

Kuhmoisten kunnan henkilöstön tietoturvaohje

Kuhmoisten kunnanhallitus xx.xx.2026 §

Sisällys

1.	Johdanto	2
1.1	Keskeiset ohjeet	2
1.2	Mitä tietoturvallisuudella tarkoitetaan?	4
1.3	Miksi tietoturvallisuus on tärkeää?	4
1.4	Lainsäädäntö tietoturvallisuuden perustana	5
2.	Asianhallinta ja tietojenkäsittely	5
2.1	Työhön liittyvät tiedot	5
2.2	Salassapitovelvollisuus	6
2.3	Haastattelut ja kysely	6
2.4	Omat tiedot ja yksityisyys	6
3.	Työpaikalla	7
3.1	Tietokoneen käyttö	7
3.2	Käyttäjätunnukset ja salasanat	7
3.3	Internet ja sähköposti	7
3.4	Toimitilojen turvallisuus	8
4.	Liikkuva työ	9
5.	Ongelmatilanteet	9
5.1	Ilmoitusvelvollisuus ja ongelmatilanteessa	9
5.2	Seuraamukset	10
6.	Ohjeiden valvonta ja päivittäminen	10
7.	Lisätietoa	10

1. Johdanto

Tämä ohje on tarkoitettu Kuhmoisten kunnan henkilöstölle tietoturvallisuutta koskevaksi ohjeeksi. Ohjeessa on tiivistettynä keskeisimmät tietoturvallisuuden perusasiat ja käytännön neuvot tietotekniikkaa työssään käyttäville työntekijöille. Asiakaskeskeinen, tietoturvan huomioonottava ja häiriötön palvelutuotanto on yhteinen haasteemme. Vastuu tietoturvallisuudesta kuuluu omalta osaltaan jokaiselle, myös sinulle.

Julkisuuslain 24 §:n perusteella organisaation sisäiseen turvallisuuteen liittyvät suunnitelmat ovat salassa pidettäviä asiakirjoja. Tämän ohjeiston sisältö ei kuitenkaan ole niin yksityiskohtaista, että se olisi turvallisuutta vaarantava asia. Kaikkien tietojärjestelmiä koskevien asiakirjojen säilytyksessä tulee kuitenkin ottaa turvallisuus huomioon.

1.1 Keskeiset ohjeet

1. **Perehdy ja pysy ajan tasalla.** Lue tämä ohje huolellisesti ja seuraa kunnan tietoturvaan liittyviä tiedotteita ja ohjeita. Osallistu sinulle tarjottuun koulutukseen ja toimi saamiesi ohjeiden mukaisesti.
2. **Valvo työtiloja ja laitteita.** Älä jätä ulkopuolista henkilöä valvomatta kunnan toimitiloihin tai työhuoneeseesi, etenkin jos siellä on tietojärjestelmiä tai asiakirjoja esillä.
3. **Pidä tunnuksesi omana tietonasi.** Älä anna kenenkään käyttää tietokonettasi, mobiililaitettasi, käyttäjätunnuksiasi tai salasanojasi.
4. **Noudata puhtaan pöydän ja näytön periaatteita.** Säilytä salassa pidettävät asiakirjat ja laitteet lukitussa tilassa, äläkä jätä tietoja näkyville työpöydälle tai näytölle.
5. **Käsittele tietoa huolellisesti kaikissa muodoissa.** Huolehdi tietojen turvallisesta käsittelystä riippumatta siitä, onko tieto sähköisessä muodossa, paperilla, puhelimessa tai keskustelussa.
6. **Suojaa salasanasi ja tunnistautumisesi.** Käytä vahvoja salasanoja ja monivaiheista tunnistautumista aina kun mahdollista. Vaihda salasanasi heti, jos epäilet sen paljastuneen.

7. **Lukitse laitteesi aina poistuessasi.** Estä asiattomien pääsy tietoihin lukitsemalla tietokoneesi tai puhelimesi heti, kun poistut työpisteestäsi.
8. **Käytä laitteita ja järjestelmiä vain työtehtäviisi.** Kunnan tietojärjestelmät, laitteet ja sovellukset on tarkoitettu työtehtäviin. Älä asenna ohjelmia tai tee ohjelmiin asetusten muutoksia ilman tietohallinnon lupaa.
9. **Tallenna työsi turvallisesti.** Tallenna työsi aina kunnan hyväksymille verkkoasemille tai pilvipalveluihin, joista tiedot varmuuskopioidaan automaattisesti. Älä säilytä pysyvästi tiedostoja työasemasi kovalevyllä tai henkilökohtaisissa pilvipalveluissa.
10. **Hae tulosteesi ajoissa ja käsittele paperitietoa vastuullisesti.** Nouda tulosteet heti ja hävitä salassa pidettävä aineisto tietoturvamateriaalin keräysastiaan.
11. **Muista roolisi verkossa.** Kun käytät kunnan sähköpostia, mobiililaitetta tai verkkoa, toimit aina organisaation edustajana. Käyttäydy verkossa asiallisesti ja vastuullisesti.
12. **Suojaa tiedonsiirto.** Käytä aina salattuja yhteyksiä (esim. VPN) ja kunnan hyväksymiä tiedonsiirtotapoja, kun käsittelet tai siirrät salassa pidettävää tietoa verkon kautta.
13. **Käytä ulkoisia muistivälineitä varoen.** Jos siirrät aineistoa muistitikulla tai muulla laitteella, varmista että se on tarkistettu virustorjuntaohjelmalla ennen käyttöä.
14. **Huolehdi laitteiden ja sovellusten päivityksistä.** Salli automaattiset tietoturvapäivitykset ja varmista, että käyttämäsi ohjelmistot ovat ajantasaisia.
15. **Toimi turvallisesti etätöyssä.** Käytä vain kunnan hyväksymiä laitteita ja yhteyksiä. Huolehdi, että muut eivät näe näyttöäsi tai kuule luottamuksellisia keskusteluja.
16. **Suojaa tiedot mobiililaitteilla.** Käytä laitteen lukitusta, PIN-koodia tai biometrisiä tunnisteita. Ilmoita välittömästi, jos laite katoaa tai varastetaan.
17. **Käytä tekoälyä vastuullisesti.** Älä käsittele luottamuksellisia tai henkilötietoja tekoälypalveluissa (esim. ChatGPT, Copilot jne.) ilman lupaa. Noudata kunnan tekoälyohjeistusta.
18. **Ilmoita poikkeamista ja epäilyistä.** Kerro välittömästi omalle esihenkilöllesi tai hallintojohtajalle, jos havaitset tietoturvaloukkauksen, virheen, väärinkäytöksen tai muun uhkatilanteen. Nopealla reagoinnilla voidaan estää vahingot.

19. **Kysy rohkeasti neuvoa.** Jos jokin tietoturvaan tai tietosuojaan liittyvä asia on epäselvä, kysy ohjeistusta esihenkilöltäsi tai hallintojohtajalta.

20. **Ota tietoturva osaksi arkea.** Älä koskaan vähättele tietoturvaan liittyviä asioita. Jokaisen huolellinen toiminta on osa kunnan yhteistä tietoturvaa ja kuntalaisten luottamuksen säilyttämistä.

1.2 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuudella tarkoitetaan, että laitteistot, ohjelmistot, tietoliikenneyhteydet ja tiedot on suojattu fyysisesti, teknisesti ja toiminnallisesti.

Tietoturvallisuuden keskeiset osa-alueet ovat:

- **Luottamuksellisuus:** tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä.
- **Eheys:** tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia. Ne eivät ole hallitsemattomasti muuttuneet tai muutettavissa.
- **Käytettävyys:** tiedot, järjestelmät ja palvelut ovat niiden käyttöön oikeutettujen käytettävissä.

Tietosuoja on tietojen valtuudettoman saannin estämistä ja luottamuksellisuuden säilyttämistä. Se on myös henkilötietojen suojaamista valtuudettomalta tai henkilöä vahingoittavalta käytöltä.

1.3 Miksi tietoturvallisuus on tärkeää?

Tietoturvaa ylläpitämällä turvataan yksilön, yhteisön ja yhteiskunnan etuja.

Tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Yhteiskunnan toiminnot ovat nykyään suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta.

Tietoturvallisuudesta huolehtiminen on jokaisen työntekijän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleensä kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuuden toteutumiseen ei siis riitä vain tekniikka, vaan myös jokapäiväiset toimintatapamme ja asenteemme.

Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki.

1.4 Lainsäädäntö tietoturvallisuuden perustana

Julkishallinnossa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Tietosuoja ja tietoturvaa koskevia lakeja on useita. Päivittäisessä työssä on noudatettava henkilötietolain ja viranomaisen toiminnan julkisuutta koskevan lainsäädännön määräyksiä.

Lainsäädäntö velvoittaa viranomaisia huolehtimaan tietoaineistojensa yhdenmukaisesta ja laadukkaasta hallinnasta sekä julkisuusperiaatteen tietoturvalisesta toteuttamisesta. (Laki julkisen hallinnon tiedonhallinnasta 1 §)

EU:n yleisen tietosuoja-asetuksen mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet taatakseen riskien mukaisen turvallisuustason. Arvioinnissa on otettava huomioon erityisesti käsittelystä aiheutuvat riskit, kuten vahingossa tai laittomasti tapahtuva hävittäminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy henkilötietoihin. (GDPR art. 32)

2. Asianhallinta ja tietojenkäsittely

2.1 Työhön liittyvät tiedot

Tunnista käsittelemäsi asiakirjan julkisuus/salassapito ja selvitä siihen liittyvät käyttöä, luovutusta ja käsittelyä koskevat rajoitukset.

Mikäli käsittelet salassa pidettävää asiakirjaa, vastaat omalta osaltasi tiedon salassa pysymisestä.

Jos käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo myös syöttämästä salasanojasi siten, että joku näkee salasanasi sormiesi liikkeistä.

Muista tallentaa työsi verkkoasemalle. Verkkoasema varmuuskopioidaan säännöllisesti. Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella laitteella tai tietovälineellä, jonka varmuuskopiointi ei ole säännöllistä.

Tarkista organisaation ulkopuolelta tuotu muistitikku tai muu tiedonsiirtoväline virustorjuntaohjelmalla ennen käyttöä. Säilytä salassa pidettävää tietoa sisältävät tallennusvälineet ja kannettavat tietokoneet lukitussa paikassa.

Huolehdi siitä, ettei luottamuksellisia papereita jää lojumaan verkkotulostimille tai kopiokoneille. Hae tulosteet verkkotulostimelta välittömästi. Luottamuksellisen tiedon

välittämistä puhelimitse tulee välttää. Jos puhelinta kuitenkin on käytettävä, tulee pyrkiä varmistamaan toisen osapuolen henkilöllisyys mahdollisimman hyvin.

2.2 Salassapitovelvollisuus

Salassapitovelvollisuudesta säädetään julkisuuslaissa sekä useissa muissa laeissa. Kaikilla Kuhmoisten kunnan työntekijöillä on vaitiolo- ja salassapitovelvollisuus lainsäädännön perusteella ei-julkisiksi määritellyistä tiedoista.

2.3 Haastattelut ja kysely

Ohjaa haastattelu- ja kyselypyynnöt asiasta vastaavalle henkilölle ja toimi Kuhmoisten kunnan tiedotusohjeen mukaisesti.

Varo antamasta viattomankin oloisten keskustelujen tai lomakkeiden yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista.

Ohjaa tietojen luovutus- ja tutkimuspyynnöt aineiston vastuuhenkilölle, jonka tehtävänä on päättää luovutuksesta ja mahdollisesta kustannusten korvattavuudesta.

2.4 Omat tiedot ja yksityisyys

Älä käytä työ sähköpostiosoitetta yksityiseen viestintääsi.

Älä tallenna omia yksityisiä tiedostoja työasemalle tai verkkokansioon.

Huomaa että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, myös sähköpostiliikenteestä ja Internetin selaamisesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäyttöksiin voidaan puuttua.

3. Työpaikalla

3.1 Tietokoneen käyttö

Tietokoneen käytöllä tarkoitetaan sekä oman työaseman että verkon kautta käytettävien palveluiden käyttämistä.

Vastaat käyttämästäsi tietokoneesta. Ole siis huolellinen.

Vain valtuutettu henkilö saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia.

Kirjaudu koneelle aina omilla käyttäjätunnuksillasi.

Lukitse tai sammuta työasemasi aina kun poistut työpisteestäsi.

Tallenna työsi käyttämällä välitallennuksia. Älä jätä työtäsi tallentamatta, kun poistut työpisteestäsi.

Tallenna työsi verkkoasemalle, joka varmuuskopioidaan säännöllisesti.

Jos työaseman kiintolevy tai muu tallennusväline, kuten muistitikku rikkoontuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Toimita tallennusväline IT-tuen hävitettäväksi.

3.2 Käyttäjätunnukset ja salasanat

Käyttäjätunnuksesi on henkilökohtainen. Älä luovuta sitä toiselle henkilölle.

Jokainen vastaa käyttäjätunnustensa turvallisesta säilyttämisestä. Vastuualueiden esihenkilöt vastaavat henkilöstömuutosten yhteydessä tapahtuvista tunnusten vaihtamisista ja lopettamisista.

Käytä riittävän monimutkaisia salasanoja. Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.

3.3 Internet ja sähköposti

Internet ja sähköposti ovat keskeisiä työvälineitä sekä tiedonhakuun että viestintään. On kuitenkin tärkeää muistaa, että kaikki verkkoliikenne ei oletusarvoisesti ole suojattua, ja suojaamattomana lähetetyt tiedot voivat päätyä väärin käsiin.

Sähköpostin ja muiden verkkopalveluiden käyttö edellyttää käyttäjältä huolellisuutta ja organisaation tietoturvakäytäntöjen noudattamista.

Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi.

Älä käytä Internetin palveluissa samoja salasanoja kuin työpaikan palveluissa.

Käytä vain sellaisia palveluita, jotka tiedät asiallisiksi. Haittaohjelmat ja virukset voivat levitä huomaamattomasti pelkästään Internet-sivuja selaamalla.

Tekijänoikeussäännöt on huomioitava Internetistä peräisin olevan aineiston käytössä.

Työsähköpostiosoitetta käyttäessäsi esiinnyt kunnan edustajana kaikessa toiminnassasi verkoissa.

Muista, että viranomaisella on velvollisuus käsitellä virkasähköpostiin saapuvat viestit.

Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Muista että sinulla on vaitiolovelvollisuus vahingossa tietoosi saamastasi viestistä.

Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi.

Roskapostia ei saa lähettää eikä välittää eteenpäin vaan se tulee poistaa välittömästi. Roskapostiin ei saa missään tapauksessa vastata.

Suhtaudu aina pienellä varauksella sähköpostin luotettavuuteen.

Sähköposti voi tulla myös muualta kuin viestin lähettäjänä näkyvältä henkilöltä, esimerkiksi tietokoneviruksen lähettämänä.

Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Älä avaa epäilyttäviä sähköposteja.

Varmista että sähköpostisi käsittelyyn liittyvät velvollisuutesi tulevat hoidettua myös poissaololesi aikana. Ota poissaolosi ajalle käyttöön sähköpostin automaattinen poissaolovastaus.

3.4 Toimitilojen turvallisuus

Lukitse työhuoneesi ovi, kun poistut huoneesta. Huolehdi että myös ikkunat on suljettu työpäivän päättyessä.

Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin tiloihin.

Suuntaa asiakaspalvelutilanteessa tietokoneesi näyttö oikein. Onko tarkoitus, että tiedot näkyvät asiakkaalle vai ei?

Säilytä tärkeät muistilaitteet ja paperit lukitussa tilassa.

Ohjaa vieraat tai ”eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.

4. Liikkuva työ

Liikkuvan työn välineet kehittyvät ja monipuolistuvat jatkuvasti. Ne vastaavat ominaisuuksiltaan jo työpaikan työasemia. Samat tietoturvaohjeet koskevat myös liikuteltavia välineitä. Mutta koska välineitä liikutellaan työpaikan toimitilojen ulkopuolellakin, on niiden tietoturvallisessa käytössä lisää huomioitavia asioita.

Älä jätä matkapuhelinta tai kannettavaa tietokonetta autoon tai muuhunkaan vartioimattomaan paikkaan näkyville edes lyhyeksi hetkeksi.

Älä säilytä ylimääräistä tai työhön kuulumatonta tietoa liikuteltavissa laitteissa. Laitteen joutuminen asiattomiin käsiin on aina mahdollista.

Tutustu laitteen käyttöohjeisiin huolellisesti.

Huolehdi että laitteissa on PIN-koodin ja/tai salasanan kyselyt päällä.

Mikäli et tarvitse/käytä langattomia palveluita (WLAN ja Bluetooth), niin poista ne käytöstä (sammuta). Tämä koskee myös puhelimia, joissa on mahdollista käyttää langattomia palveluita.

Muista varmuuskopioida/synkronoida mobiililaitteet säännöllisesti.

Älä puhu luottamuksellisista asioista julkisilla paikoilla.

5. Ongelmatilanteet

5.1 Ilmoitusvelvollisuus ja ongelmatilanteessa

Jos epäilet jotain tietoturvaa vaarantavaa tapahtuneen, ilmoita siitä välittömästi esihenkilöllesi tai hallintojohtajalle. He osaavat ryhtyä tarvittaviin toimenpiteisiin.

Jos saat työasemallesi oudon virhe- tai varoitusilmoituksen, älä hätäännä. Jos et tiedä, miten toimia niin kysy neuvoa esihenkilöltäsi tai IT-tuesta.

Kirjoita ylös havaintosi, tekemisesi sekä mitä mahdollisessa ilmoituksessa tai varoituksessa luki.

Jos epäilet virus- tai haittaohjelmatartuntaa työasemallasi: työasemaa ei tarvitse sammuttaa, mutta irrota verkkokaapeli työasemastasi ja ota yhteyttä IT-tukeen

Ilmoita aina, jos huomaat tai epäilet puutteita missä tahansa turvallisuuteen liittyvässä asiassa.

5.2 Seuraamukset

Lakien, määräysten ja ohjeiden rikkomisesta tai laiminlyönnistä käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Näistä tiedotetaan aina esihenkilölle.

Vakavissa tapauksissa väärinkäyttö voi johtaa vahingonkorvausvaatimuksiin ja rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös vaikutuksia työ/virkasuhteen jatkumiseen.

6. Ohjeiden valvonta ja päivittäminen

Näiden ohjeiden valvonnasta vastaavat hallintojohtaja ja esihenkilöt omalla vastuualueellaan. Ohjeiden vastaisesta toiminnasta on aina ilmoitettava.

Ohjeita päivitetään tarvittaessa. Päivitystarvetta seuraa kunnan johtoryhmä. Ohjeet hyväksyy kunnanhallitus.

7. Lisätietoa

Lisää tietoa tietoturvasta on saatavissa mm. seuraavista lähteistä:

- Lainsäädäntö. Valtion säädöstietopankki ([Finlex](#))
- Valtionvarainministeriön VAHTI-ohjeet ([Palveluiden ja turvallisuuden ohjaus - Valtiovarainministeriö](#))
- Kansallisarkisto ([Etusivu | Kansallisarkisto](#))
- Traficomin Kyberturvallisuuskeskus ([Traficomin Kyberturvallisuuskeskus | Kyberturvallisuuskeskus](#))