VALTIOVARAINMINISTERIÖ

Julkisen hallinnon digitaalinen turvallisuus Toimeenpanosuunnitelma 2020-2023

24.01.2020
LUONNOS

VALTIOVARAINMINISTERIÖ

Sisällys

VALTIOVARAINMINISTERIÖ

JOHDANTO

Julkisen hallinnon digitaalinen turvallisuus – asiakirjassa on kuvattu hallinnon toimintaa ja prosesseja tukevat keskeiset julkisen hallinnon digitaalisen turvallisuuden palvelut. Tässä toimeenpanosuunnitelmassa on kuhunkin palveluun liittyen valittu tehtäviä julkisen hallinnon digitaalisen turvallisuuden nykytilaselvityksen ja kansainvälisen vertailun perusteella. Tehtäville on asetettu tavoitteet ja aikataulu, sekä kuvattu tavoitteiden saavuttamiseksi tarvittavat toimenpiteet, niiden toteutumisen mittaaminen sekä arvioitu kustannuksia ja hyötyjä. Toimeenpanosuunnitelma on tarkoitettu myös syötteeksi ja se tukee Suomen kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua.

Toimeenpanosuunnitelman 2020-2023 vastuutahot ovat seuraavat:

- Valtiovarainministeriö (VM)
    - Julkisen hallinnon digitaalisen turvallisuuden strateginen ohjausryhmä, puheenjohtaja alivaltiosihteeri Päivi Nerg: Valvoo toimeenpanosuunnitelman ja kuntien digitaalisen tiekartan toteuttamista
    - Julkisen hallinnon ICT-osasto, palveluiden ja turvallisuuden ohjausyksikkö: Koordinoi toimeenpanosuunnitelman toteuttamista, kilpailuttaa ja ohjaa toteutussuunnitelmassa valtiovarainministeriön tehtäviksi nimetyt selvitykset, sekä ohjaa Digi- ja väestötietoviraston JUDO-hanketta.
- Digi- ja väestötietovirasto (DVV)
    - Vahti-johtoryhmä, puheenjohtaja pääjohtaja Janne Viskari: Tuottaa tilannekuvan ja riskiarvion perustan.
    - Toteuttaa toimeenpanosuunnitelmassa DVV:lle nimetyt tehtävät pääsääntöisesti Julkisen hallinnon digitaalisen turvallisuuden (JUDO) kehittämisen hankkeessa, jolle DVV on asettanut ohjausryhmän.
- Traficom/Kyberturvallisuuskeskus
    - Toteuttaa toimeenpanosuunnitelmassa Traficomille/Kyberturvallisuuskeskukselle nimetyt tehtävät osana DVV:n JUDO-hanketta.
- Muut ministeriöt, Kuntaliitto ja kunnat
    - Yhteistyössä VM:n kanssa toteuttavat toimeenpanosuunnitelmassa kuvatut tehtävät.

VALTIOVARAINMINISTERIÖ

1 JULKISEN HALLINNON DIGITAALISEN TURVALLISUUDEN KANSALLINEN JA KANSAINVÄLINEN YHTEISTOIMINTAMALLI

Kansallisen ja kansainvälisen yhteistyön kautta tehostetaan digitaalisen turvallisuuden koordinointia ja vaikuttavuutta sekä edistetään Suomen kilpailukykyä. Ministeriöt hallinnonaloineen, kunnat ja yhteisöt vaikuttavat aktiivisesti digitaalisen turvallisuuden myönteiseen kehittymiseen Euroopan unionissa sekä keskeisissä kansainvälisissä järjestöissä kuten YK ja OECD.

1.1 Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä

Tavoite: Digitalisoitumista ja digitaalista turvallisuutta edistetään tasapainoisesti.

Vastuu: Valtiovarainministeriö

Kohde: Julkinen hallinto

Aikataulu: 2020-2024

Toimenpiteet: Valtiovarainministeriö asettaa digitaalisen turvallisuuden strategisen johtoryhmän. Ryhmään kuuluvat valtioneuvoston kanslia, ulkoministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö, sosiaali- ja terveysministeriö, työ- ja elinkeinoministeriö, Turvallisuuskomitea, Kuntaliitto, kuntien edustaja, Huoltovarmuuskeskus, yliopistojen edustaja sekä asiantuntijana Digi- ja väestötietovirasto. Ryhmä koordinoi julkisen hallinnon digitaalisen turvallisuuden strategista riskiarviota, luo ja koordinoi digitaalisen turvallisuuden yhteistoimintamallia, sekä arvioi julkisen hallinnon strategista digitaalisen turvallisuuden tilannetta, ja keskeisiä kehitettäviä digitaalisen turvallisuuden palveluja, linjaa keskeisiä digitaalisen turvallisuuden asioita kuten digitaalisen turvallisuuden tavoitteita, sekä valvoo tämän digitaalisen turvallisuuden toimeenpanosuunnitelman ja kuntien digitaalisen turvallisuuden tiekartan toteutumista.

Mittaaminen: Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä on asetettu vuonna 2020 ja toiminnassa. Strategista riskiarviota on käsitelty ja resursseja on suunnattu sen perusteella vaikuttavimpiin kehittämiskohteisiin.

Kustannus/hyöty: Julkisen hallinnon digitaalisen turvallisuuden strategisen johtoryhmän työ on virkatyötä. Ryhmän osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Ryhmä onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisen turvallisuuden keskeisten strategisten riskien ennalta ehkäisemiseen, mikä

vähentää hallinnon prosessien ja toimintojen laajoja katkoksia ja lamaantumista sekä niistä aiheutuvia haittoja yhteiskunnan toiminnan jatkuvuudelle. Vähentää mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisen keskuudessa. Ryhmän onnistunut toiminta myös edistää Suomen kilpailukykyä ja mahdollistaa innovaatioita ja kasvua.

1.2 Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli

Tavoite: Valtiovarainministeriö yhdessä muiden ministeriöiden, kuntien ja yhteisöjen kanssa toimivat julkisen hallinnon digitaalista turvallisuutta tehostavan yhteistoiminta- ja hallintamallin mukaisesti.

Vastuu: Valtiovarainministeriö

Kohde: Julkinen hallinto, kansalaiset

Aikataulu: 2021-2023

Toimenpiteet: Valtiovarainministeriö yhdessä muiden ministeriöiden, kuntien ja yhteisöjen kanssa luo ja koordinoi toiminnan ja talouden sekä osaamisen kehittämisen kattavan kansallisen strategisen tason digitaalisen turvallisuuden yhteistoimintamallin. Yhteistoimintamallin valmistelussa käsitellään valtion, kuntayhtymien ja kuntien tehtäviä ja vastuita sekä julkisen hallinnon digitaalisen turvallisuuden palveluja kansalaisille, ja tutkimusyhteistyötä. Valtiovarainministeriö ja muut ministeriöt viestivät digitaalisen turvallisuuden tavoitteista ja sisällyttävät ne julkisen hallinnon toiminnallisiin tavoitteisiin.

Mittaaminen: Yhteistoimintamalli on kuvattu ja toiminnassa. Taloussuunnitelmiin sisältyy konkreettisia, digitaalisen turvallisuuden osa-alueita parantavia tavoitteita.

Kustannus/hyöty: Yhteistoimintamallin selvitys 80 000 euroa. Toimeenpanon koordinointi on pääsääntöisesti virkatyötä. Toimeenpanon kustannukset arvioidaan tarkemmin selvitystyön yhteydessä. Hyötynä on edelleen parantuvan yhteistoiminnan mahdollistama digitaalisen turvallisuuden strategisen ja operatiivisen tason sekä osaamisen kehittäminen.

1.3 Julkisen hallinnon digitaalisen turvallisuuden kansallinen operatiivisen tason kehittäminen

Tavoite: VAHTI-johtoryhmä edistää ja kehittää koko julkisen hallinnon digitaalisen turvallisuuden toimeenpanon yhteistyötä ja koordinaatiota.

Vastuu: Digi- ja väestötietovirasto

Kohde: Julkinen hallinto, kansainvälinen yhteistyö

Aikataulu: 2020-2024

Toimenpiteet: Digi- ja väestötietovirasto asettaa VAHTI-johtoryhmän operatiivisen tason poikkihallinnolliseksi ohjausryhmäksi. Uudistetun Vahti-johtoryhmän on suunniteltu muodostuvan keskusvirastojen ja keskeisten yhteisöjen ja toimielinten johdosta. Vahti-johtoryhmä edistää kansallista ja kansainvälistä osaamisen kehittämistä. Vahti-toiminnassa hyödynnetään useiden eri viranomaisten tuottamaa digitaalisen turvallisuuden tilannekuvaa.

Mittaaminen: Julkisen hallinnon operatiivinen/VAHTI-johtoryhmä on asetettu ja toimii.

Kustannus/hyöty: Vahti-johtoryhmän työ on virkatyötä. Ryhmän osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Ryhmä onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisen turvallisuuden keskeisten operatiivisten riskien ennalta ehkäisemiseen, mikä vähentää häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia sekä mainehaittoja ja luottamuksen rapautumista niin hallinnossa, yhteisöissä kuin kansalaisen keskuudessa.

1.4 Digitaalisen turvallisuuden kansainvälisen kentän julkisen hallinnon yhteistyö

Tavoite: EU-säädösten mukaisten teknologiaratkaisujen kehittyminen, sekä riittävien digitaalisen turvallisuuden vaatimusten toteutuminen julkisen hallinnon palveluissa. Tämä myös edistää Suomen kilpailukykyä kansainvälisen yhteistyön avulla.

Vastuu: Kukin ministeriö oman vastuualueensa osalta

Kohde: Kansainvälinen yhteistyö

Aikataulu: 2021-2023

Toimenpiteet: EU-asioissa valtioneuvoston kanslian ja muissa kansainvälisissä aisoissa ulkoministeriön koordinoimana kukin ministeriö oman vastuualueensa osalta yhdessä muiden ministeriöiden kanssa edistävät EU-säädösten mukaisten teknologiaratkaisujen kehittymistä, sekä riittävien digitaalisen turvallisuuden vaatimusten toteutumista julkisen hallinnon palveluissa.

Valtiovarainministeriö käynnistää yhteistyössä muiden ministeriöiden ja toimijoiden kanssa selvitystyön kansainvälisten asioiden raportoinnin keskittämistä siten, että Suomessa yksi toimija kokoaisi yhteen ja raportoisi Suomen tiedot digitaalisen turvallisuuden kansainvälisiin arviointeihin sekä eri kansainvälisiin yhteisöihin.

Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa vahvistavat julkisen hallinnon digitaalisen turvallisuuden yhteistyötä Baltian ja Pohjoismaiden kanssa. Yhteistyö koordinoidaan ulkoministeriön ja valtioneuvoston kanslian kansainvälisten digitaalisen turvallisuuden alueen toimien kanssa.

Mittaaminen: Julkisen hallinnon kansainväliselle yhteistyölle on asetettu tavoitteet, joita seurataan. Kansainvälisille yhteisöille raportoinnin keskittäminen on suunniteltu ja sitä toteutetaan. Valtiovarainministeriön sekä Baltian ja Pohjoismaiden välinen digitaalisen turvallisuuden yhteistyö tuottaa uutta tietoa päätöksenteon tueksi.

Kustannus/hyöty: Kansainvälinen yhteistyö ja raportoinnin keskittämisen suunnittelu ovat virkatyötä. Osallistujatahot vastaavat edustajiensa matka- ja muista kustannuksista. Työ onnistuessaan vaikuttaa merkittävästi julkisen hallinnon digitaalisten palvelujen hankintamahdollisuuksiin ja tuotantomalleihin sekä palvelujen, infrastruktuurin ja tietojen turvallisuuden jatkuvaan paranemiseen, koska näitä ei ole mahdollista kehittää ainoastaan Suomessa tehtävillä toimenpiteillä.

Yhteensä kohdassa 1 selvitystyötä koskevat hankinnat 80 000 euroa.

2 JULKISEN HALLINNON DIGITAALISEN TURVALLISUUDEN RISKIEN HALLINTA

Digitaalisen turvallisuuden nykytila-arvion ja kokonaiskuvan perusteella tuotettavien riskianalyysien ja vaikutusarviointien avulla valitaan kehityskohteet, joihin suunnataan resursseja.

2.1 Julkisen hallinnon strategisen tason digitaalisen turvallisuuden riskianalyysi

Tavoite: Digitaalisen turvallisuuden nykytila-arvioon ja strategisen tason kokonaiskuvaan perustuva riskianalyysi on käytettävissä.

Vastuu: Valtiovarainministeriö, Digi- ja väestötietovirasto

Kohde: Julkinen hallinto

Aikataulu: 2020-2021

Toimenpiteet: Digi- ja väestötietovirasto selvittää ja toteuttaa prosessin ja palvelut, joiden avulla se kokoaa keskitetysti tiedon organisaatioiden digitaalisen turvallisuuden uhista, riskeistä ja kypsyystasosta, sekä jakaa digitaalisen turvallisuuden kehitystoimintaan tarvittavaa tietoa. Yhteistyötahoina ovat Traficom/Kyberturvallisuuskeskus, kunnat ja yhteisöt. Riskienhallinta auttaa organisaatioita luomaan tavan tunnistaa,

analysoida ja hallita riskien ja keskinäisriippuvuuksien vaikutusta digitaalisen turvallisuuden tavoitteiden saavuttamiseksi. Riskienhallinnan avulla riskien käsittelyyn liittyvä toiminta liitetään osaksi johtamista ja päätöksentekoa.

Valtiovarainministeriö selvittää ja toteuttaa prosessin yhdessä Digi- ja väestötietoviraston kanssa, jonka avulla se ylläpitää digitaalisen turvallisuuden pitkän aikavälin strategista riskiarviota ja laatii pitkän aikavälin linjaukset kehitystoimintaa varten. Valtiovarainministeriö koordinoi linjauksia toteuttavaa toimeenpanoohjelmaa sekä arvioi säännöllisesti linjausten toteutumista.

Mittaaminen: Kokonaiskuvaan perustuva riskiarvio on luotu, toteutettu ja saatavilla.

Kustannus/hyöty: Selvitys koskien prosesseja riskien tunnistamiseen ja ylläpitoon 80 000 euroa sekä ensimmäinen riskianalyysi strategisten digiturvallisuuden uhkien osalta arviolta 60 000 euroa. Riskienhallintatyökalun ja tilannekuvan ylläpitämiseen liittyvä järjestelmäkustannus arviolta 100 000 euroa. Toteutusten kustannukset arvioidaan tarkemmin selvityksen yhteydessä. Organisaatioiden sisäinen riskienhallinta toteutetaan virkatyönä. Hyödyt on kuvattu kohdassa 1.1.

2.2 Julkisen hallinnon digitaalisen turvallisuuden vaikuttavuus-/kustannusmalli

Tavoite: Digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arviointimallien ja menettelyjen edistäminen julkisessa hallinnossa. Digitaalisen turvallisuuden menojen kokonaismäärän selvittäminen ICT-menoihin verrattuna.

Vastuu: Valtiovarainministeriö

Kohde: Julkisen hallinnon organisaatiot

Aikataulu: 2020-2022

Toimenpiteet: Valtiovarainministeriö yhdessä digi- ja väestötietoviraston, Valtiokonttorin ja Palkeitten kanssa laatii digitaalisen turvallisuuden vaikuttavuus-/kustannusmallin ja prosessin. Suunnitellaan digitaalisen turvallisuuden hallinnan ja kehittämisen vaikuttavuuden ja kustannusten arviointi julkisessa hallinnossa. Tavoite on se, että julkisen hallinto panostaisi digitaaliseen turvallisuuteen määrärahalla joka vastaa viittä prosenttia ICT-menoista. Mallia pilotoidaan ja pilotoinnin kokemusten perusteella päivitetty malli otetaan käyttöön vuonna 2022.

Mittaaminen: Malli on luotu ja toteutettu. Vaikuttavuusarviointi on saatavilla.

Kustannus/hyöty: Selvitys koskien mallin ja prosessin laadintaa 60 000 euroa. Toteutuksena tiedonsiirron rajapintoja valtion toimijoille 50 000 euroa sekä käyttöliittymän tarjoami-

nen kunnille 50 000 euroa. Tämä arvio ei sisällä tuotantoympäristön ylläpitokustannuksia. Toteutuksen kustannukset sisältäen kunnissa tapahtuvan työn kustannukset tarkennetaan mallin ja prosessin laadinnan yhteydessä. Mallia ja prosessia tarvitaan, jotta digitaalisen turvallisuuden strateginen johtaminen voi perustua tietoon. Digitaalisen turvallisuuden strategisen johtamisen hyötyjä on käsitelty kohdassa 1.1.

Yhteensä kohdassa 2 selvitystyötä koskevat hankinnat 140 000 euroa sekä toteutusta ja ylläpitoa koskevat hankinnat yhteensä 260 000 euroa.

3 KUNNILLE TARKOITETUT YHTEISET, DIGITAALISTA TURVALLISUUTTA EDISTÄVÄT PALVELUT

Kuntien digitaalisen turvallisuuden kehittämisen tiekarttaa ylläpidetään, ja sen toteutumista seurataan.

3.1 Kuntien käytössä olevien tietoverkkojen turvallisuus

Tavoite: Kuntien havainnointi- ja reagointikyvyn kasvattaminen.

Vastuu: Valtiovarainministeriö, Kuntaliitto, kunnat

Kohde: Kunnat

Aikataulu: 2020-2022

Toimenpiteet: Valtiovarainministeriö yhdessä muiden ministeriöiden sekä digi- ja väestötietoviraston, Traficomin, Kuntaliiton ja kuntien kanssa kokoaa ryhmän selvittämään ja koordinoimaan kuntien havainnointi- ja reagointikyvyn kasvattamista. Yhtenä mahdollisena palveluna on Havaro-palvelun valmistelu kuntasektorille. Toimenpide liittyy kohtaan 8.2.

Mittaaminen: Havainnointi- ja reagointikykyä kasvattavia palveluita on kuntien käytettävissä.

Kustannus/hyöty: Selvitys 60 000 euroa. Selvityksen aikana valitaan palveluita käyttävät kunnat sekä palvelut ja arvioidaan toteutuksen kustannukset. Palvelun käyttäjät vastaavat käyttöönottoon ja palvelun käyttöön liittyvistä kuluista sekä tarvittavista lisenssimaksuista. Nopeammalla reagoinnilla turvataan kansalaisten palvelujen jatkuvuus ja turvallisuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia. Vähennetään mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisen keskuudessa.

3.2 Kuntien yhteiset digitaalisen turvallisuuden palvelut

Tavoite:	Kuntien yhteistä digitaalisen turvallisuuden kehittämisen tiekarttaa ylläpidetään ja seurataan sen toteutumista.
Vastuu:	Valtiovarainministeriö, Kuntaliitto, kunnat
Kohde:	Kunnat
Aikataulu:	2021-2023
Toimenpiteet:	Valtiovarainministeriö yhdessä muiden ministeriöiden, digi- ja väestötietoviraston, Kuntaliiton ja kuntien kanssa kokoaa työryhmän selvittämään kuntien yhteisten digitaalisen turvallisuuden kehittämishankkeiden tarvetta ja toteutusta. Selvitys perustuu tässä toimeenpanosuunnitelmassa kuvattuihin tehtäviin, jotka yhdessä muodostavat kuntien digitaalisen turvallisuuden kehittämisen tiekartan perustan. Lisäksi selvityksessä otetaan kantaa kuntien yhteisen tietoliikenneverkon tarpeeseen yhteisten digitaalisen turvallisuuden palvelujen tuottamiseksi. Selvitettäviä palveluja ovat myös esimerkiksi pilvisähköposti ja muut pilviperustaiset digitaaliset alustat sekä IoT-ympäristöt sekä digitaalisten toimintaympäristöjen valvomotoiminne (kuntien yhteinen kyber- ja tietoturvavalvomo). Valvomotoiminne olisi mahdollista toteuttaa yhteisesti saatavilla olevana valvomopalveluna ja siten, että varoitustiedot tulisivat kunnan johdon päätöksen teon tueksi. Selvitysten perusteella tarkennetaan kuntien digitaalisen turvallisuuden kehittämisen tiekarttaa.
Mittaaminen:	Työryhmä on perustettu ja selvitykset laadittu. Kuntien digitaalisen turvallisuuden tiekarttaa ylläpidetään.
Kustannus/hyöty:	Selvitys 100 000 euroa. Selvityksen aikana valitaan palveluita käyttävät kunnat sekä palvelut ja arvioidaan toteutuksen kustannukset. Valittavien palvelujen tulee olla sellaisia, joissa kaikilla tai useilla kunnilla on samanlainen palvelutarve. Jos kunnat tekevät ja selvittävät palveluja erikseen, niin julkisia voimavaroja hukkaantuu. **Yhteensä kohdassa 3 selvitystyötä koskevat hankinnat 160 000 euroa.**

4 DIGITAALISEN IDENTITEETIN HALLINTA

Edistetään Suomen kansalaisille ja kaikille Suomessa asuville mahdollisuutta sähköiseen tunnistautumiseen. Edistetään toimivien sähköisten tunnistusratkaisujen kehittymistä, jotka mahdollistavat erilaisten välineiden käytön.

Tavoite:	Julkinen hallinto takaa jokaiselle kansalaiselle ja asukkaalle luotettavan, käytettävän sähköisen identiteetin. Valtio mahdollistaa kattavasti ja syrjimättömästi digitaalisen tunnistamisratkaisun kansalaisille ja asukkaille, ja takaa henkilöllisyyden todentamisen mahdollisuuden digitaalisessa maailmassa.
Vastuu:	Valtiovarainministeriö
Kohde:	Kansalaiset
Aikataulu:	2020-2023
Toimenpiteet:	Valtiovarainministeriö koordinoi yhdessä muiden ministeriöiden kanssa tarvittavat lainsäädäntömuutokset ja Digi- ja väestötietovirastossa tarpeelliset tehtävät.
Mittaaminen:	Lainsäädäntömuutokset on tehty ja tarvittavat tehtävät määritelty. Kuinka monella on mahdollisuus sähköiseen asiointiin, huomioiden toisen puolesta asiointi ja valtuudet?
Kustannus/hyöty:	Palvelukokonaisuus toteutetaan omana hankkeena, jossa kustannukset ja hyödyt arvioidaan ja joka vastaa myös palvelukokonaisuuden rahoituksen järjestämisestä.

5 KANSALAISTEN JA HENKILÖSTÖN OSAAMISEN KEHITTÄMINEN

Kehitetään julkisen hallinnon ja yhteisöjen kaikkien henkilöryhmien sekä yksityisten kansalaisten digitaalisen turvallisuuden taitoja ja -tietoisuutta.

5.1 Digitaalisen turvallisuuden koulutuspalvelut kansalaisille ja henkilöstölle

Tavoite:	Digitaaliseen turvallisuuteen liittyvän osaamisen kasvattaminen.
Vastuu:	Digi- ja väestötietovirasto
Kohde:	Kansalaiset, henkilöstö ja johto
Aikataulu:	2021-2023
Toimenpiteet:	Digi- ja väestötietovirasto yhdessä opetus- ja kulttuuriministeriön kanssa tuotteistaa digitaalisen turvallisuuden koulutukset kansalaisille, henkilöstölle ja johdolle. Jo olemassa olevia avoimia koulutuksia kehitetään edelleen ja luodaan uusia koulutuksia. Koulutuksista kootaan kokonaisuuksia tukemaan esimerkiksi digitaaliseen turvallisuuteen liittyvää kansallista sertifiointia. Virasto tuottaa koulutuksille

jakelukanavan. Opetus- ja kulttuuriministeriö kehittää kansalaisten digitaalisen turvallisuuden osaamista kattavasti osana suomalaista koulutusjärjestelmää.

Mittaaminen: Koulutuskokonaisuudet on laadittu ja jakelukanava on käytössä.

Kustannus/hyöty: Kustannukset arviolta 80 000 euroa vuodessa. Koulutusten jakelukanavana voidaan käyttää nykyisiä alustoja, joten lisenssi- ja käyttöönotosta syntyvät kustannukset ovat maltilliset. Kustannukset koostuvat uuden materiaalin tuottamisen sekä ylläpitämiseen liittyvistä kuluista, koulutusmateriaalien lisensseistä ja palvelumaksuista sekä verkkosivuston ja palvelualustan lisenssikustannuksista (esim. Pilvipalvelualustan vuosikustannus). Osaamisen kehittämisellä turvataan hallinnon palvelujen turvallisuutta ja toimintavarmuutta sekä kansalaisten ja asukkaiden mahdollisuuksia käyttää hallinnon palveluja.

5.2 Digitaalisen turvallisuuden sertifikaatti kansalaisille ja organisaatioille

Tavoite: Kansalaisten ja organisaatioiden sertifiointijärjestelmän kehittäminen luottamuksen lisäämiseksi ja osaamisen tunnistamiseksi.

Vastuu: Digi- ja väestötietovirasto

Aikataulu: 2021-2022

Toimenpiteet: Digi- ja väestötietovirasto yhdessä yhteisöjen kanssa selvittää olemassa olevien kansalaisille ja yhteisöille luotujen sertifiointijärjestelmien soveltuvuutta kansalliseen käyttöön. Selvityksessä otetaan kantaa sertifiointijärjestelmien laajuuteen digitaalisen turvallisuuden eri osa-alueilla sekä soveltuvuuteen kansalaisille ja yhteisöille. Selvityksen avulla kartoitetaan vaihtoehdot yhtenäiseksi sertifiointimalliksi, jonka avulla eri tyyppiset yhteisöt ja kansalaiset kykenevät varmistamaan ja todentamaan digiturvallisuuden minimivaatimusten täyttymisen. Selvityksessä kartoitetaan myös vaihtoehdot vaatimustenmukaisuuden arviointiin. Tällaisia ovat esimerkiksi itsearviointi tai ulkopuolinen auditointi. Selvityksessä esitetään etenemisvaihtoehdot sertifiointimallin toteuttamiselle.

Mittaaminen: Selvitys digitaalisen turvallisuuden sertifiointimalleista on tehty. Selvityksen perusteella on valittu toteutusmalli. Valitut toteuttajat ovat toteuttaneet mallin ja palvelu on tarjolla kansalaisille ja yhteisöille.

Kustannus/hyöty: Selvitys 40 000 euroa. Yhteiskunnan toimijat, kansalaiset ja yhteisöt voivat osoittaa noudattavansa digiturvallisia toimintatapoja. Hyötynä markkinaehtoisten palveluiden yhteismitallinen tapa osoittaa niiden luotettavuus. Sertifikaatilla/digiturvamerkillä ohjataan kulutusta turvallisiin palveluihin. Kustannukset syntyvät sertifiointiohjelman laatimisesta tai nykyisen (esim. tietoturvamerkki) kehittämisestä

tarkoitukseen sopivaksi, auditoinneista, viestinnästä sekä syntyneen kokonaisuuden ylläpitämisestä (esim. sertifiointitietokanta ja palvelun sivusto).

Yhteensä kohdassa 5 selvitystyötä koskevat hankinnat 40 000 euroa ja toteutusta koskevat hankinnat 80 000 euroa vuodessa kolmen vuoden ajan eli yhteensä 240 000 euroa.

6 JULKISEN HALLINNON DIGITAALISEN TURVALLISUUDEN ASIANTUNTIJAPALVELUT

Digitaalisen turvallisuuden keskitettyjä asiantuntijapalveluita kehitetään ja tarjotaan laajasti koko julkisen hallinnon käyttöön.

Tavoite:	Yhteiset digitaalisen turvallisuuden asiantuntijapalvelut on järjestetty julkiselle hallinnolle.
Vastuu:	Digi- ja väestötietovirasto
Kohde:	Julkinen hallinto
Aikataulu:	2020-2021
Toimenpiteet:	Digi- ja väestötietovirasto yhdessä Hanselin kanssa selvittää ja kehittää edelleen julkisen hallinnon digitaalisen turvallisuuden konsultoinnin ja -auditoinnin palveluja ja niiden hankintamenettelyjä. Selvitys kattaa palveluntarjoajien yhtenäiset mahdollisuudet palvelujen tarjontaan, julkisen hallinnon organisaatioiden tarpeen digitaalisen turvallisuuden konsultointiin ja -auditointiin sekä asiantuntijapalvelun hankintaan liittyvät vaihtoehtoiset mallit. Selvityksen perusteella Digi- ja väestötietovirasto rakentaa julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelun sekä sitä tukevat työkalut.
Mittaaminen:	Asiantuntijapalvelu ja työkalut ovat käytössä.

Kustannus/hyöty: Toteutetaan virkatyönä. Hyötynä palveluiden saatavuus koko julkiselle hallinnolle.

7 JULKISEN HALLINNON PALVELUJEN JA PALVELUTUOTANNON DIGITAALISTEN TURVALLISUUDEN ARVIOINTI

Edistetään normeihin ja standardeihin perustuvaa digitaalisten palvelujen ja palvelutuottajien arviointia ja varmentamista.

Tavoite: Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1046/2011) sekä lain tietoturvallisuuden arviointilaitoksista (1045/2011) mahdolliset uudistamistarpeet selvitetään ja johtopäätösten perusteella toteutetaan mahdollinen säädösvalmistelu vastaamaan muuttunutta digitaalista toimintaympäristöä.

Vastuu: Valtiovarainministeriö

Kohde: Julkinen hallinto

Aikataulu: 2021-2022

Toimenpiteet: Valtiovarainministeriö yhdessä liikenne- ja viestintäministeriön sekä Traficomin ja muiden ministeriöiden ja mahdollisesti kuntien kanssa selvittävät nykytilan ja uudistamistarpeet vuonna 2021. Johtopäätösten perusteella lainvalmistelu 2021-2022. Mahdolliset uudet lakiehdotukset eduskuntaan alkusyksystä 2022.

Mittaaminen: Selvitys on tehty. Selvityksen aiheuttamat jatkotoimenpiteet on toteutettu.

Kustannus/hyöty: Selvitys ja mahdollinen säädösten valmistelu laaditaan virkatyönä. Valmisteluun sisältyy vaikuttavuusarviointi ja taloudellisten vaikutusten arviointi. Traficomin työ ei sisälly kustannusarvioon.

8 JULKISEN HALLINNON TARVITSEMAN DIGITAALISEN INFRASTRUKTUURIN SUOJAAMINEN

Keskeisten yhteisten teknologioiden ja palveluiden turvallisuutta edistetään siten, että julkisen hallinnon toiminnan, prosessien ja palvelujen jatkuvuus ja tiedot ovat turvatut.

8.1 Julkisen hallinnon turvallisuusarkkitehtuuri

Tavoite: Julkisen hallinnon turvallisuusarkkitehtuurilla ohjataan digitaalisen infrastruktuurin kehittämistä.

Vastuu: Valtiovarainministeriö

VALTIOVARAINMINISTERIÖ

Kohde: Julkinen hallinto

Aikataulu: Selvitys 2020-2021, toimeenpano 2021-2023

Toimenpiteet: Valtiovarainministeriö yhdessä muiden ministeriöiden sekä Digi- ja väestötietoviraston ja Traficomin kanssa laatii julkisen hallinnon turvallisuusarkkitehtuurin. Työssä hyödynnetään Tiedonhallintalain toimeenpanon yhteydessä laadittavia tiedonhallintakarttoja ja –malleja.

a) Kuvataan mille tasolle kansallinen kyvykkyys rakennetaan ja mitkä ovat sellaisia kriittisiä digitaalisia palveluita, tietoa ja infrastruktuuria, johon liittyy erityiset kansalliset hallinnan ja turvaamisen vaatimukset. Valmistellaan linjaukset siitä, miltä osin palveluita tuotetaan ja infrastruktuuria rakennetaan kansallisin toimin ja resurssein, miltä osin tukeudutaan esimerkiksi EU:n yhteiseen kehittämiseen tai muuhun kansainväliseen yhteistyöhön ja erityisesti julkisessa hallinnossa siihen, kuinka julkisten digitaalisten palveluiden tuotannossa tulisi ja voidaan hyödyntää erilaisia uusia palvelumalleja ja teknologian tarjoamia mahdollisuuksia.

b) Laaditaan ja otetaan käyttöön julkisen hallinnon palveluiden ja tietojärjestelmien kriittisyyden luokitusjärjestelmä sekä arvioidaan tietojärjestelmärekisterin tarve ja arvioidaan kriittisten palveluiden, tietojärjestelmien ja tietoliikenneratkaisuiden vaatimustenmukaisuuden nykytilanne.

c) Valmistellaan luettelo teknologioista, joiden käyttöä julkisen hallinnon digitaalisissa palveluissa suositellaan. Valmistellaan myös luettelo teknologioista, joiden käyttöä on vältettävä ja mahdollinen käyttö on arvioitava riskienhallinnan näkökulmasta, esimerkiksi vanhentunut teknologia.

d) Kohtaan 7 liittyen laaditaan suunnitelma palveluiden ja palveluverkkojen turvallisuuden tarkistamisen kehittämiseksi.

Toimenpiteet arkkitehtuurin noudattamiseksi:

e) Kootaan tietopohja yhteiskunnan kriittisten tietojärjestelmien, tietovarantojen sekä tietoverkkojen pitkän aikavälin kehittämistarpeista sekä laaditaan suunnitelma keskitetyllä rahoituksella toteutettavan kehittämisohjelman käynnistämiseksi. Tähän liittyen tarkastellaan erityisesti kriittisten vanhojen tietojärjestelmien haavoittuvuuksien kartoittamista ja elinkaaren suunnittelua.

f) Laaditaan pitkän aikavälin kehittämissuunnitelma kriittisten palveluiden, tietojärjestelmien ja tietoliikenneratkaisuiden vaatimustenmukaisuuden parantamiseksi ja olemassa olevan korjausvelan hallitsemiseksi.

Mittaaminen: Kohdat a-d on tehty. Kohdat e-f on toteutettu julkisen hallinnon tai valtion hallinnon yhteisten palvelujen osalta.

Kustannus/hyöty: Selvitys nykytilanteesta ja puutteiden kartoitus 60 000 euroa. Turvallisuusarkkitehtuurin kehittämistarpeiden kuvaaminen/selvitys sisältäen kohtien a-d mukaiset asiat 100 000 euroa. Teknologisten linjausten laadinta 120 000 euroa. Teknologisten linjausten toteuttamisesta ja niiden mukaisen ympäristöjen rakentamisesta kohtien e-f osalta vastaa kukin viranomainen, ja nämä kustannukset arvioidaan hankekohtaisesti. Turvallisuusarkkitehtuurin taso vaihtelee, jos jokainen viranomainen valmistelee erikseen turvallisuusarkkitehtuuriin kuuluvat asiat. Keskitetyllä koordinaatiolla on mahdollista vähentää kustannuksia ja parantaa suunnittelun tulosten yhdenmukaisuutta ja laatua sekä tuotettavien palvelujen ja niiden tuotantoympäristöjen turvallisuuta, valmiutta ja varautumista.

8.2 Julkisen hallinnon tarvitsema havainnointi, reagointi ja analysointi

Tavoite: Digitaalisen turvallisuuden häiriöiden käsittelyn nopeuttaminen ja haavoittuvuuksien tunnistaminen.

Vastuu: Digi- ja väestötietovirasto, Traficom/Kyberturvallisuuskeskus

Kohde: Julkinen hallinto sekä yhteisöt

Aikataulu: 2021, suunnitelman toimeenpano 2022

Toimenpiteet: Digi- ja väestötietovirasto yhdessä Kyberturvallisuuskeskuksen kanssa laatii ohjeita ja suosituksia julkisen hallinnon palvelujen havainnointi- ja reagointikyvyn kehittämiseksi sekä VIRT-häiriötilanteiden hallintamallin parantamiseksi. Kuntien tietoliikenteen osalta toimenpide toteutetaan kohdassa 3.1.

Digi- ja väestötietovirasto yhdessä Kyberturvallisuuskeskuksen kanssa suunnittelee julkisen hallinnon kriittisten tietojärjestelmien, tietoliikenneverkkojen ja IoT-laiteiden tunnistamisen. Suunnitelmassa käsitellään haavoittuvuustestausten toteutusta siten, että kriittiseksi tunnistettujen tietojärjestelmien, tietoliikenneverkkojen ja IoT-laitteiden omistajat laativat suunnitelman haavoittuvuuksien löytämiseksi. Suunnitellaan havaintojen kerääminen yhteen jaettavaksi kriittisten tietojärjestelmien, tietoliikenneverkkojen ja IoT-laitteiden käyttäjäorganisaatioille. Lisäksi suunnitellaan elinkaarensa loppupuolella olevien tietojärjestelmien haavoittuvuuksien kartoittaminen ja elinkaaren hallinta.

Cert-fi toimintaa kehitetään edelleen lisäämällä havainnointikykyä ja kokoamalla yhteen nykyisiä havaintotietoja. Havainnointiin tarvitaan teknisiä välineitä (esim.

Havaro), skannauspalveluja ja tietoja kriittisten järjestelmien haavoittuvuuksien määrien kehittymisestä. Suunnitellaan hankinnat ja käyttöönoton tukipalvelut ja toimeenpanovastuut kaikille suunnitelman tehtäville.

Mittaaminen: Ohjeet ja suositukset on laadittu ja tukipalvelu on käytössä. Haavoittuvuustestausten toteutuminen suunnitelmaa vasten.

Kustannus/hyöty: Selvitys 60 000 euroa. Nopeammalla reagoinnilla turvataan kansalaisten palvelujen jatkuvuus ja turvallisuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia. Vähennetään mainehaittoja ja luottamuksen rapautumista sekä hallinnossa, yhteisöissä että kansalaisen keskuudessa.

8.3 Julkisen hallinnon tiedon turvallisuus pilvipalveluissa

Tavoite: Pilvipalveluihin tallennetun tiedon turvallisuus tiedon elinkaaren aikana.

Vastuu: Digi- ja väestötietovirasto

Kohde: Julkinen hallinto

Aikataulu: 2021-2023

Toimenpiteet: Digi- ja väestötietovirasto yhdessä Valtorin kanssa ja Traficomin/Kyberturvallisuuskeskuksen tukemana määrittävät tiedon salauksen käyttötapaukset ja vähimmäisvaatimukset.

Digi- ja väestötietovirasto laatii pilvipalvelujen soveltamisohjeen. Ohje sisältää sopimuslausekkeita, määrittelydokumentteja ja vaatimusmäärittelyjä palvelun vaihtamista tai käytön päättämistä varten (ns. pilvi-exit), jolloin palvelujen siirtäminen toiseen pilviympäristöön tulee myös mahdolliseksi. Suunnitellaan ohjeen käyttäminen palveluverkostojen varmentamisessa.

Mittaaminen: Käyttötapaukset ja vähimmäisvaatimukset on kuvattu.

Kustannus/hyöty: Soveltamisohjeen valmistelu 50 000 euroa. Yhtenäisellä ohjeistuksella on mahdollista vähentää kustannuksia ja parantaa ohjeistuksen laatua sekä tiedon salaamisen ja pilvipalveluiden turvallisuutta, valmiutta ja varautumista.

Yhteensä kohdassa 8 selvitystyötä koskevat hankinnat 270 000 euroa ja toteutustyötä koskevat hankinnat 120 000 euroa.

9 JULKISEN HALLINNON AUTONOMISTEN JA OPPIVIEN JÄRJESTELMIEN SEKÄ PALVELUJEN TURVALLINEN KEHITTÄMINEN

Autonomisten ja oppivien järjestelmien sekä digitaalisten palvelujen turvallisuudesta huolehditaan riskienhallinnan avulla.

9.1 Julkisen hallinnon autonomisten ja oppivien järjestelmien valvonta

Tavoite: Autonomisten ja oppivien järjestelmien valvonnasta huolehditaan. Autonomisten ja oppivien järjestelmien kehittämiseen ja valvontaan liittyvät turvallisuusperiaatteet ja kontrolliympäristö on määritetty ja sen toteutumista valvotaan.

Vastuu: Valtiovarainministeriö

Kohde: Julkinen hallinto sekä yhteisöt

Aikataulu: 2022-2023

Toimenpiteet: Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa asettaa työryhmän selvittämään autonomisten ja oppivien järjestelmien turvallisuuteen liittyviä kontrolliympäristöjä. Selvityksen perusteella laaditaan järjestelmien kehittämiseen ja valvontaan liittyvät periaatteet sekä kontrolliympäristö, joka ohjaa järjestelmien kehitystä ja ylläpitoa sekä viestintää myös kansalaisille. Luottamuksen on säilyttävä palvelun sisältöön ja tuloksiin eri tilanteissa. Palvelun toiminta tulee läpinäkyvästi viestiä kansalaisille.

Autonomisten ja oppivien järjestelmien turvallisuusperiaatteiden ja kontrolliympäristön tulee ottaa kantaa kehitys- ja valvontavaatimuksiin seuraavilla osa-alueilla:

- oikeudenmukaisuus; mallien on oltava lainmukaisia ja niiden on käsiteltävä tietoa puolueettomasti
- eheys ja häiriönsieto; mallit toimivat johdonmukaisesti eri toimintaympäristöissä ja toimintatavat häiriötilanteissa on määritetty
- selitettävyys; mallien tapa oppia ja tehdä päätöksiä on tulkittavissa ja selitettävissä

Valtiovarainministeriö edistää aktiivisesti autonomisten ja oppivien järjestelmien eettisen säännöstön ja kontrolliympäristön kehittämistä kansainvälisessä yhteisössä.

Digi- ja väestötietovirasto laatii standardin mukaisen kansallisen soveltamisohjeen autonomisten ja oppivien järjestelmien kehittämiseen ja käyttöönottoon. Virasto kehittää asiantuntijapalvelun järjestelmien testaamiseen ja varmentamiseen.

Autonomisten ja oppivien järjestelmien kontrolliympäristö edellyttää uusien uhkaskenaarioiden ja riskien sekä niiden hallintaan sopivien kontrollien määrittelyä. Kontrolliviitekehyksen tai eettisen säännöstön ja kontrolliympäristön laatiminen koostuu riskianalyysistä, kontrollien määrittelytyöstä sekä soveltamisohjeen kirjoittamisesta. Lisäksi hankkeessa tulee tehdä pilotti, jossa testataan kontrollien sopivuutta julkisen sektorin organisaatioon.

Mittaaminen: Kansallinen soveltamisohje on valmisteltu.

Kustannus/hyöty: Selvitys koskien riskianalyysiä, kontrollien määrittelyä sekä ohjeistoa ja sen pilotointia 100 000 euroa. Yhdenmukaisella ohjeistuksella turvataan oppien ja autonimisten järjestelmien turvallisuus ja jatkuvuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia, ja mainehaittoja.

9.2 Julkisen hallinnon turvallinen palvelukehitys

Tavoite: Julkisen hallinnon palvelukehitysprosessissa huomioidaan jatkuvasti päivittyvät tietoturvallisuusvaatimukset riskienhallinnan avulla.

Vastuu: Digi- ja väestötietovirasto

Kohde: Julkinen hallinto

Aikataulu: 2022-2023

Toimenpiteet: Digi- ja väestötietovirasto määrittää miten palvelukehityksessä asetetaan riskienhallinnan kautta jatkuvasti päivittyvät digitaalisen turvallisuuden vaatimukset. Palvelukehitykseen liittyvien turvallisuusvaatimusten tulee kattaa eri sovelluskehitysmalleihin sopivat turvallisuuden varmistamiseen liittyvät toimenpiteet. Lisäksi Digi- ja väestövirasto laatii ohjeistuksen suositelluista menetelmistä, kuten DevSecOps-kehitysmenetelmä. Digi- ja väestötietovirasto tuotteistaa turvallisen palvelukehityksen koulutuksia julkishallinnon ja elinkeinoelämän käyttöön.

Mittaaminen: Vaatimusten muodostumisprosessi ja keskeisiä vaatimuksia kuvattu ja niitä käytetään riskienhallinnan avulla palvelukehityshankkeissa.

Kustannus/hyöty: Selvitys koskien uhka- ja riskianalyysitietojen analysointiin tarvittavan mallin luomista 40 000 euroa. Testausmenetelmän ja sitä tukevien työkalujen määrittely

40 000 euroa. Koulutusten valmistelu ja toteutus 50 000 yhtenä vuonna. Mahdollisista keskitetyistä ohjelmistoista kuten testaustyökaluista päätetään erikseen. Yhdenmukaisella uhka- ja riskianalyysitietojen mallilla turvataan digitaalisten palvelujen turvallisuus ja jatkuvuus sekä pienennetään häiriötilanteiden ja toteutuneiden tietoturvaloukkausten aiheuttamia kustannuksia, ja mainehaittoja.

Yhteensä kohdassa 9 selvitystyötä koskevat hankinnat 180 000 euroa ja toteutusta koskevat hankinnat 50 000 euroa.

Alustava yhteenveto kustannuksista

Yhteenveto selvityksiä ja toteutusta koskevista hankinnoista:

	Selvitys	Toteutus
Kohta 1	80 000 €	0 €
Kohta 2	140 000 €	260 000 €
Kohta 3	160 000 €	0 €
Kohta 4	0 €	0 €
Kohta 5	40 000 €	240 000 €
Kohta 6	0 €	0 €
Kohta 7	0 €	0 €
Kohta 8	270 000 €	120 000 €
Kohta 9	180 000 €	50 000 €
Yhteensä	870 000 €	670 000 €

Toimeenpanosuunnitelman toteuttamiseksi tarvittavat selvitystöitä koskevat hankinnat ovat arviolta 870 000 euroa ja toteutusta koskevat hankinnat 670 000 euroa.

Lisäksi selvitystöitä koskevan henkilöstömäärätarpeen on arvioitu olevan valtiovarainministeriössä, digi- ja väestötietovirastossa sekä Traficomissa yhteensä noin 11 henkilötyövuotta vuodessa, joista noin 10% on nykyisiä resursseja.

Toteutusta koskeva henkilötyömäärätarve valtiovarainministeriössä ja digi- ja väestötietovirastossa on arviolta sama kuin selvitystöiden aikana. Traficomin toteutustyön vaatimaa henkilötyötä on edelleen tarkennettava.

Pysyvät kustannuslisäykset ja niiden vaikuttavuusarviot on tarkoitus arvioida selvitysvaiheessa.