Valtiontalouden tarkastusviraston toimintakäsikirja

Tietoturvapolitiikka 2014 - 2020

Sisällys

Valtiontalouden tarkastusviraston tietoturvapolitiikka

VTV2020 strategian valmistelun yhteydessä tarkastusvirasto on valmistellut toimintapolitiikat, joiden tehtävänä on tukea strategian toimeenpanoa ja työyhteisön kehittymistä. Tietoturvapolitiikalla tarkoitetaan niitä tarkastusviraston vahvistamia tietoturvallisuuden yleisiä perusteita, tavoitteita ja toimia, joilla tarkastusvirasto ja sen henkilökunta toteuttavat hyvää tietoturvallisuutta. Tietoturvapolitiikkaa täydentää viraston antama määräys tietoturvallisuudesta. Lisäksi tietoturvapolitiikan toteuttamista ohjaavat tarkastusviraston arvot ja niitä täydentävät toimintaperiaatteet.

Valtiontalouden tarkastusvirasto on, yhteistoimintakokouksen ja viraston johtoryhmän sekä laajennetun johtoryhmän puollettua tietoturvapolitiikan hyväksymistä, päättänyt vahvistaa osaksi tarkastusviraston toimintakäsikirjaa tietoturvapolitiikan vuosille 2014–2020.

Helsingissä 4 päivänä maaliskuuta 2015

Pääjohtaja Tuomas Pöysti

Ylijohtaja Tytti Yli-Viikari

JAKELU

VTV henkilöstö

TIEDOKSI

Eduskunnan tietohallintotoimisto

1 Johdanto

Tietoturvallisuudella tarkoitetaan tietojen, tietojärjestelmien ja niiden palveluiden luottamuksellisuuden, eheyden, saatavuuden ja käytettävyyden suojaamista siten, että niihin kohdistuvat uhat eivät aiheuta merkittävää vahinkoa tarkastusviraston toiminnoille. Tarkastusviraston toiminnoissa on otettava huomioon säännöksissä, määräyksissä sekä ohjeissa olevat velvoitteet ja vaatimukset, jotka ovat keskeisiä kriteereitä tietoturvatoimenpiteiden laadun arvioimisessa.

Valtiontalouden tarkastusvirasto tuottaa eduskunnalle, valtioneuvostolle ja sen alaiselle hallinnolle hyödyllistä ja luotettavaa valvonta- ja tarkastustietoa. Tarkastusvirastolla on perustuslaissa säädetty oikeus saada viranomaisilta ja muilta valvontansa kohteina olevilta tehtävänsä hoitamiseksi tarvitsemansa tiedot. Osa näistä tiedoista voi olla salassa pidettäviä tai arkaluonteisia.

Tarkastusviraston tietoturvavelvoitteet perustuvat viranomaisten toiminnan julkisuudesta annetun lain (621/1999) sekä henkilötietolain (533/1999) säännöksiin. Valtiontalouden tarkastusviraston tietoturvapolitiikassa (220/01/2014) määritellään tietoturvallisuuden yhteys viraston strategisiin tavoitteisiin, tietoturvallisuuden tavoitteet, strategiset painopistealueet, vastuut, turvaamisperiaatteet ja tiedottaminen tarkastusvirastossa. Tietoturvapolitiikkaa täydentää määräys tarkastusvirastossa noudatettavasta tietoturvallisuudesta (169/01/2014). Se sisältää tarkemmat määräykset tietoturvallisuuden hallintajärjestelmästä, hallinnollisesta turvallisuudesta, henkilöstöturvallisuudesta, tietoaineistoturvallisuudesta, fyysisestä turvallisuudesta, tietoteknisestä turvallisuudesta sekä toiminnasta poikkeustilanteissa. Tietoturvallisuuden muut osa-alueet on ohjeistettu tietotekniikan tietoturvaohjeessa. Tietoturvamääräystä täydentävät tarkastusviraston omat ohjeet sekä eduskunnan tietoturvamääräykset ja -ohjeet. Tarkastusviraston tietoturvaohjeistusta laadittaessa huomioidaan soveltuvin osin valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) antama ohjeet.

2 Vastuut

2.1 Tarkastusviraston tietoturvavastuut

Pääjohtaja vastaa tietoturvapolitiikan yleisistä linjauksista ja kehittämisestä. Tarkastusvirastossa noudatettava tietoturvapolitiikka ja määräys tietoturvallisuudesta tarkastusvirastossa ovat pääjohtajan hyväksymiä. Tarkastusviraston ylin johto vastaa tietoturvallisuuden huomioonottamisesta viraston strategisissa tavoitteissa. TL:n, TF:n, FV:n, JT:n ja HY:n päälliköt vastaavat oman toimintansa osalta tietoturvapolitiikan huomioon ottamisesta, toteuttamisesta sekä kehittämisestä toiminnassaan. Hallintoyksikkö tuottaa, ylläpitää ja kehittää tietoturvallisuuden prosesseja ja palveluita sekä tukee organisaatiota tietoturvapolitiikan toteuttamisessa. Hallintoyksikön päällikkö vastaa tietoturvapolitiikan yleisestä valmistelusta ja toimeenpanosta sekä raportoinnista. ICT-ryhmä antaa tarvittaessa lisäohjeita ja tekee muutosehdotuksia.

Tarkastusviraston henkilöstöllä on merkittävä rooli ja tehtävä tietoturvapolitiikan käytännön toteuttamisesta ja oman osaamisensa ylläpitämisessä ja kehittämisessä. Esimiesten tehtävänä on huolehtia henkilöstön riittävästä perehdyttämisestä viraston tietoturvallisuutta koskeviin ohjeisiin ja määräyksiin sekä valvottava niiden noudattamista.

2.2 Yhteistyökumppaneiden vastuut

Valtiontalouden tarkastusvirasto käyttää monia eduskunnan hankkimia ja ylläpitämiä ICT-järjestelmiä. Näiden järjestelmien osalta järjestelmien kehitys- huolto- ja ylläpitovastuu on eduskunnalla. Virasto vastaa omien tietojen ylläpidosta näillä järjestelmillä. Eduskunnan järjestelmien osalta noudatetaan tarkastusviraston omien määräysten lisäksi eduskunnan antamia määräyksiä sekä eduskunnan sisäisiä tietoturvakäytäntöjä. Ulkoistettujen palvelujen toimittajien on noudatettava soveltuvin osin tarkastusviraston tietoturvaohjeita ja -määräyksiä ja ne on otettava huomioon sopimuksia tehtäessä.

3 Nykytilan kuvaus

Tietoturvallisuuden tavoitteena on huolehtia siitä, että tarkastusviraston tarkastuskohteilta saatuja ja omassa toiminnassa syntyneitä tietoaineistoja käsitellään koko elinkaaren ajan säännösten, määräysten ja ohjeiden mukaisesti. Tarkastusviraston henkilöstön velvollisuutena on huolehtia omassa työssään tietoturvallisuuden riittävästä ja asianmukaisesta toteuttamisesta sekä kiinnittää huomiota tietoaineistoihin ja tietojärjestelmiin kohdistuviin uhkiin. Jokaisen velvollisuutena on tuoda esiin tietoturvallisuuteen kohdistuvat riskit suunnitelmissa ja ohjeissa kuvatuilla tavoilla.

3.1 Tietoturvatoimintaa ohjaavat tekijät

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:ssä säädetään viranomaiselle toisaalta velvollisuudesta huolehtia siitä, että julkinen tieto on oikeaan aikaan käytettävissä ja toisaalta velvollisuudesta suojata salassa pidettävät tiedot väärinkäytöltä. Henkilötietolain (523/1999) 32 §:n mukaan rekisterinpitäjällä on velvollisuus toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Arkistolain 12 §:ssä (831/1994) säädetään arkistonmuodostajan velvollisuudesta huolehtia asiakirjojen säilytyksestä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä.

Sähköisestä asioinnista viranomaistoiminnassa annetun lain 1 §:ssä (13/2003) yhdeksi tarkoitukseksi on määritelty tietoturvallisuuden lisääminen hallinnossa, millä pyritään puolestaan mahdollistamaan sähköisten tiedonsiirtomenetelmien käyttö asiointivälineenä. Edellä olevan lain 5 §:n mukaan viranomaisten on järjestettävä tietoturvallisuus riittävälle tasolle niin kansalaisille, yrityksille kuin yhteisöillekin tarkoitetuissa sähköisissä palveluissa ja viranomaisten välisessä sähköisessä tiedonsiirrossa ja asioinnissa.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Laissa säädetään erityisesti henkilöstöturvallisuuteen liittyvistä asioista, kuten työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta.

Tarkastusviraston arkistonmuodostussuunnitelma (26/01/2014) käsittää perustiedot viraston toiminnan tuloksena syntyvien tietoaineistojen käsittelystä, rekisteröinnistä, säilytystavoista ja -muodoista, julkisuudesta sekä maininnat tietojärjestelmistä ja muista asiakirjojen käsittelyyn liittyvistä ohjeista.

3.2 Tietoturvallisuuteen kohdistuvat uhat ja riskit

Tietoturvauhat kohdistuvat sähköisiin ja paperimuotoisiin tietoaineistoihin, henkilöstöön, fyysiseen turvallisuuteen, laitteistoihin, ohjelmistoihin, tietoliikennepalveluihin ja järjestelmien käyttöön. Uhkia seurataan jatkuvasti ja niistä raportoidaan johdolle ja muille vastuuhenkilöille.

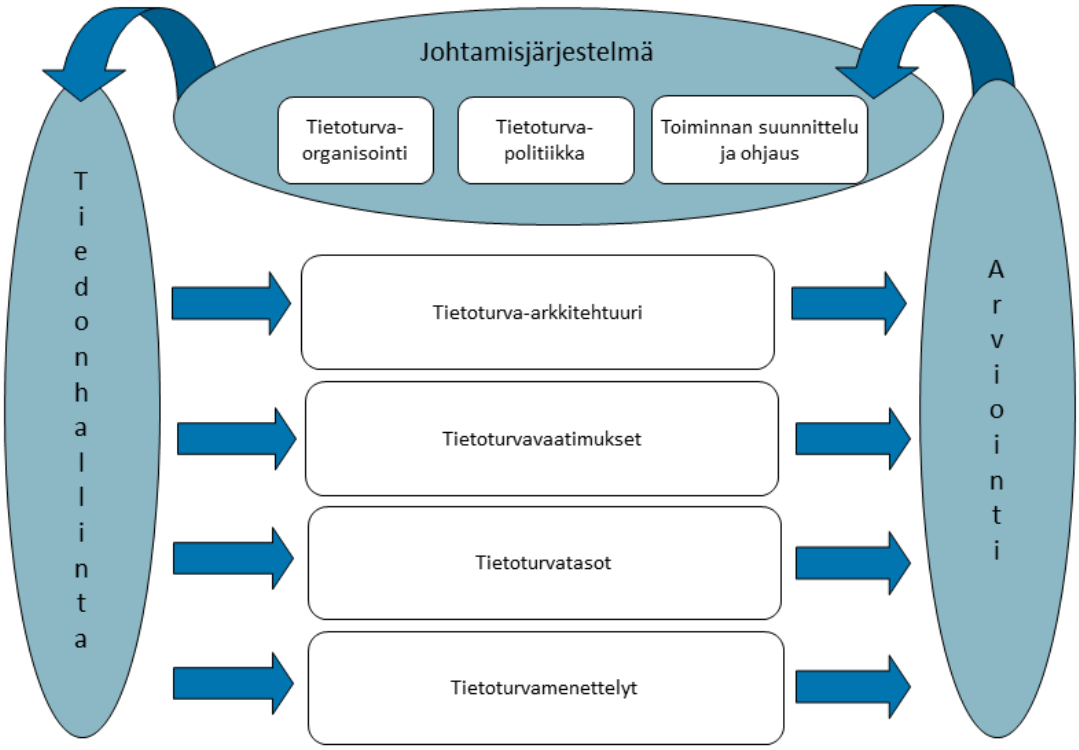
Tietoturvallisuuteen kohdistuvat uhat ja riskit arvioidaan vuosittain sisäisen valvonnan arviointi- ja vahvistuslausuman valmisteluun kuuluvana.

Tietoturvariskit kartoitetaan ja tietoturvatoimenpiteet priorisoidaan siten, että riskien toteutuminen vaikuttaa mahdollisimman vähän viraston toimintaan. Tietoturvatoimenpiteet on priorisoitu voimassa olevassa viraston tietoturvallisuuden kehityssuunnitelmassa.

3.3 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmän toteuttaminen on kuvattu tarkemmin määräyksessä tarkastusviraston tietoturvallisuudessa. Tietoturvallisuuden hallintajärjestelmää ylläpidetään lainsäädännön,

ohjeistuksen ja menettelyiden muuttuessa. Hallintajärjestelmä on kuvattu pääpiirteissään alla olevassa kuviossa ja siinä sovelletaan standardia IEC/ISO 27001: 2005.



Kuvio 1: Tietoturvallisuuden hallintajärjestelmä

3.4 Tietoturvakoulutus ja tietoturvauhkista tiedottaminen

Tietoturvallisuus on olennainen osa viraston jatkuvaa osaamisen kehittämistä, josta huolehditaan asianmukaisella ja suunnitellulla tietoturvakoulutuksella. Koulutuspakettiin perehtyminen ja siihen liittyvän tietoturvatentin suorittaminen hyväksytysti on edellytyksenä salassa pidettävien tietoaineistojen käsittelyoikeudelle. Uusille työntekijöille järjestetään perehdytys viraston tietoturvamenettelyihin ja -ohjeistukseen perehdyttämiskoulutuksen yhteydessä. Tietoturvallisuuteen liittyvien ohjeiden päivityksistä tiedotetaan aktiivisesti ja tarvittaessa järjestetään erillisiä koulutustilaisuuksia kohderyhmittäin.

Tarkastusvirastossa tietoturvallisuuteen liittyvistä uhkista ja riskeistä tiedottamisesta vastaa hallintojohtaja yhteistyössä ICT-päällikön ja tietoturvapäällikön kanssa. Tarkastusviraston kriisiviestinnässä noudatetaan viraston viestintäsuunnitelmaa.

3.5 Tietoturvallisuuden toteutumisen valvonta

Johdon ja esimiesten tehtävänä on valvoa tietoturvallisuuden toteutumista. Henkilökunnasta jokainen on velvollinen ilmoittamaan tietoturvahavainnoistaan. Tietoturvallisuuden valvontaan osallistuvat henkilökunnan lisäksi eri yhteistyötahot. Valvonnassa korostuu johdon, esimiesten, tietohallinnon ja järjestelmien vastuuhenkilöiden rooli.

Virasto voi tehdä yhteistyötahojensa kanssa sopimuksia teknisistä valvontatehtävistä. Tällöin valvonta kohdistuu erityisesti palvelimiin ja tietoliikenteeseen.

3.6 Toiminta poikkeustilanteissa ja – oloissa

Normaaliolojen palo- ja pelastustilanteissa toimitaan tarkastusviraston suojelusuunnitelman (222/06/2014) mukaisesti. Henkilökunnalle on jaettu kirjalliset toimintaohjeet uhka- ja hälytystilanteita varten. Poikkeusoloissa tarkastusvirastossa toimitaan valmiussuunnitelman (222/06/2014) mukaisesti. Asiakirjojen poikkeusolojen suojeluryhmät on määritelty arkistonmuodostussuunnitelmassa.

4 Tietoturvapolitiikan tavoitteet ja painopistealueet

Tarkastusviraston strategiset tavoitteet on määritelty 30.1.2013 hyväksytyssä asiakirjassa "Valtiontalouden tarkastusviraston strategia vuosille 2013 - 2020". Tietoturvapolitiikka tukee tarkastusviraston strategisten tavoitteiden saavuttamista.

Tarkastusviraston tietoturvallisuuden strategisena tavoitteena on se, tarkastusvirasto käsittelee käyttämiään tietoja vähintään yhtä turvallisesti kuin nämä tiedot omistavat organisaatiotkin. Tämä varmistetaan sillä, että tietoturvamme on valtionhallinnon ja soveltuvilta osin tarkastus- ja tietoturvaorganisaatioiden normien, käytäntöjen ja standardien mukaista. Niiden noudattaminen on osa jokaisen työntekijän työtä, sen vaatimaa ammattitaitoa ja vastuunkantoa. Tarkastusvirasto noudattaa vähintään eduskunnan määrittelemää tietoturvatasoa sekä lisäksi huomioidaan tarvittavilta osin ulkoiset vaatimukset tietoturvallisuuden toteuttamiseksi.

Tietoturvallisuuden kehittämistoimenpiteet tehdään tietoturvallisuuden kehityssuunnitelman mukaisesti. Kehitystyön painopistealueita ovat hyvän tiedonhallintatavan toteuttaminen kaikissa viraston toiminnoissa, henkilöstön tietoturvaosaamisen ylläpitäminen ja kehittäminen sekä sitouttaminen tietoturvalliseen toimintaan ja tietoturvaohjeisiin. Tietoturvallisuuden operatiiviset painopistealueet ovat järjestelmien käytettävyys, tiedon salaus, luotettava käyttäjän tunnistus, käyttöoikeushallinta, tietoturvakoulutuksen järjestäminen ja ohjeistus sekä ulkopuolisten hyökkäyksien torjunta, roskapostin suodattaminen ja haittaohjelmien torjunta.