Tietoturva- ja tietosuojapolitiikka 2026

Kunnanhallitus 8.6.2026 § 125

Kunnanvaltuusto 15.6.2026 § 20

TIIVISTELMÄ

Tietoturva- ja tietosuojapolitiikka määrittelee organisaation tietoturvan tavoitteet, soveltamisalan sekä keskeiset periaatteet. Toiminta perustuu lainsäädäntöön ja viitekehyksiin, ja vastuut on selkeästi määritelty.

Tietojen ja tietojärjestelmien käyttöä ohjataan käyttöoikeuksin, hallituin laittein ja kirjautumisvaatimuksin. Riskienhallinta, jatkuvuuden turvaaminen ja kyberturvallisuus muodostavat toiminnan perustan.

Poikkeamien hallinta, lokitus ja valvonta varmistavat tietoturvan toteutumisen, ja henkilöstön koulutus sekä sitoutuminen tukevat turvallista toimintaa. Tietoturvaa kehitetään jatkuvasti politiikan ylläpidon ja päivityksen kautta.

SISÄLLYSLUETTELO

Asiakirjan tila	**Valmis**
Versio	**2.0**
Päivämäärä	**27.4.2026**
Omistaja	**Kunnanjohtaja**
Hyväksyjä	**Kunnanvaltuusto**
Katselmointiväli	**Vähintään vuosittain ja aina olennaisen muutoksen tai tietoturvapoikkeaman jälkeen**
Julkisuusluokka	**JULKINEN**

Versiohistoria ja keskeiset muutokset

Versio	Päiväys	Laatija / käsittelijä	Muutos
1.0	2018	Karstulan kunta	Aiempi tietoturvapolitiikan pohja ja vastuumalli.
2.0	27.4.2026	Luonnos	Päivitetty lainsäädäntöviittaukset, Traficom/Kyberturvallisuuskeskuksen ohjeiden mukaiset kyberturvallisuuden johtamiskäytännöt, hallittujen laitteiden kirjautumisvaatimus sekä poikkeama-, hankinta- ja toimittajahallinnan linjaukset.

1. JOHDANTO JA TARKOITUS

Karstulan kunnan toiminnassa käsitellään julkista, salassa pidettävää ja henkilötietoihin liittyvää tietoa. Tieto on välttämätön voimavara kunnan palvelutuotannossa, päätöksenteossa, lakisääteisten tehtävien hoitamisessa ja kuntalaisten oikeuksien toteuttamisessa.

Tämän tietoturvapolitiikan tarkoituksena on määritellä Karstulan kunnan tietoturvallisuuden ja tietosuojan johtavat periaatteet, vastuut ja vähimmäisvaatimukset. Politiikka ohjaa tietoturvasuunnitelmaa, henkilöstöohjeita, teknisiä vaatimuksia, hankintoja, sopimuksia ja jatkuvuudenhallintaa.

Tietoturvallisuudella tarkoitetaan hallinnollisia, toiminnallisia, fyysisiä ja teknisiä menettelyjä, joilla varmistetaan tiedon luottamuksellisuus, eheys, saatavuus ja tarvittaessa kiistämättömyys normaalioloissa, häiriötilanteissa ja poikkeusoloissa. Tietosuojalla tarkoitetaan henkilötietojen käsittelyn lainmukaisuuden ja rekisteröityjen oikeuksien varmistamista.

2. SOVELTAMISALA

Politiikka koskee Karstulan kunnan kaikkia toimielimiä, viranhaltijoita, työntekijöitä, luottamushenkilöitä, harjoittelijoita, määräaikaisia työntekijöitä, sidosryhmiä ja palveluntuottajia silloin, kun ne käsittelevät kunnan omistamaa, hallinnoimaa tai kunnan lukuun käsiteltävää tietoa.

Politiikkaa sovelletaan kaikkeen tietoon riippumatta tiedon muodosta, tallennuspaikasta, suojaustasosta, elinkaaren vaiheesta tai siirtotiestä. Politiikka koskee myös kunnan hankkimia pilvipalveluja, ulkoistettuja palveluja, integraatioita, mobiilikäyttöä, etäkäyttöä ja luottamushenkilöiden työskentely-ympäristöjä.

3. SÄÄDÖKSET JA OHJAAVAT VIITEKEHYKSET

Karstulan kunnan tietoturvallisuus ja tietosuoja perustuvat voimassa olevaan lainsäädäntöön, riskienhallintaan sekä viranomaisohjeisiin. Keskeisiä säädöksiä ja ohjeita ovat erityisesti:

- EU:n yleinen tietosuoja-asetus (EU) 2016/679 ja tietosuojalaki 1050/2018.
- Laki julkisen hallinnon tiedonhallinnasta 906/2019, erityisesti tiedonhallintayksikön vastuu, tietoturvallisuustoimenpiteet, tietojen siirto, käyttöoikeuksien hallinta ja lokitiedot.
- Laki viranomaisten toiminnan julkisuudesta 621/1999 sekä asiakirjojen julkisuutta, salassapitoa, arkistointia ja tiedonhallintaa koskevat muut säädökset.
- Laki sähköisen viestinnän palveluista 917/2014 ja laki yksityisyyden suojasta työelämässä 759/2004 silloin, kun käsitellään viestintää, välitystietoja, sähköpostia, lokitietoja tai työntekijöiden teknistä valvontaa.
- Traficomin Kyberturvallisuuskeskuksen ohjeet, Kybermittari sekä julkisen hallinnon Julkri-arviointikriteeristö soveltuvin osin.
- Kunnan omat hallintosääntö, riskienhallinnan ja sisäisen valvonnan ohjeet, hankintaohjeet sekä tietoturvasuunnitelmasta johdetut tarkentavat ohjeet.

Lainsäädäntö ei pääsääntöisesti määrää yksittäistä teknistä ratkaisua, vaan velvoittaa kunnan valitsemaan käsiteltävien tietojen ja järjestelmien riskeihin nähden asianmukaiset hallinnolliset, toiminnalliset ja tekniset suojaustoimet. Tämän vuoksi politiikassa asetetaan riskiperusteisia vähimmäisvaatimuksia, kuten monivaiheinen tunnistautuminen ja hallittujen päätelaitteiden käyttö.

4. TIETOTURVALLISUUDEN JA TIETOSUOJAN PERIAATTEET

Periaate	**Kunnan linjaus**
Riskiperusteisuus	Tietoturvatoimenpiteet mitoitetaan toiminnan kriittisyyden, tiedon luokituksen, uhkaympäristön, lainsäädännön ja vaikutusten perusteella.
Vähimmän oikeuden periaate	Käyttöoikeudet annetaan vain työtehtävän tai luottamustehtävän edellyttämässä laajuudessa ja vain niin pitkäksi ajaksi kuin tarve on olemassa.
Sisäänrakennettu ja oletusarvoinen tietosuoja	Tietosuoja ja tietoturva huomioidaan jo palvelun, prosessin, hankinnan ja tietojärjestelmän suunnitteluvaiheessa.
Omaisuudenhallinta	Kunnan tiedot, järjestelmät, laitteet, palvelut, integraatiot ja riippuvuudet tunnistetaan ja niiden elinkaarta hallitaan.
Jatkuva parantaminen	Tietoturvaa johdetaan vuosikellon, seurannan, mittareiden, riskikäsittelyn, harjoitusten ja auditointien avulla.
Toimittajavastuu	Ulkoistaminen ei poista kunnan vastuuta. Toimittajille asetetaan sopimuksissa tietoturva-, tietosuoja-, jatkuvuus- ja ilmoitusvelvoitteet.
Läpinäkyvyys ja oikeasuhtaisuus	Henkilöstöä ja luottamushenkilöitä informoidaan tietoturvavaatimuksista, lokituksesta ja valvonnasta. Valvonta rajataan välttämättömään ja perusteltuun tarkoitukseen.

5. TIETOTURVALLISUUDEN ORGANISOINTI JA VASTUUT

Rooli	Vastuu
Kunnanvaltuusto	Hyväksyy tietoturvapolitiikan.
Kunnanhallitus	Vastaa sisäisen valvonnan ja riskienhallinnan järjestämisestä sekä seuraa tietoturvallisuuden toteutumista.
Kunnanjohtaja	Omistaa tietoturvapolitiikan, vastaa tietoturvallisuuden ja tietosuojan toteuttamisen kokonaisuudesta sekä raportoinnista kunnanhallitukselle.
Johtoryhmä	Ohjaa riskienhallintaa, jatkuvuudenhallintaa, kehittämissuunnitelmaa ja merkittävien poikkeamien käsittelyä.
Palvelukekusjohtajat ja esihenkilöt	Vastaavat omien palveluidensa, prosessiensa, tietojensa ja järjestelmiensä tietoturvasta, käyttöoikeuksien tarpeellisuudesta ja henkilöstön perehdytyksestä.
Tiedon omistaja	Määrittää tiedon luokituksen, käsittelytarpeen, säilyttämisen, luovutukset ja käyttöoikeuksien asiasisällölliset perusteet.
Tietojärjestelmän omistaja	Vastaa järjestelmän riskienhallinnasta, tietoturvavaatimuksista, käyttöoikeuksien katselmoinneista, jatkuvuudesta ja toimittajayhteistyöstä.
Tietosuojavastaava	Neuvoo ja seuraa henkilötietojen käsittelyn lainmukaisuutta, tukee vaikutustenarviointeja ja toimii yhteyspisteenä valvontaviranomaiseen.
Tietosuojaryhmä / tietoturvaryhmä	Seuraa tietoturvan ja tietosuojan tilannekuvaa, käsittelee kehitystoimia, tukee poikkeamien hallintaa ja valmistelee ohjeita.
IT ja IT-palveluntuottajat	Toteuttavat teknisiä suojaustoimia, päätelaitehallintaa, käyttöoikeushallintaa, lokitusta, varmistuksia ja teknistä valvontaa sovittujen vastuiden mukaisesti.
Henkilöstö ja luottamushenkilöt	Noudattavat ohjeita, käyttävät vain hyväksyttyjä työvälineitä ja ilmoittavat poikkeamista, riskeistä ja epäilyttävistä tapahtumista viipymättä.

Sidosryhmät ja toimittajat	Noudattavat sopimuksissa ja erillisissä sitoumuksissa asetettuja tietoturva- ja tietosuojavaatimuksia.

6. TIEDON JA TIETOJÄRJESTELMIEN KÄYTTÖ

Kunnan tietojärjestelmiä, tietoverkkoja, sähköpostia, pilvipalveluja, työasemia ja mobiililaitteita käytetään ensisijaisesti työ- ja luottamustehtävien hoitamiseen. Kunnan tietoa saa tallentaa vain kunnan hyväksymiin tallennuspaikkoihin, järjestelmiin ja palveluihin.

- Käyttöoikeudet perustuvat hyväksyttyyn tarpeeseen, työtehtävään, rooliin tai luottamustehtävään.
- Yhteiskäyttöisiä tunnuksia vältetään. Henkilökohtainen tunnus, vahva salasana ja monivaiheinen tunnistautuminen ovat lähtökohta kaikissa keskeisissä palveluissa.
- Pääkäyttäjä- ja ylläpitotunnukset erotetaan henkilökohtaisista perustunnuksista, ja niitä käytetään vain ylläpitotehtäviin.
- Kunnan järjestelmiin ei saa asentaa luvattomia ohjelmistoja eikä niitä saa kytkeä hyväksymättömiin palveluihin tai integraatioihin.
- Salassa pidettävää tietoa ja henkilötietoja käsitellään vain niille hyväksytyissä järjestelmissä ja suojatuilla yhteyksillä.

7. HALLITTUJEN LAITTEIDEN KIRJAUTUMISVAATIMUS

> *Karstulan kunnan omistamiin, hallinnoimiin tai kunnan lukuun hankittuihin tietojärjestelmiin, pilvipalveluihin, etäyhteyksiin ja sähköisiin työtiloihin kirjautuminen sallitaan vain kunnan hallinnassa olevilta päätelaitteilta. Henkilökohtaisilla tai ulkopuolisen organisaation hallitsemilla laitteilla kirjautuminen on estetty, ellei tietojärjestelmän omistaja, IT ja tietosuojavastaava ole hyväksyneet kirjallista, riskiperusteista ja määräaikaista poikkeusta.*

Hallittu laite tarkoittaa laitetta, joka on kunnan omistama tai kunnan erikseen hyväksymä ja jonka tietoturva-asetukset, päivitykset, levyjen salaus, haittaohjelmasuojaus, palomuuri, näytön lukitus, etähallinta, etätyhjennys ja vaatimustenmukaisuuden tarkistus ovat kunnan tai sen valtuuttaman palveluntuottajan hallinnassa

Vaatimuksen oikeudellinen peruste on kunnan velvollisuus varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan, mitoittaa suojaustoimet riskiarvioinnin mukaisesti, suojata salassa pidettävien tietojen siirto sekä hallita käyttöoikeuksia ja lokitietoja. Henkilötietojen osalta vaatimus on osa rekisterinpitäjän velvollisuutta toteuttaa riskitasoon nähden asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla estetään luvaton pääsy, tietojen vuotaminen, muuttuminen, häviäminen tai muu lainvastainen käsittely.

Rajoitus on oikeasuhtainen, koska henkilökohtaisten laitteiden suojaustasoa, päivityksiä, haittaohjelmatilannetta, salausasetuksia, käyttäjäprofiileja, lokitusta ja tietojen poistamista ei voida luotettavasti todentaa. Hallittu laite mahdollistaa kunnan lakisääteisten velvoitteiden, tietoturvapolitiikan ja henkilötietojen suojaamisen käytännön toteuttamisen.

Poikkeus voidaan myöntää vain, kun palvelun käyttö on kunnan tehtävän kannalta välttämätöntä eikä hallittua laitetta ole saatavilla. Poikkeus kirjataan poikkeusrekisteriin, sille määritetään voimassaoloaika, sallittu käyttötapa, tekniset lisäsuojaukset ja vastuuhenkilö. Poikkeuksissa suositaan selain- tai virtuaalityöpöytäratkaisua, joka estää tietojen paikallisen tallentumisen ja edellyttää monivaiheista tunnistautumista.

8. RISKIENHALLINTA, JATKUVUUS JA KYBERTURVALLISUUS

Tietoturvallisuus on osa kunnan kokonaisriskienhallintaa, valmiutta ja jatkuvuudenhallintaa. Kunta ylläpitää ajantasaista kuvaa kriittisistä palveluista, tietojärjestelmistä, tietoaineistoista, toimittajista, integraatioista ja avainhenkilöistä.

- Riskit arvioidaan säännöllisesti sekä aina olennaisen toimintatapamuutoksen, hankinnan, käyttöönoton, poikkeaman tai uhkatilanteen yhteydessä.
- Kriittisille palveluille määritetään jatkuvuus- ja toipumisvaatimukset, kuten palautumisaikatavoite, palautumispistetavoite, varamenettelyt ja viestintävastuut.
- Kunta hyödyntää soveltuvin osin Traficomin Kyberturvallisuuskeskuksen Kybermittaria ja Julkri-kriteeristöä tietoturvan arvioinnissa, kehittämisessä ja johdon raportoinnissa.
- Varmuuskopiointi, palautustestit, päivitystenhallinta, haavoittuvuuksien käsittely, tietoturvaharjoitukset ja toimittajariippuvuuksien hallinta ovat jatkuvuuden vähimmäistoimenpiteitä.

9. HANKINNAT JA TOIMITTAJAHALLINTA

Tietoturva- ja tietosuojavaatimukset määritellään jo hankinnan suunnitteluvaiheessa. Tarjouspyyntöihin, sopimuksiin ja palvelukuvauksiin sisällytetään vähintään tiedon käsittelyn sijaintia, käyttöoikeuksia, lokitusta, varmistuksia, haavoittuvuuksien korjaamista, alihankkijoita, auditointioikeutta, jatkuvuutta, poikkeamailmoituksia ja sopimuksen päättymisen jälkeistä tietojen palauttamista tai hävittämistä koskevat ehdot.

Toimittajan kanssa tehdään henkilötietojen käsittelysopimus, jos toimittaja käsittelee henkilötietoja kunnan lukuun. Toimittajan pääsy kunnan tietoihin tai ympäristöihin rajataan välttämättömään, määräaikaiseen ja valvottuun käyttöön. Kriittisissä palveluissa edellytetään toimittajalta jatkuvuusjärjestelyjä, varahenkilöitä ja kykyä toimia häiriötilanteissa.

10. POIKKEAMAT, VALVONTA JA LOKIT

Tietoturva- ja tietosuojapoikkeamat käsitellään viipymättä, johdonmukaisesti ja dokumentoidusti. Jokaisella työntekijällä, luottamushenkilöllä ja toimittajalla on velvollisuus ilmoittaa epäillystä tietoturvapoikkeamasta, tietovuodosta, haittaohjelmasta, kadonneesta laitteesta, virheellisestä käyttöoikeudesta tai kalasteluviestistä sovitun ilmoituskanavan kautta.

- Poikkeamat luokitellaan vaikutuksen, kiireellisyyden ja tietosuojariskin perusteella.
- Henkilötietojen tietoturvaloukkaus arvioidaan tietosuoja-asetuksen mukaisesti, ja tarvittavat ilmoitukset tehdään tietosuojavaltuutetun toimistolle ja rekisteröidyille määräajoissa.

- Vakavista kyberpoikkeamista voidaan ilmoittaa Traficomin Kyberturvallisuuskeskukselle avun, tilannekuvan ja varoitusten hyödyntämiseksi.
- Lokitietoja kerätään tietoturvallisuuden, väärinkäytösten selvittämisen, järjestelmien toimivuuden ja lakisääteisten velvoitteiden vuoksi. Lokien käsittely rajataan valtuutetuille henkilöille ja määriteltyihin tarkoituksiin.
- Työntekijöiden tekninen valvonta käsitellään lain edellyttämällä tavalla, mukaan lukien tarpeellinen yhteistoimintamenettely ja henkilöstön informointi.

11. KOULUTUS, SITOUTUMINEN JA SEURAAMUKSET

Kunta huolehtii henkilöstön, luottamushenkilöiden ja tarvittaessa sidosryhmien tietoturva- ja tietosuojaosaamisesta perehdytyksellä, toistuvalla koulutuksella, kohdennetuilla ohjeilla ja harjoituksilla. Koulutus kattaa vähintään salasanat ja monivaiheisen tunnistautumisen, kalastelun tunnistamisen, etätyön, mobiililaitteet, salassa pidettävät tiedot, henkilötietojen käsittelyn, poikkeamailmoitukset ja hallittujen laitteiden käytön.

Kunnan tietoturva- ja tietosuojaohjeiden rikkominen voi johtaa käyttöoikeuksien rajoittamiseen, työnjohdollisiin seuraamuksiin, sopimusseuraamuksiin, vahingonkorvausvastuuseen tai asian ilmoittamiseen toimivaltaiselle viranomaiselle. Seuraamukset arvioidaan tapauskohtaisesti, oikeasuhtaisesti ja voimassa olevan lainsäädännön mukaisesti.

12. POLITIIKAN YLLÄPITO

Viite	**Käyttö tässä asiakirjassa**
Laki julkisen hallinnon tiedonhallinnasta 906/2019	Tietoturvallisuuden johtaminen, tietoaineistojen ja tietojärjestelmien tietoturvallisuus, tietojen siirto, käyttöoikeudet ja lokit.
EU:n yleinen tietosuoja-asetus (EU) 2016/679 ja tietosuojalaki 1050/2018	Henkilötietojen käsittelyn lainmukaisuus, osoitusvelvollisuus, sisäänrakennettu ja oletusarvoinen tietosuoja sekä käsittelyn turvallisuus.
Laki viranomaisten toiminnan julkisuudesta 621/1999	Julkisuus, salassapito ja asiakirjojen käsittelyn periaatteet.
Laki sähköisen viestinnän palveluista 917/2014	Tietoliikenteen ja viestinnän tietoturvan toteuttaminen sekä välttämättömät suojaustoimet.

Laki yksityisyyden suojasta työelämässä 759/2004	Työntekijöiden sähköpostin käsittely, tekninen valvonta ja henkilötietojen käsittely työelämässä.
Traficom / Kyberturvallisuuskeskus: Kybermittari	Kyberturvallisuuden kypsyystason arviointi, riskienhallinnan tuki ja kehitystoimenpiteiden priorisointi.
Traficom / Kyberturvallisuuskeskus: ohjeet tietomurroilta suojautumiseen, etätyöhön, IT-omaisuuden hallintaan, Entra ID -asetuksiin ja reunalaitteisiin	Päivitykset, monivaiheinen tunnistautuminen, hallitut päätelaitteet, pääsyn rajoittaminen, omaisuudenhallinta ja etäyhteyksien suojaus.
Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)	Julkishallinnon tietoturvan arvioinnin, hankintojen ja vaatimustenmukaisuuden tukikehys.
Kunnan sisäiset ohjeet ja sopimukset	Käyttövaltuuspolitiikka, lokienhallintapolitiikka, varmuuskopiointi, hankintaohje, etätyöohje, tietoturva- ja tietosuojasitoumukset.