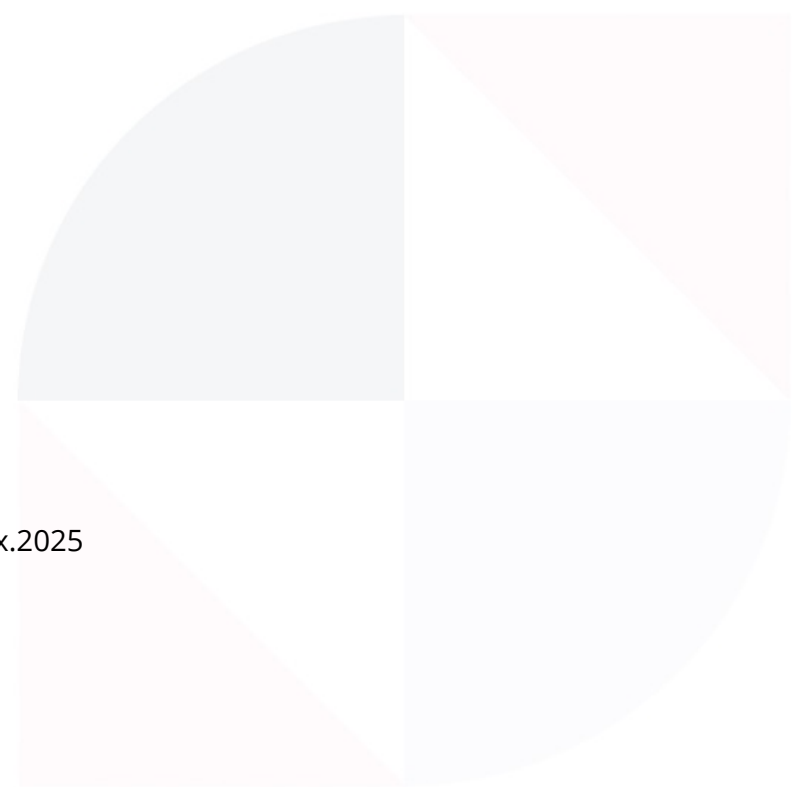


SASKY koulutuskuntayhtymä
Tiedonhallinnan, tietoturvan ja tietosuojan raportti
(tietotilinpäättö)

Hyväksytty yhtymähallituksessa x.x.2025



Sisältö

1	Tietotilinpäättöksen tarkoitus	3
2	Tiedonhallinnan, tietoturvallisuuden ja tietosuojan toteuttaminen	3
2.1	Tietosuojavastaava	4
2.2	Tietoturvan vastuuhenkilö	5
2.3	Tietoturva- ja tietosuoja-asioiden perehdytys ja ohjeistus	5
2.4	Henkilötietojen käsittely ja käsittelystä tiedottaminen	5
3	Tiedonhallinta ja asiakirjajulkisuus	6
4	Seuranta ja mittaaminen	7
4.1	Henkilörekistereihin kohdistuvat tietopyynnot	7
4.2	Tietoturvaloukkaukset ja -poikkeamat	7
4.3	Ilmoituskanava	8
5	Arviointi ja kehittäminen	9
5.1	Tiedonohjaussuunnitelma ja tiedonhallintamalli	9
5.2	Riskienhallinta ja arviointi	9
5.3	Tietoturvan ja tietosuojan arviointi	10
5.4	Kehittäminen	10

1 Tietotilinpäätöksen tarkoitus

Asiakirjassa Tiedonhallinnan vastuut sekä tietoturva- ja tietosuojapolitiikka linjataan tiedonhallinnan, tietoturvan ja tietosuojan keskeiset tehtävät ja niihin liittyvät vastuut SASKY koulutuskuntayhtymässä (Sasky). Tämä tilinpäätös kuvaa, miten linjauksen mukaiset toimijoiden vastuut ja tehdyt toimenpiteet ovat toteutuneet sekä raportoidaan mahdolliset tapahtumat ja päätettyjen kehittämiskohteiden eteneminen. Tietotilinpäätöksellä vastataan myös EU:n Yleisen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, rekisterinpitäjän vastuu).

Tietotilinpäätöksen laatimisesta on vastannut hallintojohtaja, tietosuojavastaava ja tietohallintopäällikkö. Tietotilinpäätös laaditaan kerran vuodessa keväällä.

2 Tiedonhallinnan, tietoturvallisuuden ja tietosuojan toteuttaminen

Saskyn tiedonhallinta on tiedon keräämistä, organisointia ja tallentamista niin, että tieto saadaan käyttöön tarkoituksenmukaisesti ja hallitusti. Lisäksi tiedonhallinnan sekä tietoturvan ja tietosuojan onnistunut toteuttaminen edellyttää poikkihallinnollista yhteistyötä kuntayhtymän eri tulosalueiden sekä muiden toimijoiden ja yhteistyötahojen kesken. Myös kuntayhtymälle palveluita tuottavien yritysten ja muiden kuntayhtymäorganisaation lukuun toimivien on sitouduttava sopimuksin noudattamaan kuntayhtymän tiedonhallintaan liittyviä ohjeita sekä tietoturva- ja tietosuoja vaatimuksia. Jokaisen on tunnettava vastuunsa tiedonhallinta-, tietoturva- ja tietosuojatyössä. Toiminnan läpinäkyvyys ja viestintä ovat myös tiedonhallinnassa välttämättömiä toimintatapoja.

Yhtymähallituksella on

1. vastuu tiedonhallintalain mukaisten kuvausten koostamisesta ja ylläpidosta (tiedonhallintamalli, muutosvaikutusten arviointi ja asiakirjajulkisuutta koskeva kuvaus),
2. vastuu tietoaaineistojen sähköiseen muotoon muuttamisesta ja saatavuudesta,
3. vastuu tietoturvallisuusjärjestelyistä, tietojärjestelmien toiminnasta ja yhteentoimivuudesta sekä tietovarantojen yhteentoimivuudesta
4. vastuu asianhallinnan ja palvelujen tiedonhallinnan järjestämisestä sekä tietoaaineistojen säilyttämisen järjestämisestä.

Hallintojohtaja toimii asiakirjahallinnon johtavana viranhaltijana. Hallintojohtaja johtaa yhtymähallituksen alaisena asiakirjahallintoa ja vastaa kuntayhtymän pysyvästi säilytettävistä asiakirjatiedoista sekä

1. vastaa yhtymähallituksen asiakirjahallinnon viranomaistehtävien valmistelusta ja täytäntöönpanosta,
2. ohjaa ja kehittää asiakirjahallintoa osana kuntayhtymän tiedonhallintaa,
3. hyväksyy tiedonkäsittelyn, säilytyksen ja arkistoinnin ohjeistuksen,
4. vastaa keskusarkistosta ja pysyvästi säilytettävistä asiakirjatiedoista,
5. laatii kuntayhtymän asiakirjahallinnon ohjeen ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä
6. huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta.

2.1 Tietosuojavastaava

Saskyn tietosuojavastaava on nimetty. Tietosuojavastaava on riippumaton asiantuntija, joka tukee henkilöstöä henkilötietojen asianmukaisessa käsittelyssä.

Tietosuojavastaava seuraa ja valvoo tietosuojalainsäädännön ja tietosuojaa koskevien tiedonhallintalain periaatteiden noudattamista ja raportoi päätöksentekijöille ja operatiiviselle johdolle sekä tarvittaessa tietosuojaviranomaiselle tietoonsa tulleista poikkeamista. Tietosuojavastaava toimii yhteyshenkilönä kansalliseen tietosuojan valvontaviranomaiseen ja kansalaisiin päin. Tietosuojavastaava osallistuu pyydettyäessä

tietosuojaan vaikutusten arviointiin ja valvoo arviointien toteutusta. Tietosuojavastaava osallistuu tietoturva- ja tietosuojatyöryhmän sekä tiedonhallintatyöryhmän työhön.

2.2 Tietoturvan vastuuhenkilö

Tietohallintopäällikkö toimii hallintojohtajan alaisuudessa tietoturvan vastuuhenkilönä ja vastaa tietoturvaan liittyvien asioiden kehittämisestä, ohjeistamisesta, tiedottamisesta sekä toteutuksen seurannasta yhteistyössä tietosuojavastaavan sekä tietoturva- ja tietosuojatyöryhmän kanssa. Tietoturvan vastuuhenkilö vastaa tietoturvaohjeistuksen laatimisesta ja päivittämisestä yhteistyössä tietoturva- ja tietosuojatyöryhmän kanssa. Tietoturvan vastuuhenkilö tukee tietoturvariskien ja -vaatimusten huomioimisessa tietojärjestelmiä kehitettäessä ja hankittaessa. Lisäksi tietoturvan vastuuhenkilö tukee tietohallintoa tavoitteiden toteuttamisessa, ICT-riskienhallinnassa ja tietoturvan tilannekuvan raportoimisessa. Tietoturvan vastuuhenkilö vastaa tietoturvaan liittyvien poikkeustilanteiden tutkinnasta ja hallinnasta ICT-jatkuvuussuunnitelman mukaisesti. Tietoturvan vastuuhenkilö osallistuu tietoturva- ja tietosuojatyöryhmän sekä tiedonhallintatyöryhmän työhön.

2.3 Tietoturva- ja tietosuoja-asioiden perehdytys ja ohjeistus

Henkilöstöä perehdytetään säännöllisesti tietoturvallisuuden huomioimiseen omassa työssään. Henkilöstöä informoidaan tarvittaessa tietoturvaa uhkaavista tilanteista. Henkilöstö osallistuu säännöllisesti tietosuojakoulutukseen, joka toteutetaan sähköisellä alustalla suoritettavana koulutuksena ja testinä. Uudet palkattavat henkilöt suorittavat testin osana perehdyttämistä. Testin hyväksytysti suorittaminen on pakollista. Tietoturva- ja tietosuojaohjeistus on tallennettu intranetiin. Esihenkilö vastaa ja valvoo, että henkilöstö noudattaa tietoturvaan ja tietosuojaan liittyvää ohjeistusta. Opetushenkilöstö ohjaa ja neuvoo opiskelijoita sähköisten välineiden ja palveluiden turvallisessa käytössä.

2.4 Henkilötietojen käsittely ja käsittelystä tiedottaminen

Henkilötietojen käsittely on suunniteltua ja käsittelystä informoidaan rekisteröityjä. Henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja

rekisteröityjen oikeudet. Tietosuojaselosteet julkaistaan verkkosivuilla, jossa ne toimivat asiakkaiden informaatioasiakirjoina ([Tietosuoja | SASKY koulutuskuntayhtymä](#)). Selosteissa on ilmoitettu kunkin rekisterin vastuuhenkilöt. Rekisteröidyt voivat ottaa oikeuksiinsa liittyvissä asioissa yhteyttä tietosuojavastaavaan ja tarvittaessa myös tietosuojavaltuutetun toimistoon. Jos rekisterissä käsitellään ainoastaan henkilöstön henkilötietoja, käsittelystä tiedotetaan intranetissa.

3 Tiedonhallinta ja asiakirjajulkisuus

Tiedonhallintalaki (laki julkisen hallinnon tiedonhallinnasta 906/2019) määrittää kuvaus- ja dokumentointivelvoitteet. Saskyn tiedonhallintamalli on sisäinen määräys siitä, miten tiedonhallinta ja tietojenkäsittely on toteutettava tiedonhallintamallin mukaisesti käsiteltäessä tietoaaineistoja.

Tiedonhallintamalli auttaa:

1. hallitsemaan jatkuvasti lisääntyvän tietomäärän
2. hahmottamaan ja hallitsemaan tiedon elinkaarta
3. tunnistamaan ja hallitsemaan myös uusien digitaalisten palvelujen käyttämiseen liittyviä riskejä

Tiedonhallintamallissa on lain mukaiset toimenpiteet aikataulutettu ja vastuut määritetty.

Saskyn asiakirjajulkisuuskuvaukset on julkaistu verkkosivuilla ([Toimintaa ohjaavat asiakirjat | SASKY koulutuskuntayhtymä](#)). Asiakirjajulkisuuskuvauksen tarkoituksena on antaa yleiskuvaus siitä, miten koulutuskuntayhtymän asiarekisteri sekä palvelujen tiedonhallinta ovat jäsenyneet. Tietoaaineistojen kuvausten yhteydessä on esimerkinomaisesti lueteltu hakutekijöitä, joilla tietoja voidaan hakea tietovarannon sisältämistä tietojärjestelmistä tai arkistoista. Asiakirjajulkisuuskuvaukset sisältää myös kuntayhtymätasoisien ohjeistuksen siitä, miten tietoja voidaan pyytää.

4 Seuranta ja mittaaminen

4.1 Henkilörekistereihin kohdistuvat tietopyynnöt

Saapuneet tietopyynnöt kirjataan asianhallintajärjestelmään. Vuonna 2024 ei ole tullut henkilörekistereihin kohdistuvaa tietopyyntöä.

4.2 Tietoturvaloukkaukset ja -poikkeamat

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Kaikki tietoturvaloukkaukset dokumentoidaan ja niiden käsittelylle on toimintaohjeet. Tapaus arvioidaan Tietosuojavaltuutetun toimiston ohjeiden mukaisesti. Arvioinnin perusteella todetaan, millainen riski tietoturvaloukkauksesta on aiheutunut vuodon kohteena olevan henkilön oikeuksille ja vapauksille. Jos ilmoituskynnys täyttyy, henkilötietojen tietoturvaloukkauksesta ilmoitetaan valvontaviranomaiselle 72 tunnin kuluessa. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava myös rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittamisesta päättää arvioinnin tuloksen perusteella hallintojohtaja.

Vuonna 2024 on havaittu yksittäisiin henkilöihin kohdistuvia henkilötietojen käsittelyn tietoturvaloukkauksia, jotka eivät ole kuitenkaan aiheuttaneet korkeaa riskiä henkilön oikeuksille tai vapauksille. Sasky koulutuskuntayhtymän henkilötietojen käsittelystä on tehty yksi ilmoitus Tietosuojavaltuutetun toimistolle, johon on annettu vastineen. Opiskelijahallintojärjestelmään kohdistui tietomurto, joka koski alle kymmenen rekisteröidyn tietoa. Tapauksesta on tehty sekä ilmoitus Tietosuojavaltuutetun toimistolle että rikosilmoitus. Lisävahingot saatiin estettyä yhteistyössä järjestelmän toimittajan kanssa.

Tietoturvapoikkeama tarkoittaa tahallista tai tahatonta tapahtumaa, jonka seurauksena organisaation vastuulla olevien tietojen tai palveluiden eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyytaso on tai saattaa olla

vaarantunut. Näin voi tapahtua esimerkiksi tietojenkalastelun, tietomurron tai palvelunestohyökkäyksen yhteydessä.

Vuonna 2024 ei ollut yhtään kriittistä tietoturvapoikkeamaa. SASKY koulutuskuntayhtymän tietojärjestelmäympäristöön kohdistuu jatkuvasti erilaisia hyökkäysyrityksiä. Toimintaympäristöämme kohtaan hyökättiin vuonna 2024 esimerkiksi tietojenkalastelulla sekä tunnusten kalastelulla. Rikolliset lähettivät huijausviestejä ja -sähköposteja, jolla pyrkivät saamaan haltuunsa arkaluonteisia tietoja tai antamaan käyttäjätunnukset hyökkääjille. Henkilökunnan sähköpostilaatikoihin ulkoisista osoitteista tulevasta postimäärästä noin kymmenen prosenttia oli roskapostiksi automaattisesti luokiteltavaa postia. Automaattiset tietoturvamekanismit tunnistivat ja torjuivat vuonna 2024 saapuneesta sähköpostista satoja vaarallisia ja haitallisia viestejä roskapostin lisäksi.

Digitaalisen toimintaympäristömme tietojärjestelmiin kohdistunut ulkopuolisten hyökkääjien aktiviteettitaso pysyi myös vuonna 2024 korkeana. Kyberuhkien nopea tunnistaminen ja näiden torjunta vaati ja tulee vaatimaan edelleen aktiivista seuranta, nopeaa reagoitua ja vahvaa varautumista. Erittäin tärkeänä osana tietoturvan toteutumista on elinkaarimallin noudattaminen kaikessa digitaalisessa toiminnassa. Tietoverkkoihin ja tietojärjestelmiin kytkettävät sekä asennettavat komponentit otetaan hallitusti käyttöön. Lisäksi järjestelmien koko elinkaaren ajalle on suunniteltu ja resursoitu ylläpito myös tietoturvan kannalta. Tietojärjestelmille määritellään vähintään järjestelmän omistaja, sisällöllinen pääkäyttäjä sekä tekninen pääkäyttäjä.

4.3 Ilmoituskanava

SASKY:ssa on käytössä väärinkäytösilmoituskanava (whistleblowing). Ilmoittajasta ei tallenneta IP-osoitetta tai mitään muitakaan yksilöintitietoja järjestelmään. Järjestelmässä on kattavat tietoturva- ja tietosuojakontrollit luottamuksellisuuden takaamiseksi. Jokaisesta ilmoituksesta tehdään ratkaisu kolmen kuukauden kuluessa, jos se on mahdollista. Käsittelijät antavat ratkaisun tiedoksi ilmoittajalle, kun käsittely on saatu päätökseen.

Vuonna 2024 ilmoituskanavan kautta on tullut yksi varsinaisesti kanavaan kuuluva ilmoitus. Väärinkäytösilmoituksen mukainen asia on viety päätökseen. Muihin esiin nostettuihin epäkohtiin on puututtu.

5 Arviointi ja kehittäminen

Henkilötietojen käsittelyssä noudatetaan hyvää tiedonhallintatapaa ja toimintatapoja arvioidaan ja kehitetään arviointien perusteella edelleen.

5.1 Tiedonohjaussuunnitelma ja tiedonhallintamalli

Tiedonohjaussuunnitelmaa päivitetään säännöllisesti. Sähköisen tiedonhallintamallin rakentaminen aloitettiin kuluneena vuonna. Malliin kuvataan toimintaprosessit, tietovarannot, tietoaineistot ja tietojärjestelmät. Kuvausten valmistuttua järjestelmästä voidaan muodostaa ajantasaisia, vaatimusten mukaisia dokumentaatioita ja raportteja.

5.2 Riskienhallinta ja arviointi

Tietoturvan ja tietosuojan riskienarviointi tehdään tarvittaessa ja koko toiminta arvioidaan vähintään kerran vuodessa. Arvioinnissa määritetään riskin taso ja hallintatoimenpiteet. Riskienarviointiin liittyy myös sisäisen valvonnan ja riskienhallinnan kysely henkilöstölle ja yhtymähallitukselle.

Seuraukseltaan ja todennäköisyydeltään korkeimpia tietohallinnon tunnistettuja riskejä (riskitaso = 8-12 (todennäköisyys * seuraus)) on arvioitu olevan henkilöstöön liittyvät riskit, henkilöstövaje ja osaamisvaje.

Seuraukseltaan ja todennäköisyydeltään korkeimpia tietosuojariskejä (riskitaso = 8-12 on arvioitu olevan kaksi kappaletta:

1. Kerätään ylimääräistä tietoa.
2. Väliaikaisesti säilytettävien henkilötietojen säilytys

Riskeille on määritetty hallintatoimienpiteet riskin pienentämiseksi.

5.3 Tietoturvan ja tietosuojan arviointi

Itsearviointinnissa arvioidaan tietosuojan hallinnan nykytilaa. Aihealueina ovat ne vaatimukset, jotka tietosuoja-asetuksen ja hyvien käytäntöjen mukaisen tietosuojan hallinnan ja henkilötietojen käsittelyn tulee täyttää. Vaatimukset jakautuvat tietosuojan hallintaa sekä tiedon elinkaarta ja prosesseja koskeviin vaatimuksiin. Tietoturvan osalta arvioidaan tiedon suojaamisen menettelyihin ja tekniikkaan liittyviä aihealueita, jotka ovat keskeisiä henkilötietojen suojaamisen kannalta. Toiminta on kehittynyt parempaan suuntaan kehitettäväksi päätettyjen kokonaisuuksien osalta. Asetuksen mukaisessa toimintatavassa on kehitettävää joissain toiminnoissa, kuten henkilötiedon elinkaaren hallinnassa ja joiltain osin järjestelmien kuvauksissa tai muussa dokumentaatiossa.

Rakenteilla on sähköinen alusta, joka auttaa tietosuojakäytänteiden, tiedonhallinta- ja julkisuuslain vaateiden seurantaan ja toimien kehittämiskohteiden valintaa sekä helpottaa raportointia. Käytössä on myös palvelu, joka auttaa arvioimaan sitä, toteutuuko tietosuoja-asetuksen vaatimukset kyseisten sovellusten, ohjelmistojen ja sähköisten palveluiden osalta. Palvelussa arvioidaan kaikki jo käytössä olevat sekä uudet ohjelmistot ja palvelut, ja se on osa Saskyssa tehtävää kokonaisarviota. Kokonaisarvioon kuuluvat tietoturvan ja tietosuojan lisäksi pedagoginen soveltuvuus ja/tai hallinnollisen käytettävyyden arviointi.

5.4 Kehittäminen

Toimintoja kehitetään arviointien ja tietoturva- ja tietosuojatyöryhmän esittämän vuosittaisen kehittämissuunnitelman avulla. Keskeiset kehittämistoimet ovat:

1. Henkilöstön perehdytys ja koulutus, mm. materiaalien ajantasaisuuden varmistaminen ja kehittäminen.
2. Vaikutustenarviointien tekeminen kriittisille järjestelmille.
3. Asiakirjajulkisuuskuvauksen ja tietosuoja-asetusten julkaisu tiedonhallinnan sähköisen alustan (Digiturvamalli) kautta.

Lisäksi tietoturva- ja tietosuojaryhmä osallistui 14.11.2024 Digi- ja väestötietoviraston järjestämään TAISTO 2024 -harjoitukseen, joka on Suomen suurin digitaalisen

turvallisuuden harjoitus. Harjoitus tarjosi turvallisen tilaisuuden harjoitella, testata ja kehittää organisaation digiturvan toimintamalleja kuvitteellisten häiriötilanteiden kautta. Harjoituksessa esiin nousseita havaintoja on käsitelty organisaation tietoturva- ja tietosuojaryhmässä osana tietosuojaan- ja -turvaan liittyvien prosessien ja toimintamallien kehittämistä.