Ranuan kuntakonsernin tietoturva- ja tietosuojapolitiikka

RANUA

VERSIOHISTORIA:

Versio	Päiväys	Henkilö	Muutos/kuvaus
0.1	22.5.2005	Antti Hyvärinen ja Heikki Karppinen	Luonnos
0.2	9.2.2006	Jouko Niskavaara	
0.3	19.5.2006	Sirpa Hakala	
0.50	27.3.2020	Jaakko Lohi	Uudistettu dokumentti
0.51	14.2.2022	Jaakko Lohi	Muutama korjaus
1.0	22.1.2024	Jaakko Lohi	Päivitys

KATSELMOINTI/HYVÄKSYNTÄHISTORIA:

Versio	Päiväys	Katselmoija	Päiväys	Hyväksyjä	Kommentti
0.3	19.5.2006		29.5.2007	Khall § 147	
			26.11.2012	Khall § 307	
1.0	24.1.2024 16.2.2024	Tuoma Aikkila, Johanna Koivunen, Juha-Matti Sääskilahti	4.3.2024	Khall § 42 Valtuusto	

SISÄLLYSLUETTELO

Ranuan kuntakonsernin tietoturva- ja tietosuojapolitiikka

1. JOHDANTO

Tietoturva- ja tietosuojapolitiikka on kunnanvaltuuston hyväksymä dokumentti, jossa määritellään tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot Ranuan kuntakonsernissa. Tietoturvan ja tietosuojan parantaminen on osa kunnan ja kuntakonsernin toiminnan kehittämistä. Tietoturva- ja tietosuojapolitiikka määrittelee tietoturva- ja tietosuojapolitiikan toteuttamisen Ranuan kunnassa ja kuntakonsernissa. Kuntakonsernin johto tiedostaa, että organisaation tietojenkäsittelyn on oltava tietoturvallista, virheetöntä ja tehokasta. Tietoturva- ja tietosuojapolitiikkaan on koko henkilöstön sitouduttava ja se vaatii koulutusta sekä hyvää viestintää.

Tätä tietoturva- ja tietosuojapolitiikkaa täydentävät yksityiskohtaisemmat tietoturvaan ja -suojaan liittyvät kunta- ja tytäryhtiökohtaiset määräykset ja ohjeet. Ranuan kuntakonsernin tietoturva- ja tietosuojapolitiikka dokumentti on julkinen ja se on saatavilla kokonaisuudessa Ranuan kunnan internet-sivuilta.

2. KÄSITTEEET

Ymmärrettävä terminologia helpottaa dokumentin ymmärtämistä ja lukemista. Alle on koottu dokumentin sisältämiä peruskäsitteitä.

2.1. Tietoturva

Tietoturva ts. tietoturvallisuus on riskienhallintaa ja osa konsernin turvallisuutta. Tämä pitää sisältään tiedon saatavuuden, luottamuksellisuuden ja eheyden.

2.2. Tietosuoja

Tietosuoja turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen sisältyvät tietosuojaan.

2.3. Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan tietojen säilymistä luottamuksellisina. Tietoihin ja tietojenkäsittelyyn oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

2.4. Eheys

Eheys varmistaa, että tietojen tai tietojärjestelmien sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus ovat kunnossa.

2.5. Käytettävyys

Käytettävyydellä varmistetaan, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille turvallisesti saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

2.6. Henkilötieto

Luonnollista henkilöä kuvaava tieto, josta hänet voidaan tunnistaa. Useasti henkilötieto on tallennettu henkilörekisteriin.

2.7. Henkilötietojen käsittely

Henkilötietojen käsittely tarkoittaa mm. henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.

3. KATTAVUUS

Ranuan kunnan kunnanhallituksen vahvistama tietoturva- ja tietosuojapolitiikka koskee Ranuan kunnan kaikkia organisaatiota tytäryhtiöineen. Jokaisen kuntakonsernin viranhaltijan, työntekijän, luottamushenkilön, harjoittelijan, sekä muiden henkilöiden on tunnettava tietoturva- ja tietosuojapolitiikka. Myös muuhun ohjeistukseen on sitouduttava. Esihenkilöt vastaavat siitä, että henkilöstö tuntee ja noudattaa ohjeita. Myös ulkopuoliset toimijat on sitoutettava noudattamaan tietoturva- ja tietosuojaohjeita.

Asiakkaiden ja muiden sidosryhmien välisissä sopimuksissa ja tietoturvakäytäntöjen toteuttamisessa on vähimmäisvaatimuksena tämä politiikka ja tähän politiikkaan liittyvät ohjeet.

Kaikkien edellä mainittujen, on tunnettava tämän politiikan sisältö ja sitouduttava noudattamaan politiikassa kuvattuja periaatteita tavoitellun tietoturvallisuus- ja

tietosuojatason saavuttamiseksi. Tietoturvan hallintamenetelmät kohdistuvat kaikkeen aineistoon riippumatta tiedon esitystavasta.

4. TIETOTURVA- JA TIETOSUOJAPOLITIIKAN TAVOITTEET

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tietosuoja on tiedon luottamuksellista käsittelyä. Ranuan kuntakonsernin tavoitteena on turvata keskeiset toiminnot ja palvelut, johon kriittisenä osana sisältyy tietojärjestelmien keskeytymätön toiminta.

Kunta ja tytäryhtiöt varautuvat myös häiriö- ja poikkeusoloihin siten, että toimintaa ja palveluja voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa paikasta riippumatta. Politiikan tavoitteena on estää luottamuksellisten tietojen valtuuttamaton käyttö sekä turvata tietojen eheys tahattomalta tai tahalliselta tuhoutumiselta sekä muuttumiselta.

Erityistä huomiota kiinnitetään arkaluontoisen ja luottamuksellisen tiedon suojaamiseen ja salaamiseen. Tietoturvallisuutta kehitetään jatkuvasti ja kehitystyöllä pyritään ennalta pienentämään tietojenkäsittelyyn ja tietoon kohdistuvat uhat ja rajoittamaan vaikutukset hyväksyttävälle tasolle.

Tietoturvallisuudesta ja tietosuojasta huolehditaan kansallista tietoturvaa ja tietosuojaa koskevien lakien ja säädösten mukaisesti sekä noudattaen valtionhallinnon, kuntaliiton, EU:n tietosuoja-asetusta ja tietosuojavaltuutetun antamia ohjeita ja suosituksia.

5. RISKIENHALLINTA

Tietoturvan ja tietosuojan riskien arvioinnista vastaavat kunnan johto ja tytäryhtiöiden toimitusjohtajat/vastaava isännöitsijä. Tämä on osa kuntakonsernin sisäistä riskien hallintaa. Riskihallintaprosesseista vastaa kukin osastopäällikkö yhdessä esihenkilöiden kanssa ja tytäryhtiöiden osalta toimitusjohtajat/vastaava isännöitsijä sekä esihenkilöt. Tietoturva- ja tietosuojatyö on osana kunnan ja tytäryhtiöiden perustoimintoja, joita kehitetään jatkuvasti havaittujen epäkohtien pohjalta. Riskienhallinta kuuluu jokaisen työntekijän vastuulle.

6. ORGANISAATIO, ROOLIT JA VASTUUT

6.1. Kunta

6.1.1. Kunnanhallitus

- kunnan tietoturva- ja tietosuojapolitiikan linjausten ja päätösten hyväksyntä
- tietoturvallisuuden toteutumisen seuranta kunnassa

6.1.2. Kunnanjohtaja

- kokonaisvastuu tietoturva- ja tietosuojapolitiikan toteuttamisesta
- kunnan tietoturva-asioiden tiedottamisesta organisaation ulkopuolelle
- jatkuvuussuunnittelu poikkeusolojen varalle

6.1.3. Hallintojohtaja (Tietoturvajohtaja)

- kunnan tietoturva-asioiden tiedottaminen kunnan sisäpuolella
- vastaa tietoturva- ja tietosuojapolitiikan operatiivisesta toteutuksesta
- tietoturvallisuuteen liittyvät operatiivisen tason päätökset
- tietoturvan hallinnan organisointi, koordinointi, kehittäminen ja resursointi
- tietoturva- ja tietosuojan ohjaus
- riskienhallinnan arviointi
- raportointi kunnanhallitukselle

6.1.4. Tekninen johtaja

- toimitilojen tietoturvallisuus ylläpito ja kehittäminen yhteistyössä työsuojelupäällikön kanssa
- hälytys- ja valvontajärjestelmistä huolehtiminen

6.1.5. Osastopäälliköt

- osaston tietoturvatoimenpiteiden toimeenpano ja organisointi

- osastonsa tietoturva- ja tietosuojaohjeiden noudattamisen valvonta
- osaston omistamien tietojärjestelmien vastuuhenkilöiden/pääkäyttäjien nimeäminen
- osaston tietoturvakoulutusten järjestäminen
- tietojen käsittelyn lainmukaisuuden varmistaminen

6.1.6. Esihenkilöt

- yksikön tietoturvatoimenpiteiden toimeenpano ja organisointi
- vastaa käyttäjäoikeuksien hallinnasta ja ajantasaisuudesta
- valvoo ja varmistaa, että jokainen työntekijä on suorittanut kunnan tarjoamat tietoturva- ja tietosuojakoulutukset
- ohjeistaa, opastaa ja vastaa työntekijää päivittäisissä tietoturva- ja tietosuoja-asioissa sekä vastaa uusien työntekijöiden perehdyttämisestä kunnan tietoturva- ja tietoturvaohjeisiin
- työntekijöiden tietoturva- ja tietosuojapoikkeamista raportoiminen tietosuojavastaavalle

6.1.7. Tietosuojavastaava

- valvoo ja seuraa osaltaan tietosuojan toteutumista sekä raportoi organisaation johdolle tietosuojan ja tietoturvan tilasta ja kehittämistarpeista
- on mukana tietosuojan suunnittelussa, ohjeistamisessa, neuvonnassa sekä toteuttaa tai hankkii tarvittavia koulutuksia

6.1.8. ICT

- tietoturvaan ja tietosuojaan liittyvä ylläpito ja kehittäminen
- tietojärjestelmien ja tietotekniikan tietoturvan kehittäminen
- tietojärjestelmien varmistusprosessien ja palautumisen ylläpito ja kehittäminen
- tietoturvasta ja tietoturvapoikkeamista raportoiminen
- tietojärjestelmien käyttäjien ohjeistaminen

- tietoturvan koulutuksen järjestäminen
- jatkuvuussuunnitelman ylläpito

6.1.9. Tietojärjestelmien pää- ja varapääkäyttäjät

- tekee yhteistyötä ohjelmatoimittajan kanssa mm. ylläpidosta ja ohjelman päivitystarpeista
- huolehtii ohjelman päivityksestä ICT-asiantuntijoiden kanssa

6.1.10. Henkilöstö ja luottamushenkilöt

- noudattaa kunnan tai työnantajan ja esihenkilön antamia kirjallisia ja suullisia ohjeita
- toimii tietoturva- ja tietosuojapolitiikan sekä tietoturvaohjeiden mukaisesti
- käyttää tietojärjestelmiä lakien ja ohjeiden mukaisesti
- tietoturva- ja tietosuojapoikkeamista raportoiminen esihenkilölle/ tietosuojavastaavalle
- osallistuu tietoturvakoulutuksiin

6.2. Tytäryhtiöt

6.2.1. Hallitus

- yhtiöiden tietoturva- ja tietosuojapolitiikan linjausten ja päätösten hyväksyntä
- tietoturvallisuuden toteutumisen seuranta yhtiössä

6.2.2. Toimitusjohtaja/vastaava isännöitsijä

- kokonaisvastuu tietoturva- ja tietosuojapolitiikan toteuttamisesta
- yhtiön tietoturva-asioiden tiedottamisesta organisaation ulkopuolelle
- jatkuvuussuunnittelu poikkeusolojen varalle

6.2.3. Esihenkilöt

- valvoo ja varmistaa, että jokainen työntekijä on suorittanut konsernin tarjoamat tietoturva- ja tietosuojakoulutukset
- vastaa käyttäjäoikeuksien hallinnasta ja ajantasaisuudesta
- ohjeistaa, opastaa ja vastaa työntekijää päivittäisissä tietoturva- ja tietosuoja-asioissa sekä vastaa uusien työntekijöiden perehdyttämisestä yhtiön tietoturva- ja tietoturvaohjeisiin
- työntekijöiden tietoturva- ja tietosuojapoikkeamista raportoiminen toimitusjohtajalle tai vastaavalle isännöitsijälle
- riskienhallinnan arviointi

6.2.4. Tietojärjestelmien pää- ja varapääkäyttäjät

- tekee yhteistyötä ohjelmatoimittajan kanssa mm. ylläpidosta ja ohjelman päivitystarpeista
- vastaa käyttäjäoikeuksien hallinnasta ja ajantasaisuudesta

6.2.5. Henkilöstö

- noudattaa yhtiön tai työnantajan ja esihenkilön antamia kirjallisia ja suullisia ohjeita
- toimii tietoturva- ja tietosuojapolitiikan sekä tietoturvaohjeiden mukaisesti
- käyttää tietojärjestelmiä lakien ja ohjeiden mukaisesti
- tietoturva- ja tietosuojapoikkeamista raportoiminen esihenkilölle
- osallistuu tietoturvakoulutuksiin

7. TIETOTURVAN SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Ranuan kuntakonserni ylläpitää tietoturvallisuutta hallinnollisin, fyysisin ja teknisin menetelmin. Tietoturvan jatkuva kehittäminen varmistetaan yhteistyöllä ja riittävällä resursoinnilla.

Tietoturvadokumenttien ja kartoitusten avulla tunnistetaan tietoaineistot ja tietojärjestelmät, arvioidaan tietoaineistoon ja tietojen käsittelyyn liittyvät riskit, sekä

kehitetään menetelmät ja toimintatavat riskien poistamiseksi tai laskemiseksi hyväksyttävälle tasolle.

Henkilökunnalle kohdennetulla ohjeistuksella, koulutuksella teknisillä ratkaisulla sekä tiedottamisella varmistetaan, että henkilökunnalla on riittävät valmiudet paikasta riippumattomaan tietoturvalliseen työskentelytapaan. Organisaation kattavalla tietoturvan seurannalla varmistetaan, että tietojenkäsittely tapahtuu tietoturvallisesti, tietosuojaa noudattaen. Sisäisillä tarkastuksilla ja valvonnalla varmistutaan, että tietoturvakäytännöt on ymmärretty ja otettu käyttöön kaikissa kuntakonsernin toiminnoissa. Tietoturvallisuutta kehitetään aktiivisesti sidosryhmien, kuten tietotekniikan toimittajien kanssa.

Kunnan ja tytäryhtiöiden tietojenkäsittelyä ja tietojärjestelmien tietoturvan tasoa arvioidaan ja seurataan tarvittaessa ulkoisen tarkastuksen keinoin. Käyttäjätunnuksia ja käyttöoikeuksien muutoksia tehdään vain esihenkilön kirjallisesta pyynnöstä.