiriötilanteissa ja poikkeusoloissa

Erilaisissa häiriötilanteissa ja poikkeusoloissa toimitaan tarvittaessa riskienhallintaan ja varautumiseen liittyvien suunnitelmien mukaisesti. Poikkeusolojen toiminnan suunnittelua koordinoi alueellinen pelastuslaitos