

Kauniaisten kaupungin tietoturva-, tietosuoja- ja salassapito-ohje luottamushenkilöille

Tämä ohje koskee niitä laitteita, joita luottamushenkilö käyttää luottamushenkilötehtävissään.

1. Tietoturva

- Laitteet ja tietojärjestelmät
 - Luottamushenkilö vastaa käytössään olevista omista työasemista ja muista laitteista, joita käyttää luottamushenkilötehtävissään.
 - Luottamustehtävässä saatua tietoaineistoa tulee käsitellä huolellisesti ja mahdollisesti annettujen lisäohjeiden mukaan.
 - Kaupungin tietojärjestelmistä tulee kirjautua ulos ja huolehtia laitteiden lukitsemisesta, kun niitä ei käytä.
 - Havaituista kaupungin tietojärjestelmiin liittyvistä väärinkäytöksistä tulee välittömästi ilmoittaa osoitteeseen paatosvalmistelu@kauniainen.fi.
 - Tuntemattomien tai epäilyttävien viestien tai linkkien vastaanottamisessa tulee olla varovainen, kun on kaupungin tietoteknisessä ympäristössä.
 - Jos epäilee, että käyttämäänsä työasemaan on tullut haittaohjelma, tulee lopettaa työskentely kyseisellä työasemalla ja ilmoittaa asiasta välittömästi osoitteeseen paatosvalmistelu@kauniainen.fi.
 - Kaupungin tarjoama tietosuoja- ja tietoturvakoulutus tulee suorittaa.
- Sähköposti ja käyttäjätunnukset
 - Luottamustehtävässä tulee käyttää kauniainen.fi -sähköpostia ja käyttäjätunnusta.
 - Kaupungin sähköpostista ei saa luoda uudelleenohjauksia toiseen sähköpostiosoitteeseen.
 - Kirjautumisessa kaupungin järjestelmiin on käytössä kaksivaiheinen tunnistautuminen.
 - Työasemia ja tietojärjestelmiä tulee käyttää omalla käyttäjätunnuksella ja salasanalla.
 - Henkilökohtaiset tunnistautumistiedot tulee säilyttää huolellisesti eikä niitä, kuten käyttäjätunnusta tai salasanaa, saa säilyttää esimerkiksi lompakossa tai käsilaukussa.
 - Käyttäjätunnusta ja salasana ei saa antaa muiden käyttöön.
 - Samaa käyttäjätunnusta ja salasanaa ei saa käyttää muissa järjestelmissä tai palveluissa.
 - Luottamushenkilö vastaa omalla käyttäjätunnuksella tehdyistä merkinnöistä ja muusta omilla tunnuksilla tehdystä käytöstä.
 - Tunnuksilla tehdystä käytöstä kerätään lokitietoa. Lokitieto tarkoittaa dokumentoitua tietoa jostakin tapahtumasta järjestelmissä, verkoissa tai muussa ympäristössä tai toiminnassa jonakin tiettyinä hetkenä.
- Ulkomaan käyttö
 - Kaupungin sähköpostin ja kokoushallintajärjestelmän käyttö ulkomailla – tai tilanteissa, joissa työaseman maantieteellinen sijainti (IP-osoitteen perusteella) näkyy ulkomailla sijaitseväksi esimerkiksi VPN-yhteyden vuoksi – aiheuttavat kaupungille automaattisia tietoturvaan liittyviä hälytyksiä. Nämä hälytykset voivat johtaa lisäselvityksiin ja mahdollisiin kustannuksiin kaupungille, sillä ulkomailta tuleva käyttö nähdään poikkeavana ja siihen suhtaudutaan varauksella tietoturvan varmistamiseksi.
 - Jotta tällaiset tilanteet voidaan ennakoida ja minimoida turhat hälytykset sekä niistä aiheutuvat kustannukset, kaupunki ilmoittaa palveluntuottajalle etukäteen niiden luottamushenkilöiden nimet, jotka tulevat käyttämään kaupungin sähköpostia ja kokoushallintajärjestelmää luottamustoimensa aikana.

2. Tietosuoja

- Henkilötietojen käsittely
 - Luottamustehtävässä saa käsitellä vain sellaisia henkilötietoja, joiden käsittely kuuluu tehtävään. Henkilötietoja ovat kaikki tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti, esimerkiksi nimi, henkilötunnus, kotiosoite, sähköpostiosoite, puhelinnumero, henkilökortin numero, auton rekisterinnumero, matkapuhelimen paikannustiedot ja IP-osoite.
 - Henkilötietojen käsittely tarkoittaa henkilötietoihin kohdistuvia toimintoja, joko tietojärjestelmässä tai manuaalisesti, kuten henkilötietojen keräämistä, tallentamista, muokkaamista ja poistamista. Pelkkä henkilötietojen haku ja katselu on niiden käsittelyä.
 - Luottamustehtävään liittyviä henkilötietoja saa käsitellä vain siinä tarkoituksessa, mitä varten ne on kerätty ja vain siinä määrin kuin on välttämätöntä tehtävän tekemisen kannalta.
- Henkilötietoihin kohdistuva tietoturvaloukkaus
 - Havaituista luottamustehtävään liittyvistä henkilötietoihin kohdistuneista tietoturvaloukkauksista tulee välittömästi ilmoittaa osoitteeseen paatosvalmistelu@kauniainen.fi.
 - Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan luottamustehtävään kuulumattomien henkilötietojen katselu, väärin määritellyt käyttöoikeudet tai murtautuminen henkilötietoja sisältävään järjestelmään. Tietoturvaloukkauksen seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho. Ulkopuolinen taho voi olla myös luottamushenkilö, jolla ei ole oikeutta tiedon käsittelyyn.

3. Salassapito

- Luottamustehtävän aikana ja sen päätyttyä ei saa ilmaista sivulliselle tehtävään liittyviä, kaupunkia ja sen henkilöstöä, asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja, esim. liike- tai ammattisalaisuuksia tai henkilön perhe-elämää tai muita henkilökohtaisia oloja koskevia tietoja, ellei lainsäädännöstä tai asianomaisen antamasta suostumuksesta muuta johdu. Tehtävässä saatuja tietoja ei saa käyttää hyväkseen missään muussa toiminnassa.
- Salassa pidettävän tai arkaluonteisen tietoaineiston käsittelyssä tulee noudattaa erityistä huolellisuutta eikä sellaista saa luovuttaa eteenpäin. Tällainen aineisto tulee tuhota tietoturvallisesti heti, kun sitä ei enää tarvita.
- Luottamustehtävän päättyessä tulee tuhota tai palauttaa kaikki käyttöön saadut tietoaineistot ja niistä tehdyt kopiot.

4. Seuraamukset

- Tietojen oikeudettomasta käytöstä voi seurata rikos- ja vahingonkorvausoikeudellisia seuraamuksia.

Tätä tietoturva-, tietosuoja- ja salassapito-ohjetta tulee noudattaa. Lisäksi tulee noudattaa tietoturvaa, tietosuojaa ja salassapitoa koskevia lakeja, asetuksia ja muita säännöksiä sekä kaupungin antamia määräyksiä ja ohjeita, jotka koskevat tietoturvaa, tietosuojaa ja salassapitoa.

Grankulla stads anvisning om datasäkerhet, dataskydd och sekretess för förtroendevalda

Den här anvisningen gäller den utrustning som en förtroendevald använder i sina förtroendeuppdrag.

1. Datasäkerhet

- Apparater och informationssystem
 - Som förtroendevald ansvarar du för dina arbetsstationer och andra apparater som du använder i dina förtroendeuppdrag.
 - De data som du fått i ditt förtroendeuppdrag ska du behandla omsorgsfullt och enligt eventuella ytterligare anvisningar.
 - Logga ut ur stadens informationssystem och se till att låsa utrustningen när du inte använder den.
 - Meddela omedelbart till adressen paatosvalmistelu@kauniainen.fi om du upptäcker missbruk av informationssystemen.
 - Var försiktig om du får okända eller misstänkta meddelanden eller länkar i stadens informationstekniska miljö.
 - Om du misstänker att arbetsstationen som du använder har ett sabotageprogram ska du sluta arbeta på arbetsstationen i fråga och omedelbart anmäla saken till adressen paatosvalmistelu@kauniainen.fi.
 - Det är obligatoriskt att genomföra den utbildning i dataskydd och datasäkerhet som staden erbjuder.
- E-post och användarnamn
 - I ditt förtroendeuppdrag ska du använda e-postadressen och användarnamnet grankulla.fi.
 - Det är inte tillåtet att skapa omdirigering av meddelanden från stadens e-post till andra e-postadresser.
 - Vid inloggningen till stadens system används tvåstegsautentisering.
 - Använd arbetsstationer och informationssystem med ditt eget användarnamn och lösenord.
 - Förvara personliga identifieringsuppgifter omsorgsfullt. Förvara inte användarnamn eller lösenord till exempel i plånboken eller handväskan.
 - Överlåt inte ditt användarnamn eller lösenord till någon annan.
 - Det är inte tillåtet att använda samma användarnamn eller lösenord i andra system eller tjänster.
 - Som förtroendevald ansvarar du för anteckningar som har gjorts med ditt användarnamn och för annan användning som hänför sig till ditt användarnamn.
 - Loggdata samlas in om användningen med ditt användarnamn. Loggdata betyder dokumenterad information om någon händelse i system, nätverk och andra miljöer eller i verksamheten vid en viss tidpunkt.
- Användning utomlands
 - Om du använder stadens e-post eller möteshanteringssystem utomlands eller om det geografiska läget (på basis av IP-adressen) visar att arbetsstationen du använder på grund av VPN eller någon annan orsak finns utomlands, orsakar det här automatiska datasäkerhetslarm hos staden. De här larmen kan leda till ytterligare utredningar och eventuella kostnader för staden. Användning av stadens system utomlands ses som en avvikelse och för att säkerställa datasäkerheten förhåller sig staden kritiskt till sådant.
 - För att kunna förutse sådana här situationer och minimera onödiga larm och anslutande kostnader informerar staden serviceproducenten på förhand de förtroendevaldas namn som kommer att använda stadens e-post och möteshanteringssystem under sitt förtroendeuppdrag.

2. Dataskydd

- Behandling av personuppgifter
 - Det är endast tillåtet att behandla sådana personuppgifter, vars behandling ingår i förtroendeuppdraget. Personuppgifter är alla sådana uppgifter utifrån vilka en person kan identifieras direkt eller indirekt, till exempel namn, personbeteckning, hemadress, e-postadress, telefonnummer, personkortets nummer, bilens registernummer, mobiltelefonens positionsinformation och IP-adress.
 - Behandling av personuppgifter betyder åtgärder beträffande personuppgifter antingen i informationssystem eller manuellt, såsom insamling, lagring, bearbetning eller radering. Att söka och se på personuppgifter räknas som behandling av dem.
 - Det är tillåtet att behandla personuppgifter som hänför sig till förtroendeuppdraget endast för det ändamål för vilket de har samlats in och endast i den mån det är nödvändigt med tanke på utförandet av arbetet.
- Personuppgiftsincident
 - Meddela omedelbart till adressen paatosvalmistelu@kauniainen.fi om du upptäcker en personuppgiftsincident som hänför sig till förtroendeuppdraget.
 - Personuppgiftsincidenter är exempelvis att skicka uppgifter till fel person, ett försvunnet papper med personuppgifter, att se på personuppgifter som inte hör till det egna förtroendeuppdraget, användarrättigheter som definierats på fel sätt eller intrång i ett system som innehåller personuppgifter. Till följd av en personuppgiftsincident förstörs, förloras eller ändras personuppgifter. Det kan också innebära att en utomstående part får tillgång till personuppgifter. En utomstående part kan också vara en förtroendevald som inte har rättigheter att behandla uppgifterna.

3. Sekretess

- Det är inte tillåtet att under förtroendeuppdraget och efter att det har upphört, röja för en utomstående sådana sekretessbelagda uppgifter som hänför sig till uppdraget, staden och dess anställda, kunder, avtalspartner eller andra samarbetspartner, till exempel affärs- eller yrkeshemligheter eller uppgifter som gäller en persons familjeliv eller andra personliga omständigheter, om inte något annat följer av lagstiftningen eller av samtycke som vederbörande har gett. Det är inte tillåtet att utnyttja sådana uppgifter som du har fått tillgång till under förtroendeuppdraget i någon annan verksamhet.
- Iakttäta särskild omsorg vid behandlingen av sekretessbelagda eller känsliga uppgifter och överlåt dem inte till någon annan. Radera sådant material på ett datasäkert sätt så snart du inte längre behöver det.
- När förtroendeuppdraget upphör ska du förstöra eller lämna tillbaka alla data som du har fått tillgång till och alla kopior av dem, till staden.

4. Påföljder

- Obehörig användning av uppgifter kan ha straff- och skadeståndsrättsliga påföljder.

Följ den här anvisningen om datasäkerhet, dataskydd och sekretess. Dessutom ska du följa lagar, förordningar och andra bestämmelser som gäller datasäkerhet, dataskydd och sekretess samt stadens bestämmelser och anvisningar som gäller datasäkerhet, dataskydd och sekretess.