VALTIOVARAINMINISTERIÖ

TUVEn turvallisuus-sopimuksen toimeenpano-ohje

18/2013 JulkICT-toiminta

VALTIOVARAINMINISTERIÖ

TUVEn turvallisuusverkkotoiminnan turvallisuusperiaatteista solmitun sopimuksen toimeenpano-ohje

Valtiovarainministeriön julkaisuja

18/2013 ICT-toiminta

441 729
Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Anitta Heiskanen /VM-julkaisutiimi

Juvenes Print - Suomen Yliopistopaino Oy, 2013

Kuvailulehti

Julkaisija ja julkaisuaika	Valtiovarainministeriö, elokuu 2013	
Tekijät	Turvallisuussopimushanke, Ohjausryhmän pj Esko Vainio VM, sihteeri Sami Kilkkilä ERVE	
Julkaisun nimi	TUVEn turvallisuussopimuksen toimeenpano-ohje	
Asiasanat	Turvallisuus, turvallisuussuunnittelu, tietoturva, tietoliikenneverkot, tieto- ja viestintätekniikkaverkot	
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 18/2013	
Julkaisun myynti/jakaja	Julkaisu on saatavissa pdf-tiedostona osoitteesta www.vm.fi/julkaisut. Samassa osoitteessa on ohjeet julkaisun painetun version tilaamiseen.	
Painopaikka ja -aika	Juvenes Print - Suomen Yliopistopaino Oy, 2013	
ISBN 978- 952-251-474-5 (nid.) **ISSN** 1459-3394 (nid.) **ISBN** 978-952-251-475-2 (PDF) **ISSN** 1797-9714 (PDF)	**Sivuja** 48	**Kieli** Suomi

Tiivistelmä

Tämä toimeenpano-ohjeen tarkoituksena on esittää, miten sopimusta hallinnon turvallisuusverkon turvallisuusperiaatteista sovelletaan hallinnon turvallisuusverkko-toiminnassa. Toimeenpano-ohje antaa perusteet niiden turvallisuustoimien toteuttamiseksi, jotka kunkin hallinnon turvallisuusverkkotoimintaan osallistuvan organisaation tulee omalta osaltaan huomioida turvallisuusverkon käyttäjinä, palveluntuottajina tai alihankkijoina.

Presentationsblad

Utgivare och datum	Finansministeriet, Augusti 2013	
Författare	Hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista solmitun sopimuksen toimeenpano-ohje	
Publikationens titel	TUVEn turvallisuussopimuksen toimeenpano-ohje	
Publikationsserie och nummer	Finansministeriet publikationer 18/2013	
Beställningar/distribution	Publikationen finns på finska i PDF-format på www.vm.fi/julkaisut. Anvisningar för beställning av en tryckt version finns på samma adress.	
Tryckeri/tryckningsort och -år	Juvenes Print - Suomen Yliopistopaino Oy, 2013	
ISBN 978- 952-251-474-5 (nid.) **ISSN** 1459-3394 (nid.) **ISBN** 978-952-251-475-2 (PDF) **ISSN** 1797-9714 (PDF)	**Sidor** 48	**Språk** Finska

Sammandrag

Syftet med denna verkställighetsanvisning är att redogöra för hur avtalet om säkerhetsprinciperna för förvaltningens säkerhetsnät ska tillämpas vid förvaltningens säkerhetsnätverksamhet. Verkställighetsanvisningen ger grunderna för förverkligandet av de säkerhetsåtgärder som vare organisation som deltar i förvaltningens säkerhetsnätverksamhet för egen del ska iaktta i egenskap av användare av, serviceproducent för och underleverantör till säkerhetsnätet.

Description page

Publisher and date	Ministry of Finance, August 2013	
Author(s)	Security Agreement Project, Steering Group Chair Esko Vainio, Ministry of Finance; Secretary Sami Kilkkilä, State Security Network Ltd (ERVE)	
Title of publication	TUVEn turvallisuussopimuksen toimeenpano-ohje	
Publication series and number	Ministry of Finance publications 18/2013	
Distribution and sale	The publication can be accessed in pdf-format in Finnish at www.vm.fi/julkaisut. There are also instructions for ordering a printed version of the publication.	
Printed by	Juvenes Print - Suomen Yliopistopaino Oy, 2013	
ISBN 978- 952-251-474-5 (nid.) **ISSN** 1459-3394 (nid.) **ISBN** 978-952-251-475-2 (PDF) **ISSN** 1797-9714 (PDF)	**No. of pages** 48	**Language** Finnish

Abstract

The purpose of this implementation instruction is to present how the agreement on the security principles of the public sector security network is applied in public security information security activity. The implementation instruction outlines the grounds for implementing the security measures that each organisation participating in public sector security network activity must individually take into account as security network users, service providers or subcontractors.

Sisältö

VALTIOVARAINMINISTERIÖ

Ohje VM/1448/00.00.00/2013

Julkisen hallinnon ICT-toiminto 5.7.2013

Ministeriöille, virastoille, laitoksille ja hallinnon turvallisuusverkkotoiminnan toteutukseen osallistuville

HALLINNON TURVALLISUUSVERKKOTOIMINNAN TURVALLISUUSPERIAATTEIDEN TOTEUTUS

Tämä toimeenpano-ohjeen tarkoituksena on esittää, miten sopimusta hallinnon turvallisuusverkon turvallisuusperiaatteista sovelletaan hallinnon turvallisuusverkko-toiminnassa. Toimeenpano-ohje antaa perusteet niiden turvallisuustoimien toteuttamiseksi, jotka kunkin hallinnon turvallisuusverkkotoimintaan osallistuvan organisaation tulee omalta osaltaan huomioida turvallisuusverkon käyttäjinä, palveluntuottajina tai alihankkijoina.

Tällä ohjeella halutaan helpottaa turvallisuusperiaatteista solmitun sopimuksen toteuttamista siten, että turvallisuusverkon turvallisuudelle asetettavat tavoitteet toteutuisivat verkkoon liittyvien tahojen omatoimisen turvallisuustyön tuloksena. Valtiovarainministeriö määrittää tarkastettavat kohteet, joiden turvallisuusjärjestelyt tarkastetaan ja hyväksytään määrättyjen turvallisuusviranomaisten toimesta.

Toimeenpano-ohje on pyritty laatimaan yksinkertaistettuun kaaviomuotoon kuitenkin siten, että jokaista kaaviota täydennetään perusteluosalla. Tämä toimeenpano-ohje ei pyri korvaamaan turvallisuusverkkotoiminnan turvallisuusperiaatteista solmitun sopimuksen liitteessä 2 esitettyä turvallisuusohjeistoa, vaan toimii ohjenuorana turvallisuusperiaatteiden käytännön määritystyössä ja osin myös kunkin organisaation omalle turvallisuusdokumentaatiolle asetettujen velvoitteiden toteutuksessa.

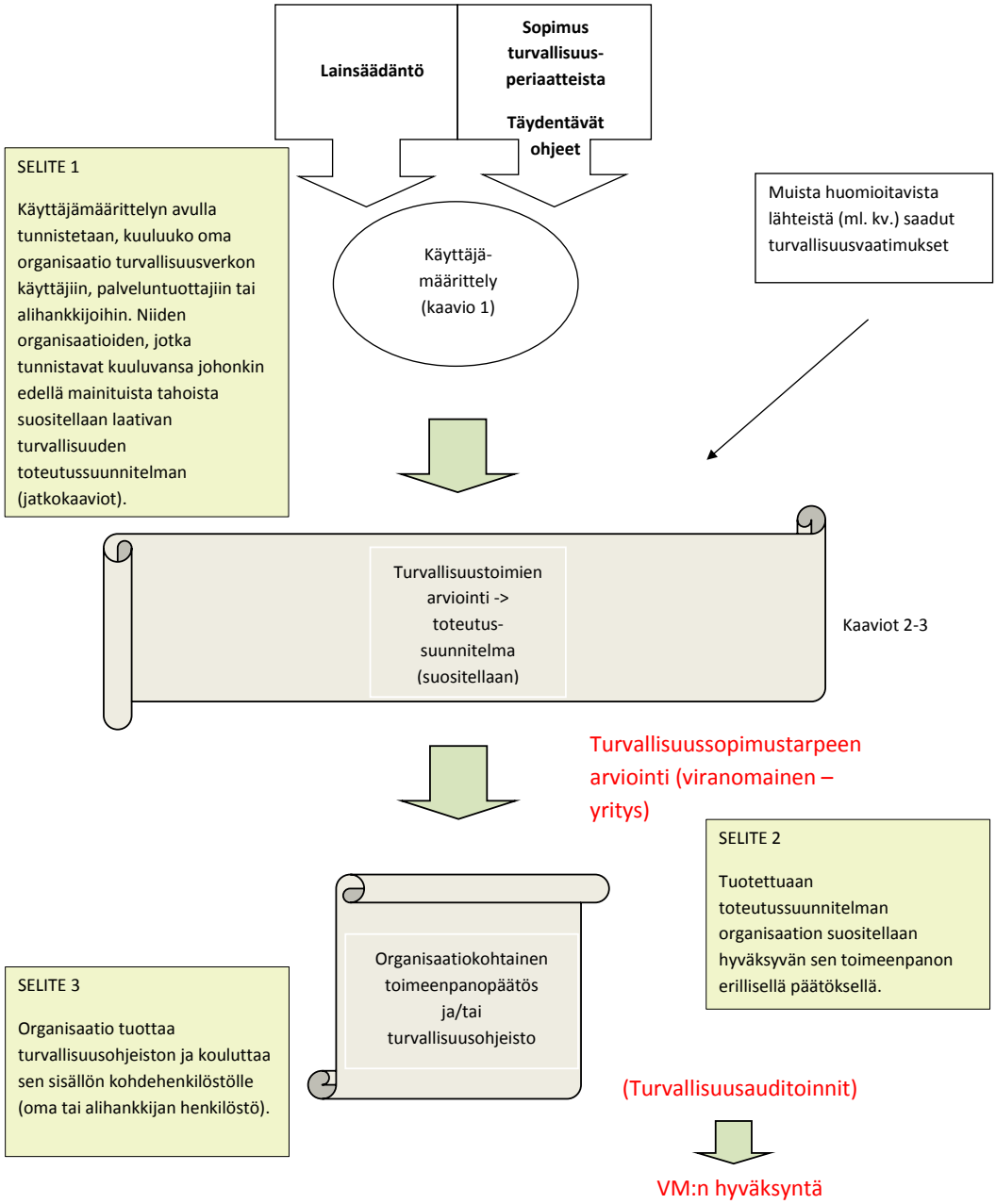
Hallinto- ja kuntaministeri Henna Virkkunen

ICT-johtaja Timo Valli

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

1. Hallinnon turvallisuusverkon turvallisuustoimenpiteiden toteutusperiaatteet



2. Hallinnon turvallisuusverkkotoiminnan turvallisuustoimenpiteiden toteutussuunnitelman laatiminen

Tämän toimeenpano-ohjeen tavoitteena on auttaa erityisesti julkishallinnon toimijoita oman toimintansa turvallisuustoimien arvioinnissa ja erityispiirteet huomioivan toteutussuunnitelman laatimisessa siinä tapauksessa, että kyseinen organisaatio harkitsee turvallisuusverkkoon liittymisen turvallisuusedellytyksiä. Tämä ohje on laadittu myös silmällä pitäen niitä julkishallintoon kuulumattomia kaupallisia toimijoita, jotka toimivat turvallisuusverkon palveluntuottajina tai näiden alihankkijoina.

Valtionhallinnon yksiköiden (virastot, laitokset, liikelaitokset) toimintaansa kohdistamat turvallisuustoimet mitoitetaan kunkin toiminnon turvallisuusvaatimuksia vastaaviksi ja poikkeavat näin huomattavasti toisistaan. Toteutuksissa on syytä huomioida paitsi tämän toimeenpano-ohjeen pääasiakirja (sopimus hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista), myös hallinnonalan (vast.) omassa turvallisuusohjeistossa esitetyt linjaukset. Hallinnonaloja (vast.), joilta puuttuvat oman toimialansa erityispiirteet huomioiva turvallisuusdokumentaatio kehotetaan laatimaan kyseinen dokumentaatio ainakin siltä osin, kuin organisaation toiminta liittyy hallinnon turvallisuusverkon käyttöön. Dokumentaatiossa on syytä ottaa huomioon erityisesti se riskiympäristö, jossa hallinnonalan (vast.) salassa pidettävää tietoa ylipäätään käsitellään. Tehty luokittelupäätös vaikuttaa omalta osaltaan turvallisuusohjeiston sisältöön, samoin kuin muilta hallinnonaloilta (vast.) tai kansainvälisistä lähteistä saadun luokitellun tiedon käsittelyyn kohdistuvat vaatimukset[1].

Yksilöitäessä toimitilaan kohdistuvia turvallisuusvaatimuksia saattaa tulla esille turvallisuussopimuksen tarve tilaajan ja toteuttajan välille. Esimerkiksi VAHTI-ohje 2/2013 (liite 2) sisältää turvallisuussopimusmalleja erilaisiin turvallisuusrakentamisen tilanteisiin.

3. Toteutussuunnitelman vähimmäissisältö

Tarkasteltaessa turvallisuuden toteutussuunnitelmaa hallinnon turvallisuusverkkoon liittymiseksi on syytä huomioida ainakin seuraavat seikat:

- organisaatiota sitovat luokittelupäätökset
    - tietoturvallisuusasetuksen velvoitteet salassa pidettävän tiedon luokittelemiseksi
    - ICT-varautumisen tasomäärittelyt jatkuvuuden hallinnan ja tiedon saatavuuden varmistamiseksi
    - TUVE-turvallisuusperiaatteista solmitun sopimuksen mukaiset velvoitteet
- hallinnolliset toimenpiteet
    - riskienhallintatoimenpiteiden mitoittaminen
    - turvallisuustoimenpiteiden organisointi ja vastuut
    - turvallisuusohjeistotyön suuntaviivat
- henkilöstöä koskevat toimenpiteet (käyttötarve huomioiden)

[1] VAHTI 1/2013, luku 2

    - henkilöstön turvallisuushallinta
    - turvallisuusselvitykset
    - turvallisuuskoulutus
- fyysisen turvallisuuden erityisvaatimukset
    - TUVE-käyttöpisteiden ja palvelintilojen kartoitus
    - TUVE-käyttöpisteiden ja palvelintilojen riskienhallinta
    - TUVE-käyttöpisteiden ja palvelintilojen fyysisen turvallisuuden toteutus
    - TUVE-verkkokokonaisuuden riskit huomioiva luokittelu ja sen mukainen fyysisen turvallisuuden toteutus
    - päätös em. kohteiden priorisoinnin osalta
- teknisen tietoturvallisuuden toteutus
    - riskienhallintapohjainen kriittisyystarkastelu verkon osakomponenttien suhteen
    - teknisen tietoturvallisuuden kokonaisratkaisun mukaisten toimenpiteiden kohdistaminen kunkin osapuolen toimintaympäristöön
- alustavan auditointivalmiuden luominen auditoitaville kohteille
    - esitys keskeisimmistä auditointivaatimuksista (esim. auditointisuunnitelman runko)

Organisaation toiminnan luonne ratkaisee toteutussuunnitelman lopullisen sisällön (ks. sopimus hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista, liite 2).

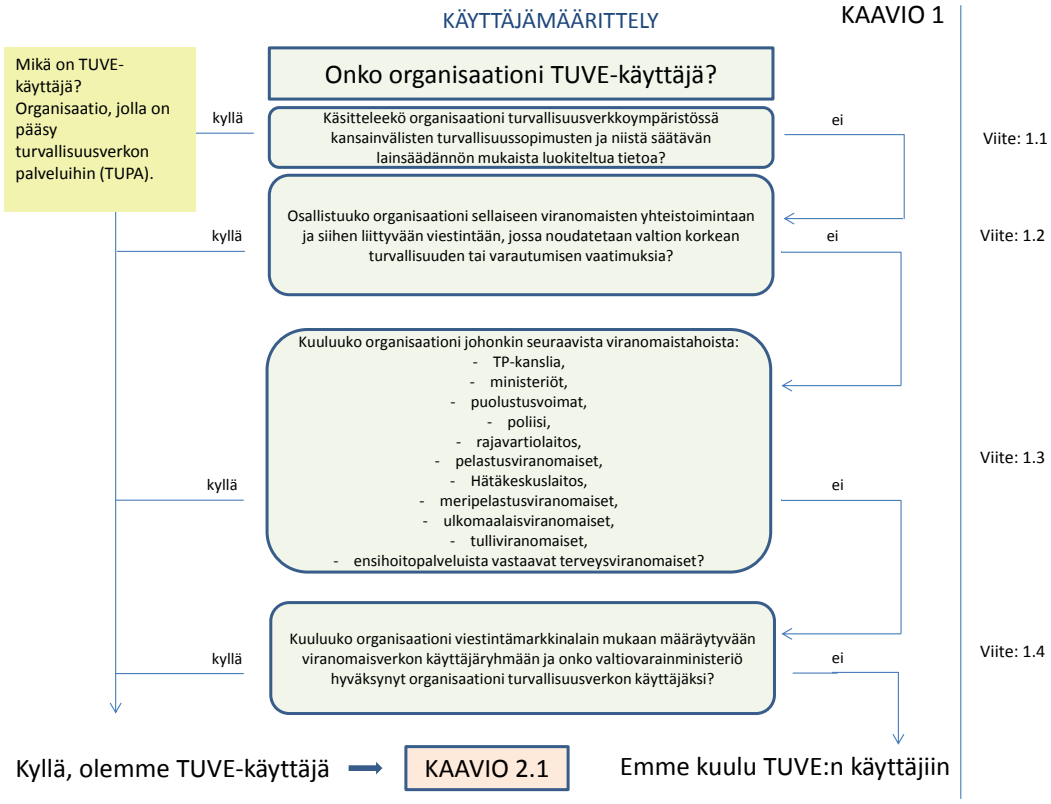
LIITTEET

Liite 1: turvallisuusverkon käyttäjämäärittely

Liite 2: TUVE:n käyttäjä- ja palveluntarjoaja-organisaatioiden turvallisuuden toteutus

Liite 3: Verkon loppukäyttäjien turvallisuuden toteutus

Liite 1
Turvallisuusverkon käyttäjämäärittely



Hallinnon turvallisuusverkon käyttäjien määräytyminen

1. Yleistä

Hallinnon turvallisuusverkon käyttämisvelvoite ja –oikeus on määritetty hallituksen esityksessä laiksi julkisen hallinnon turvallisuusverkkotoiminnasta (HE 54/2013). Toimeenpanosuunnitelman kaaviolla 1 pyritään helpottamaan organisaatioiden määrittämistyötä turvallisuusverkkoon liittymisen osalta. Verkon käyttäjät voidaan jakaa sellaisiin, jotka laki suoranaisesti nimeää turvallisuusverkon käyttäjiksi (käyttävät joko yhteisiä tai toimialakohtaisia turvallisuusviranomaispalveluita) ja sellaisiin, joiden tehtävä turvallisuusverkkohankkeen toteutumisessa määrittää ne ko. verkon käyttäjäkuntaan kuuluviksi. Kukin julkishallinnon yksikkö määrittää itse organisaationsa osalta ne tehtävät - ja niitä hoitavat henkilöt - jotka täyttävät käyttöoikeuden yleiset edellytykset ja jotka toimivat osana valtion ja yhteiskunnan turvallisuuden varmistamista. Turvallisuusverkon toimintaedellytysten luomiseen ja ylläpitämiseen keskittyvien kaupallisten toimijoiden osalta vastuuviranomaiset ohjaavat toimintaa tarvittavilta osin.

1.1

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Kansainvälisellä tietoturvallisuusvelvoitteella tarkoitetaan sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä.

Kansainvälisessä tietoturvalaissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

1.2

HE54/2013 (TuveL 2§): Turvallisuusverkon käyttövelvoite
Turvallisuusverkon käyttövelvoite koskee sellaista valtion johtamiseen ja turvallisuuteen, maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen, rajaturvallisuuteen, pelastustoimintaan, meripelastustoimintaan, hätäkeskustoimintaan, maahanmuuttoon ja ensihoitopalveluun liittyvää viranomaisten sisäistä, välistä ja ulkoista yhteistoimintaa ja viestintää, jossa noudatetaan korkean turvallisuuden tai varautumisen vaatimuksia.
Turvallisuusverkon käyttövelvoite edellyttää tämän lain 2 luvussa tarkoitettujen verkon yhteisten palvelujen sekä laitetilojen, laitteiden ja muun infrastruktuurin käyttöä.

1.3

HE54/2013 (TuveL 3§): Turvallisuusverkon käyttövelvoitteen kohteet

Seuraaviin käyttäjäryhmiin kuuluvien on käytettävä turvallisuusverkkoa silloin, kun ne hoitavat 2 §:n 1 momentissa tarkoitettuun toimintaan liittyviä tehtäviä:

1) tasavallan presidentin kanslia ja valtio-neuvostosta annetussa laissa (175/2003) tarkoitetut ministeriöt;
2) puolustusvoimista annetussa laissa (551/2007) tarkoitetut viranomaiset;
3) poliisin hallinnosta annetussa laissa (110/1992) tarkoitetut viranomaiset;
4) rajavartiolaitoksen hallinnosta annetussa laissa (577/2005) tarkoitetut viranomaiset;
5) pelastuslaissa (379/2011) tarkoitetut pelastustoimen viranomaiset;
6) hätäkeskustoiminnasta annetussa laissa (692/2010) tarkoitettu Hätäkeskuslaitos;
7) meripelastuslaissa (1145/2001) tarkoitetut viranomaiset;
8) ulkomaalaislaissa (301/2004) tarkoitetut viranomaiset;
9) tullilaissa (1466/1994) tarkoitetut viran-omaiset;
10) terveydenhuoltolaissa (1326/2010) tarkoitetut ensihoitopalvelusta vastaavat viranomaiset.

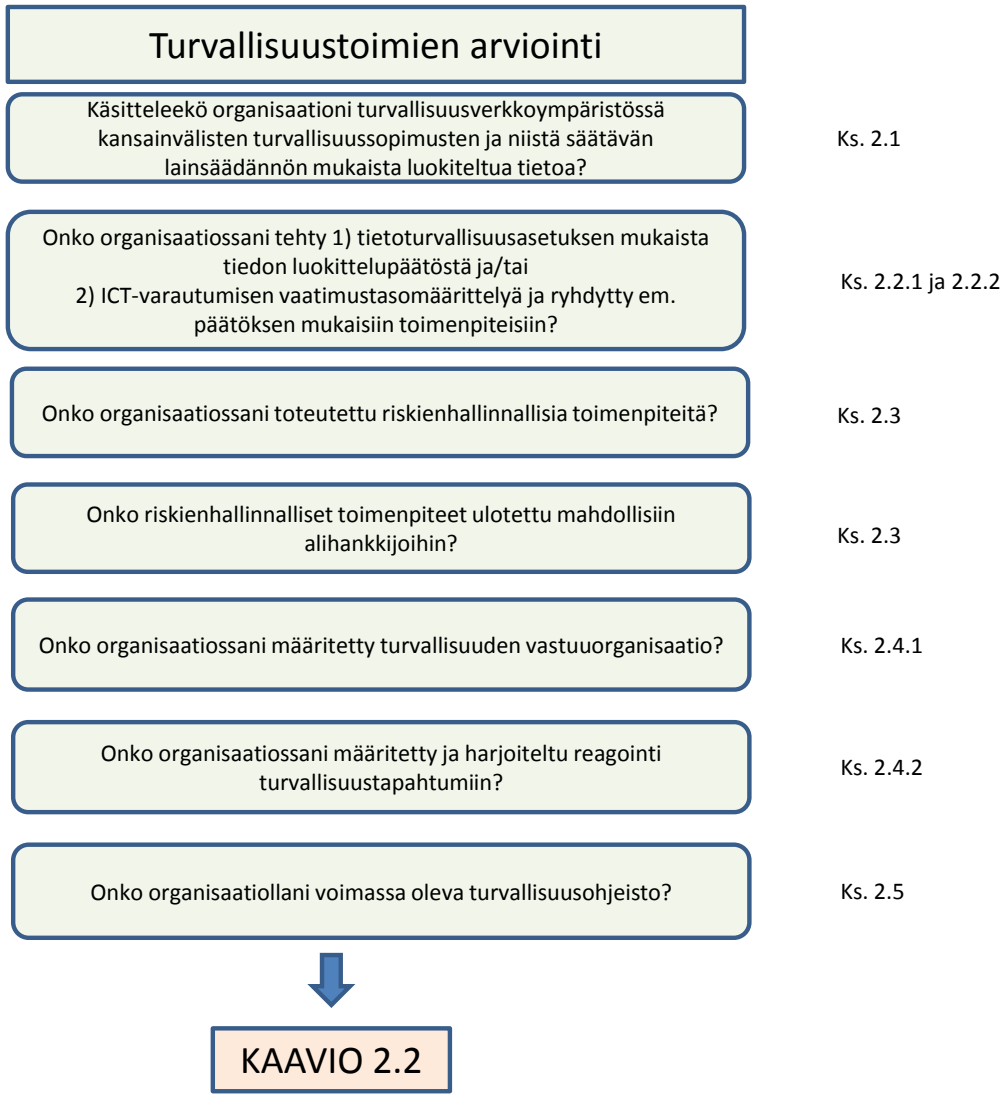
1.4

HE54/2013 (TuveL 4§): Turvallisuusverkon muu käyttö

Turvallisuusverkkoa voi käyttää myös muu kuin 3 §:ssä tarkoitettu käyttäjä, jos verkon käyttö koskee 2 §:n 1 momentissa tarkoitettuun toimintaan liittyvien tehtävien hoitamista, käyttäjä kuuluu viestintämarkkinalain mukaan määräytyvään viranomaisverkon käyttäjäryhmään ja valtiovarainministeriö on hyväksynyt käyttäjän turvallisuusverkon käyttäjäksi.

Liite 2

TUVE:n käyttäjä- ja palveluntarjoaja-organisaatioiden turvallisuuden toteutus



Julkishallinnon organisaatioiden turvallisuustoimien toteutus turvallisuusverkkoympäristössä

2. Yleistä

Hallinnon turvallisuusverkon käyttäjiä sitoo turvallisuusverkkotoiminnan turvallisuuden toteutuksesta solmittu sopimus. Sopimus määrittää kokonaisturvallisuuden näkökulmasta ne vähimmäistoimet, jotka turvallisuusverkkoon liittyvän organisaation tulee täyttää. Hallinnon turvallisuusverkon palveluntuottajina tai muussa osoitetussa tehtävässä toimivia yrityksiä ja näiden mahdollisia alihankkijoita koskevat samat velvoitteet kuin toimintaan osaa ottavia valtionhallinnon yksiköitä (julkisuuslaki).

Toimeenpanosuunnitelman kaaviolla 2 ja sen alakaavioilla pyritään helpottamaan turvallisuustoimien sisällön ja laajuuden määrittämistyötä sekä julkishallinnon organisaatioissa, että kaupallisten toimijoiden keskuudessa. Kaikkia turvallisuusverkon toimijoita koskee velvoite huolehtia seuraavien turvallisuustoimenpiteiden toteutuksesta:

- Turvallisuuden hallintamenettelyt
- Henkilöstön turvallisuushallinta
- Fyysisen turvallisuuden toteutus
- Teknisen tietoturvallisuuden toteutus.

Edellä mainittujen kokonaisuuksien oikea mitoitus pohjautuu organisaation käyttöympäristön huomioivaan riskienhallintaprosessiin.

2.1

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Kansainvälisellä tietoturvallisuusvelvoitteella tarkoitetaan sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä.

Kansainvälisessä tietoturvalaissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

2.2. Luokittelu

2.2.1 Tietoturvallisuusasetus

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. Tietoturvallisuusasetuksen mukaan tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava mm. siitä, että asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja. Yleiset tietoturvallisuusvelvoitteet koskevat valtionhallinnon viranomaisia siinäkin tapauksessa, että ne eivät luokittele tietoaineistojaan. Perustietoturvallisuustasoa koskeva 5 § on suoraan viranomaisia velvoittava säännös, joka ei ole riippuvainen siitä, minkälaisia tietoturvallisuutta koskevia ratkaisuja viranomainen tekee.

2.2.2 ICT-varautumisen vaatimukset

Valtionhallinnon tietoturvallisuuden johtoryhmän antamassa ohjeessa 2/2012 esitetään ICT-varautumisen osalta kolme vaatimustasoa, jotka vastaavat terminologisesti tietoturvallisuusasetuksessa esitettyjä tasoja (perustaso, korotettu taso, korkea taso). Ohje on suunnattu julkishallinnon toimijoille ja julkishallintoon palvelusopimussuhteessa oleville yrityksille näiden tuottamiin palveluihin liittyen.

2.2.3 Turvallisuusluokitteluohje ja -matriisi

Organisaatio tuottaa tiedon salassa pitoon ja/tai varautumiseen perustuen itselleen turvallisuusluokitusohjeen . Ohje luo esimerkein periaatteet sille, mitkä tai minkä tyyppiset tiedot luokitellaan millekin tasolle organisaation omassa toimintaympäristössä. Turvallisuusluokitteluohjeen perusteella laaditaan toimintokohtaiset turvallisuusluokittelumatriisit, joissa eri hanke-elementeille on määritetty niiden suojaus- ja/tai varautumistaso (ks. sopimus hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista, liite 2: luku 5).

2.3

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
Riskien arviointi on osa organisaation riskien hallintaa. Riskien arvioinnilla tarkoitetaan niitä suunnitelmallisia toimenpiteitä, joilla pyritään tunnistamaan uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Riskejä hallittaessa ja arvioitaessa työhön tulee sisällyttää varautuminen normaaliolojen häiriötilanteisiin sekä organisaation valmiusvelvoitteiden mukaisesti myös poikkeustiloihin.

VAHTI-ohjeessa 7/2003 on esitetty välineitä ja keinoja, joiden avulla tietoriskejä voidaan arvioida. Ohjeessa kuvataan myös riskienhallintaan kohdistuvia velvoitteita, riskien arvioinnin merkitystä ja organisointia sekä riskienhallinnan keinoja, uhkien tunnistamista, riskien suuruuden arviointia, toimenpiteiden määrittelyä ja jatkokehitystä. Riskien arvioinnin menetelminä voidaan käyttää muun muassa ohjeen luvussa 3 kuvattuja menetelmiä. Ohjeen liitteenä on tarkistuslista tietoturvauhkien tunnistamiseksi. On tärkeää tunnistaa tehtyjen analyysien kautta uhkan todennäköisyys ja seurausten vakavuus.

Huom! Sopimus hallinnon turvallisuusverkon turvallisuusperiaatteista edellyttää, että turvallisuusverkkoympäristöön hyväksyttävät *alihankkijat* täyttävät säädösten lisäksi sopimuksen mukaiset turvallisuusvaatimukset. Toimivaltaiset turvallisuusviranomaiset tarkastavat näiden velvoitteiden toteutumisen. Velvoitteiden täyttyminen ja toteutuksen tarkastaminen tapahtuu oikein perustein ainoastaan silloin, kun nimenomaisen kohteen riskiympäristö on arvioitu ennen uhkia torjuvien turvallisuustoimenpiteiden käynnistämistä.

Muita lähteitä:
- ISO 31000:2009 - Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- Riskienhallinta ja turvallisuussuunnittelu. Opas sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille. STM 2011:15.
- Kansallinen turvallisuusauditointikriteeristö, A400-osio.

2.4 Turvallisuusorganisaatio

2.4.1 Turvallisuusorganisaatio ja sen toiminta

Turvallisuusorganisaation koosta, rakenteesta tai tehtävistä ei ole valtionhallinnossa nimenomaista kirjallista ohjausta. Syynä tähän lienee jokaisen organisaation yksilöllisyys ja tätä kautta vaikeus luoda pitävää ohjausta. Turvallisuusvastuiden kantamisen osalta on ohjeistuksesta löydyttävä kuitenkin joitakin linjauksia:

- Turvallisuudesta vastaa aina organisaation johto
- Turvallisuuden vastuut organisaation eri tasoilla tunnistettuaan organisaation johto nimittää kirjallisesti turvallisuuden vastuuhenkilön/t. Turvallisuusvastuut viedään kyseisten henkilöiden tehtäväkuvauksiin ja tehtävät viestitään organisaation koko henkilöstölle. Nimetyllä turvallisuushenkilöstöllä on täten takanaan johdon tuki.
- Turvallisuusorganisaation vastuulla on organisaation turvallisuuden kokonaishallinta sekä organisaation johdon pitäminen selvillä turvallisuustilanteesta ja siinä mahdollisesti tapahtuvista merkittävistä muutoksista. Turvallisuuden hallinta edellyttää turvallisuuspolitiikkaa ja sen pohjalta laadittua, riittävän kattavaa turvallisuusohjeistusta sekä tämän kouluttamista sille osalle henkilöstöä, jota se koskee.

Hallinnon turvallisuusverkkohankkeen turvallisuusorganisaation periaatteellinen toimintatapa on kuvattu hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista solmitun sopimuksen liitteessä 2 (luku 2).

2.4.2 Reagointi turvallisuustapahtumiin

Turvallisuusverkon toimijat ovat sitoutuneet sopimuksessa verkon turvallisuusperiaatteista saattamaan välittömästi tiedoksi turvallisuusverkkoon tai sen hallintaan kohdistuvat todennetut tai epäillyt, merkittäviksi katsottavat turvallisuustapahtumat niille osapuolille, joita asian voidaan epäillä koskevan. Sopijapuolet varmistavat, että edellä mainitut toimenpiteet toteutetaan myös turvallisuusverkkoympäristössä työskentelevissä kaupallisissa toimijoissa riittäviltä osin.

Lähteitä:

- Johdon tietoturvaopas, VAHTI 2/2011
- ISO/IEC 27002
- PCI DSS 12
- COBIT 4.1
- Kansallinen turvallisuusauditointikriteeristö, A500-osio.

2.5

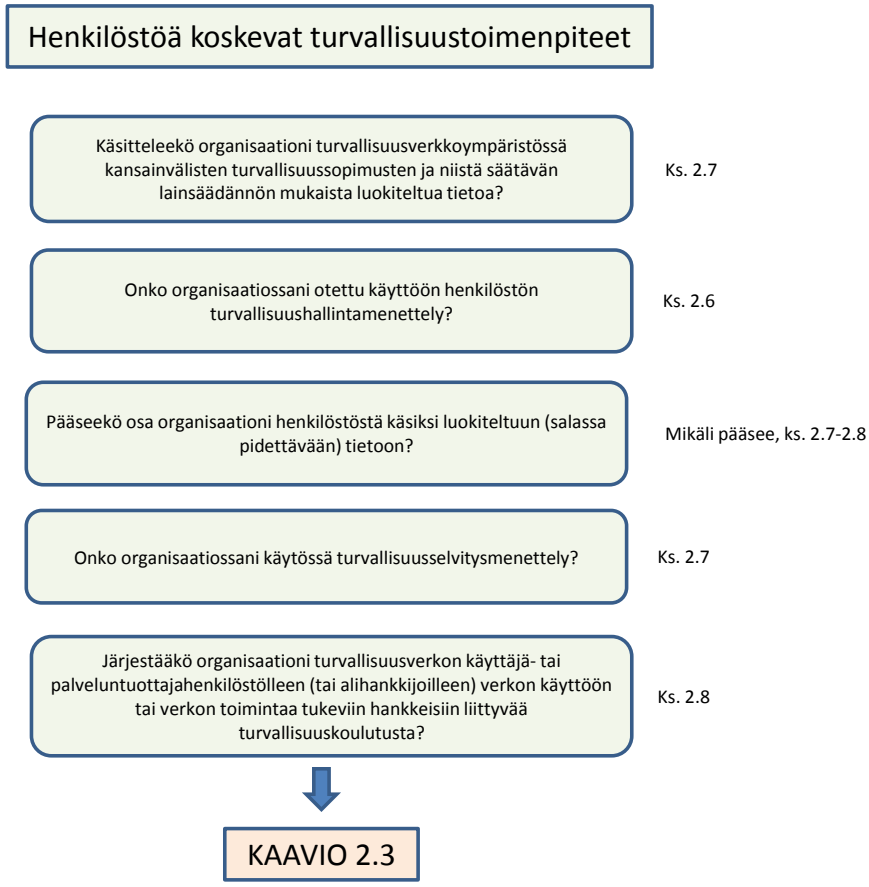
Turvallisuusohjeisto

Organisaation turvallisuuspolitiikassa ilmaistujen linjausten viemiseksi käytäntöön organisaatio tuottaa yksityiskohtiin menevän turvallisuusohjeiston. Sen sisällöstä ei ole valtionhallinnossa nimenomaista kirjallista ohjausta. Turvallisuusohjeiston merkitys organisaation turvallisuushallinnalle on keskeinen ja joitakin yhteisiä linjauksia on tunnistettavissa eri lähteistä:

- Turvallisuusohjeisto asettaa turvallisuudelle tavoitetason ja kyseisen tason saavuttamiselle mittarit.
- Turvallisuusohjeistusta ylläpidetään ja koulutetaan dokumentoidusti
- Turvallisuusohjeiston mukaisesti toimimalla havaitaan turvallisuuspoikkeamat.

Hallinnon turvallisuusverkkohankkeessa kunkin osallistuvan toimijan itselleen tuottamilla turvallisuusohjeistoilla on keskeinen asema. Ohjeiston sisältöesimerkki on esitetty hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista solmitun sopimuksen liitteessä 2 (luku 4.5).

TUVE-KÄYTTÄJIEN JA -PALVELUNTARJOAJIEN TURVALLISUUDEN TOTEUTUS KAAVIO 2.2



2.6

Henkilöstön turvallisuushallinta

Henkilöstön turvallisuushallinta tarkoittaa käsitteenä sekä työntekijöiden henkilökohtaisesta turvallisuudesta huolehtimista (henkilöturvallisuus, *safety*), että henkilöstöstä aiheutuneista turvallisuusuhkista huolehtimista (*security*). Tiedon turvaamiseen keskittyvässä turvallisuusdokumentaatiossa (turvallisuuspolitiikka ja turvallisuusohjeisto) keskitytään jälkimmäiseen aspektiin, eli henkilöstöstä aiheutuvien riskien minimointiin.

Henkilöstö muodostaa aina työympäristön suurimman riskitekijän. Henkilöstöriskien pitäminen mahdollisimman vähäisinä edellyttää sitä, että henkilöstöturvallisuudesta huolehditaan koko työsuhteen ajan ja osittain jo ennen sen solmimista. Niiden työtehtävien osalta, joihin liittyy luokitellun tiedon käsittelyä, varataan työnhakuilmoituksissa mahdollisuus turvallisuusselvityksiin ennen työsuhteen vakinaistamista. Turvallisuusverkon käyttöoikeus rajataan kirjallisella erillispäätöksellä ainoastaan niille, joiden työtehtäviin verkon käyttö oleellisesti liittyy. Työsuhteen aikana huolehditaan henkilöstön työhyvinvoinnista ja tätä kautta työtyytyväisyydestä. Jatkuvalla turvallisuuskoulutuksella aikaansaadaan turvallisuuskulttuurin kehittyminen sille tasolle, että työntekijäkunta kykenee itse tunnistamaan pääosan uhkaavista riskeistä ja toimimaan aktiivisesti niiden minimoimiseksi. Tietoturvarikkomukset käsitellään etukäteen sovitun prosessin mukaisesti. Työsuhteen päättyessä korostetaan työyhteisöstä poistuvalle henkilölle salassapitovelvoitteen jatkumista.

Lähteitä:

- Johdon tietoturvaopas, VAHTI 2/2011
- Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- ISO/IEC 27002
- PCI DSS 12.3
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki yhteistoiminnasta yrityksissä (334/2007)
- Työsopimuslaki (55/2001)
- Henkilötietolaki (523/1999)
- Luottotietolaki (527/2007)
- Kansallinen turvallisuusauditointikriteeristö: A700- A800, P100-P600.

2.7

Henkilöstön turvallisuusselvitykset

Henkilön menneisyyttä selvittämään pyrkivät taustaselvitykset ovat käytetyin henkilöstöturvallisuuden menetelmä. Selvitysten toteutus vaihtelee maittain. Suomessa henkilöturvallisuusselvitykset perustuvat lähinnä henkilöstä kertyneeseen viranomaisten hallussa olevaan rekisteritietoon. Turvallisuusselvitysten hakijatahona toimii henkilön työyhteisö eli se organisaatiotaho, jolla on intressi saada selvitys henkilön taustasta. Intressi voi olla puhtaasti lakisääteinen tai johtua esimerkiksi turvallisuusverkkoympäristöön liittyvästä kansainvälisestä hankkeesta.

- Suppea turvallisuusselvitys laaditaan yleisimmin tapauksissa, joissa kohdehenkilölle ollaan myöntämässä pääsy sellaiseen tilaan, jossa käsitellään salassa pidettäviä asioita. Selvitys tehdään tyypillisesti paikallispoliisin toimesta.
- Perusmuotoinen turvallisuusselvitys laaditaan henkilöistä, joille ollaan myöntämässä pääsy salassa pidettävään tietoon. Selvitys tehdään tyypillisesti suojelupoliisin toimesta.
- Laaja turvallisuusselvitys laaditaan henkilöstä, jolle ollaan myöntämässä pääsy muutoin kuin satunnaisesti korkeimpien suojaustasojen (ST II ja ST I) mukaiseen salassa pidettävään tietoon. Selvitys tehdään suojelupoliisin toimesta.

Mikäli henkilöön kohdistuva turvallisuusselvitys laaditaan kansainvälisen tietoturvallisuusvelvoitteen johdosta, määrittää hakijamaan viranomainen selvityksen tavoitetason. Tason määreenä käytetään yleensä suojaustasoa osoittavaa kansainvälistä turvallisuusluokitusmerkintää (CONFIDENTIAL, SECRET, TOP SECRET). Toimivaltainen viranomainen laatii selvityksen kansainväliseen turvallisuussopimukseen perustuen ja toimittaa selvityksen tuloksen tiedoksi ulkomaiselle viranomaiselle. On huomattava, että turvallisuusselvitys voidaan erityistapauksissa laatia myös ulkomaalaisesta henkilöstä, mikäli tämä on asunut toimivaltaisten viranomaisten tulkinnan mukaan riittävän pitkään siinä maassa, jonka viranomaisilta selvitystä haetaan.

Lähteitä:

- Turvallisuusselvityslaki (177/2002)
- Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- Suojelupoliisin ohje turvallisuusselvitysmenettelyn piiriin hakeutumisesta (www.poliisi.fi > Suojelupoliisi > Turvallisuus > Henkilöturvallisuusselvitykset)
- Työsopimuslaki (55/2001)
- Henkilötietolaki (523/1999)
- Luottotietolaki (527/2007)
- Kansallinen turvallisuusauditointikriteeristö, P400-osio.

2.8

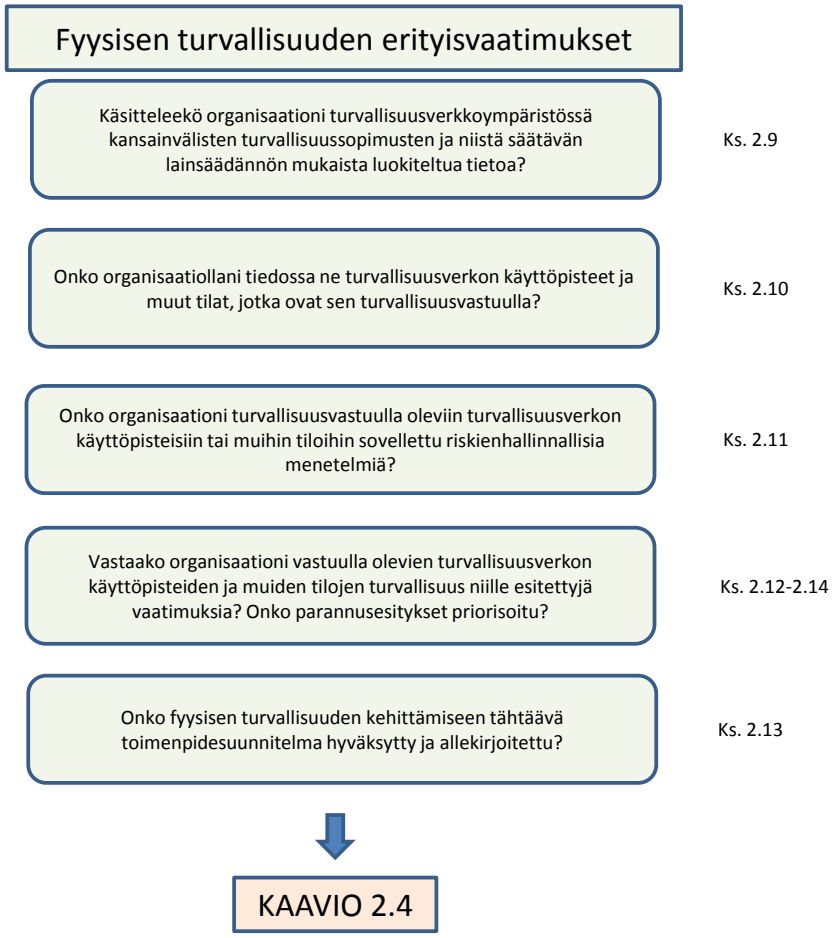
Henkilöstön turvallisuuskoulutus

Hallinnon turvallisuusverkkohankkeen turvallisuusperiaatteet koulutetaan vastuuhenkilöiden toimesta koko sille henkilöstölle, joka toimii verkon palveluiden käyttäjänä tai palveluiden tuottajana. Hyväksytysti läpikäyty koulutus on edellytys turvallisuusverkon pääsyoikeuden myöntämiselle. Alihankkijoiden turvallisuuskoulutus toteutetaan organisaation turvallisuusohjeiston mukaisesti ja sen laajuisena kuin alihankintatyö edellyttää (pääsy tiloihin/pääsy tietoon). Koulutustapahtumien ajankohta ja sisältö dokumentoidaan. Lisä- tai päivityskoulutustarvetta arvioidaan organisaation turvallisuusdokumentaatiossa määritetyin väliajoin, mutta vähintään vuosittain.

Lähteitä:

- Johdon tietoturvaopas, VAHTI 2/2011
- Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- ISO/IEC 27002
- PCI DSS 12.6
- COBIT 4.1
- Kansallinen turvallisuusauditointikriteeristö: A100, A400, A700, A800, P100, P500.

TUVE-KÄYTTÄJIEN JA -PALVELUNTARJOAJIEN TURVALLISUUDEN TOTEUTUS KAAVIO 2.3



2.9

Fyysiseen turvallisuuteen kohdistuvat kansainväliset vaatimukset
Fyysisen turvallisuuden toteutustason määrittävät taustaselvitykset ovat yleisiä kansainvälisissä hankkeissa. Tällainen erityisesti tilaan ja sen turvallisuushallintaan kohdistuva turvallisuustodistus kantaa nimeä *Facility Security Clearance*. Suomessa näistä turvallisuusselvityksistä ja -todistuksesta käytetään joko vanhempaa termiä ”yhteisöturvallisuusselvitys/todistus” tai uudempaa termiä ”yritysturvallisuusselvitys/todistus” riippumatta siitä, onko selvityksen kohteena julkisyhteisö vai yritys.

Selvitysten toteutus vaihtelee maittain. Suomessa yritysturvallisuusselvitysten mukaiset tarkastukset toteutetaan toimivaltaisten viranomaisten suorittamina auditointeina sen jälkeen, kun viranomaiset katsovat selvityksen kohteen olevan valmis kyseisiin tarkastuksiin. Valmiuden osoituksena on tyypillisesti riittävällä tarkkuudella aikaansaatu turvallisuusohjeisto ja sen toteutumisesta vastaava turvallisuusorganisaatio.

Kansainvälisen yritysturvallisuusselvitysten hakijatahona toimii sen maan viranomainen, jonka luokiteltua (salassa pidettävää) tietoa yhteishankkeessa liikkuu. Mikäli yritykseen kohdistuva turvallisuusselvitys laaditaan kansainvälisen tietoturvallisuusvelvoitteen johdosta, määrittää hakijamaan viranomainen selvityksen tavoitetason. Tason määreenä käytetään yleensä suojaustasoa osoittavaa kansainvälistä turvallisuusluokitusmerkintää (CONFIDENTIAL, SECRET, TOP SECRET). Toimivaltainen viranomainen laatii selvityksen kansainväliseen turvallisuussopimukseen perustuen ja toimittaa selvityksen tuloksen tiedoksi ulkomaiselle viranomaiselle. On huomattava, että yritysturvallisuusselvitys kohdistuu aina johonkin nimettyyn tilaan tai tilakokonaisuuteen.

Lähteitä:

- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Turvallisuusselvityslaki (177/2002)
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- Kansallinen turvallisuusauditointikriteeristö, F-osio
- Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje (Ulkoasiainministeriö 2010)
- Kansallisen turvallisuusviranomaisen käsikirja yrityksille (Ulkoasiainministeriö 2011).

2.10

Turvallisuusverkon käyttöön liittyvät tilat

Turvallisuusverkkoon välittömästi kuuluvat laitetilat ja laitteet omistaa tai niitä hallitsee Suomen valtio. Valtion omistuksessa olevien laitetilojen ja laitteiden omistus-, hallinta- tai käyttöoikeus voidaan kuitenkin luovuttaa valtion kokonaan omistamalle yhtiölle (HE54/2013/TuveL 5§). Rakennustyön viranomaisvalvonta ei koske turvallisuusverkkotoimintaa varten toteutettavaa rakentamista (HE54/2013/TuveL 24§).

Turvallisuusverkon käyttöpisteiden ja muiden turvallisuusverkon käyttöön liittyvien tilojen turvallisuusvastuu kuuluu sille organisaatiolle, joka niitä hallinnoi. Vastuista sovitaan erillisin yhteistoimintasopimuksin. Mikäli turvallisuusverkon käyttäjien tai palveluntuottajien keskuudessa on edellä mainittujen vastuiden osalta epäselvyyttä, ratkaisee valtiovarainministeriö epäselvyydet turvallisuusverkkotoiminnan neuvottelukunnan esittelystä (ks. HE54/2013/TuveL 16-17§ sekä sopimus hallinnon turvallisuusverkon turvallisuusperiaatteista, liite 2: kuva 2).

2.11

Turvallisuusverkon käyttöön liittyviin tiloihin kohdistetut riskienhallintatoimenpiteet

Turvallisuusverkon käyttöpisteisiin ja muihin tiloihin sovelletaan samaa riskienhallinnan yleisperiaatetta kuin verkkokokonaisuuteen (ks. edellä 2.3). Niiden tilojen osalta, joiden luokittelussa ja tästä johtuen rakenteellisissa vaatimuksissa esiintyy vastuuorganisaatioiden välisiä epäselvyyksiä, noudatetaan edellä kappaleessa 2.2.3 kuvattua luokittelumenettelyä. Mikäli vastuuorganisaatiot eivät pääse luokittelusta yhteisymmärrykseen, ratkaisee valtiovarainministeriö epäselvyydet turvallisuusverkkotoiminnan neuvottelukunnan esittelystä.

2.12

Turvallisuusverkon käyttöön liittyvien tilojen turvallisuusvaatimukset

Turvallisuusverkon tilojen turvallisuusvaatimuksiin sovelletaan kulloinkin ajantasaisinta ohjeistusta kuitenkin siten, että tilojen tultua määrätyn turvallisuusviranomaisen toimesta hyväksytysti tiettyyn turvallisuustasoon, on hyväksyntä voimassa viisi vuotta huolimatta tänä aikana mahdollisesti muuttuneista vaatimuksista. Valtiovarainministeriö voi hyväksyä poikkeuksen tästä säännöstä painavista syistä turvallisuusverkkotoiminnan neuvottelukunnan esittelystä.

Lähteitä:
- Toimitilojen tietoturvaohje, VAHTI 2/2013
- Kansallinen turvallisuusauditointikriteeristö, P-osio.

2.13

Turvallisuusverkon käyttäminen hyväksyttyjen tilojen ulkopuolelta

Mikäli turvallisuusverkon palveluita ollaan toiminnan luonteen vuoksi pakotettuja käyttämään hyväksyttyjen tilojen ulkopuolelta, tulee käyttäjän yhdessä organisaationsa kanssa huolehtia siitä, että työskentely-ympäristö täyttää turvallisuusverkon käyttämiselle esitetyt vaatimukset ottaen huomioon kulloinkin käsiteltävän aineiston suojaustason. Suojaustasoon IV kuuluvia asiakirjoja voidaan käsitellä tilapäisissä työskentely-ympäristöissä uhkaympäristö asianmukaisesti huomioon ottaen ilman erillisiä fyysisiä turvallisuustoimia. Mikäli vähintään suojaustasoon III kuuluvaa aineistoa käsitellään tai säilytetään organisaation toimitilojen ulkopuolella, ei kyseisen tilan turvallisuustoimia voida mitoittaa satunnaistyöskentelyn mukaisiksi. Mahdolliset jäännösriskit täytyy hyväksyä tapauskohtaisesti ja kirjallisesti työyksikön turvallisuusohjeistuksessa kuvatulla menettelyllä. Valtiovarainministeriö ratkaisee tarvittaessa tapaukset turvallisuusverkkotoiminnan neuvottelukunnan esityksestä.

Kuljetettaessa luokiteltuja tietoja pääasiallisen toimipisteen ja etätyöpisteen välillä, on huolehdittava tietoaineiston turvallisuudesta joko kuriiritoiminnan keinoin tai esimerkiksi salassa pidettävää tietoaineistoa sisältävien muistimedioiden asianmukaisella salauksella.

2.14

Liikkuva työ

Liikkuvaan työhön liittyy korostunut ja jatkuva uhka-arviointitarve. Käsiteltäessä vähintään suojaustasoon III luokiteltuja tietoja liikkuvassa työympäristössä, tulee hallinnonalan tai organisaation itsensä antaa asiasta erilliset fyysisen turvallisuuden soveltamisohjeet, jotka tähtäävät jäännösriskien minimoimiseen.

2.15

Turvallisuusverkon käyttöön liittyvien tilojen fyysisen turvallisuuden kehityssuunnitelma

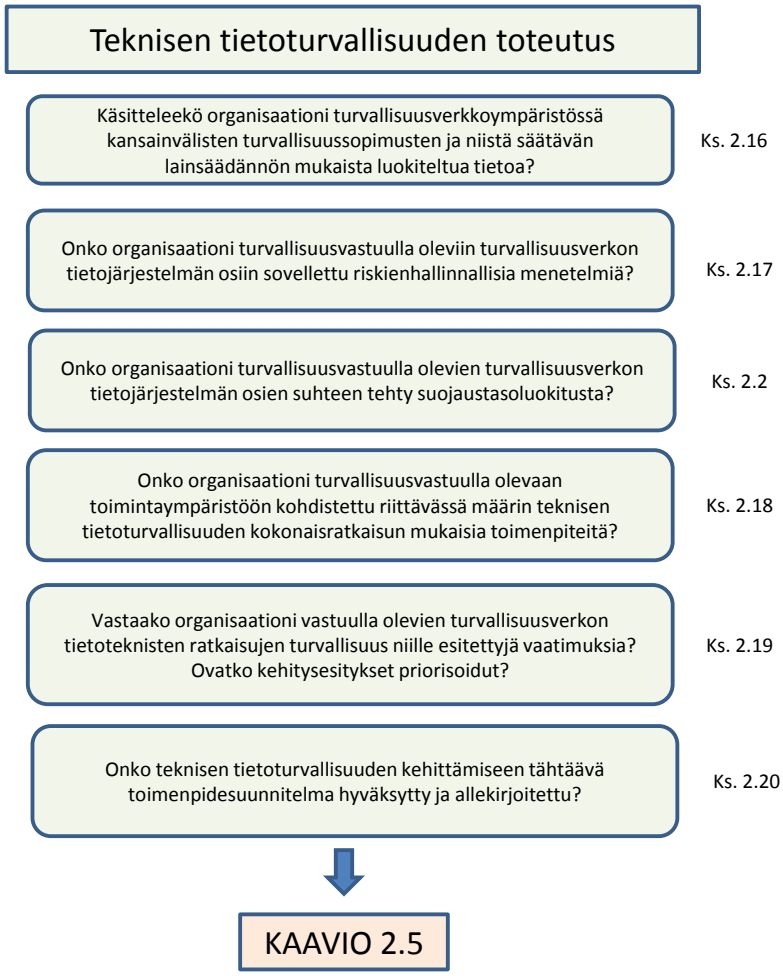
Havaittaessa, ettei käytössä olevien tilojen fyysinen turvallisuus täytä vaatimuksia, laaditaan asian kuntoon saattamista ohjaamaan kehityssuunnitelma. Kehityssuunnitelman allekirjoittaa budjettivastuussa oleva esimies ja se esitellään turvallisuusverkkotoiminnan neuvottelukunnalle. Esittelevä taho on velvollinen raportoimaan vuosittain kehityssuunnitelman toteutumisesta. Mikäli toimivaltainen turvallisuusviranomainen niin tulkitsee, se voi myöntää tilalle tilapäisen käyttöluvan kehityssuunnitelmaan ja mahdollisiin pikaisiin korjaaviin toimenpiteisiin perustuen.

Lähteitä:

- Toimitilojen tietoturvaohje, VAHTI 2/2013
- Kansallinen turvallisuusauditointikriteeristö, P-osio.

TUVE-KÄYTTÄJIEN JA -PALVELUNTARJOAJIEN TURVALLISUUDEN TOTEUTUS

KAAVIO 2.4



2.16

Tekniseen tietoturvallisuuteen kohdistuvat kansainväliset vaatimukset
Teknisen tietoturvallisuuden toteutustaso määräytyy kansainvälisistä alkuperää olevan luokitellun tiedon käsittelytapauksissa joko kansainvälisten turvallisuussopimusten tai käyttötarkoitukseen erikseen sovittujen turvallisuussäännöstöjen kautta. Suomessa toimivaltaisena yhteys- ja tarkastusviranomaisena toimii Viestintäviraston NCSA-yksikkö, joka toimii tietojärjestelmien kansallisena hyväksyntätahona.

Ennen Viestintäviraston hyväksyntäprosessin käynnistymistä organisaation halutaan tuottavan hyväksyntäviranomaisen käyttöön seuraavat dokumentit:
- vaatimusmäärittely, erityisesti SSRS (System-Specific Security Requirements Statement)
- verkkokuvat
- lista käytetyistä käyttöjärjestelmistä ja ohjelmistoista versiotietoineen
- tiedot mahdollisista aikaisemmista tarkastuksista ja/tai hyväksynnistä raportteineen

Ideaalitilanteessa dokumenteista selviää verkon rakenne, IP-osoitteet, vyöhykkeet, segmentit, palomuurisäännöstöt, verkkolaitteiden käyttöjärjestelmä-/firmware-versiot, palvelinten ja tuotantojärjestelmien ohjelmistoversiot ja asetukset, ja muut vastaavat tiedot sillä tarkkuudella, että niiden perusteella ulkopuolinen pystyy saattamaan vikaantuneet verkot ja järjestelmät käyttökuntoon.

Siirrettävän tiedon luokittelusta riippuen saattaa kansainvälinen osapuoli varata itselleen hyväksyntämahdollisuuden. Tällöin isäntäviranomainen (Viestintävirasto) ja kansainvälinen osapuoli valmistelevat yhteistyössä (akreditointipaneeli) yksityiskohtaisen akreditointisuunnitelman, joka tyypillisesti myös toteutetaan yhteisesti, kuitenkin taustalla olevan sopimuksen sisällöstä riippuen.

Lähteitä:
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

2.17

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
Riskien arviointi on osa organisaation riskien hallintaa. Riskien arvioinnilla tarkoitetaan niitä suunnitelmallisia toimenpiteitä, joilla pyritään tunnistamaan uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Riskejä hallittaessa ja arvioitaessa työhön tulee sisällyttää varautuminen normaaliolojen häiriötilanteisiin sekä organisaation valmiusvelvoitteiden mukaisesti myös poikkeustiloihin.

VAHTI-ohjeessa 7/2003 on esitetty välineitä ja keinoja, joiden avulla tietoriskejä voidaan arvioida. Ohjeessa kuvataan myös riskienhallintaan kohdistuvia velvoitteita, riskien arvioinnin merkitystä ja organisointia sekä riskienhallinnan keinoja, uhkien tunnistamista, riskien suuruuden arviointia, toimenpiteiden määrittelyä ja jatkokehitystä. Riskien arvioinnin menetelminä voidaan käyttää muun muassa ohjeen luvussa 3 kuvattuja menetelmiä. Ohjeen liitteenä on tarkistuslista tietoturvauhkien tunnistamiseksi. On tärkeää tunnistaa tehtyjen analyysien kautta uhkan todennäköisyys ja seurausten vakavuus.

Huom! Sopimus hallinnon turvallisuusverkon turvallisuusperiaatteista edellyttää, että turvallisuusverkkoympäristöön hyväksyttävät *alihankkijat* täyttävät säädösten lisäksi sopimuksen mukaiset turvallisuusvaatimukset. Toimivaltaiset turvallisuusviranomaiset tarkastavat näiden velvoitteiden toteutumisen. Velvoitteiden täyttyminen ja toteutuksen tarkastaminen tapahtuu oikein perustein ainoastaan silloin, kun nimenomaisen kohteen riskiympäristö on arvioitu ennen uhkia torjuvien turvallisuustoimenpiteiden käynnistämistä.

Muita lähteitä:
- ISO 31000:2009 - Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- Kansallinen turvallisuusauditointikriteeristö, A400-osio, I700-osio.

2.18

Turvallisuusverkon teknisen tietoturvallisuuden kokonaisratkaisun soveltaminen

Tekninen tietoturvallisuus on osa turvallisuusverkon kokonaisturvallisuutta. Teknistä tietoturvallisuutta kehitettäessä otetaan huomioon teknisen tietoturvallisuuden erillisvaatimusten lisäksi esim. sellaiset hallinnolliset turvallisuustoimet, jotka vaikuttavat teknisen tietoturvallisuuden vastuukentän hallintaan tai tukevat sitä.

Teknisen tietoturvallisuuden toteutussuunnitelmaa laadittaessa vastuutahot tekevät kiinteää yhteistyötä muiden turvallisuuden osa-alueiden vastuutahojen kanssa.

Lähteitä:

- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- Kansallinen turvallisuusauditointikriteeristö (kokonaisuudessaan)
- Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje (Ulkoasiainministeriö 2010)
- Kansallisen turvallisuusviranomaisen käsikirja yrityksille (Ulkoasiainministeriö 2011).

2.19

Turvallisuusverkon tietoteknisten ratkaisujen vaatimusmäärittely

Turvallisuusverkon tietoteknisten ratkaisujen turvallisuus on avaintekijä paitsi verkossa siirrettävän tiedon luottamuksellisuuden takaamiseksi, myös turvallisuusverkon käytettävyyden varmistamiseksi.

Turvallisuusverkon tietoteknisiä ratkaisuja määritettäessä turvallisuusvaatimukset on huomioitava keskeisenä elementtinä sekä verkon arkkitehtuurityössä, että sitä tukevissa ratkaisuissa. Turvallisuusverkon turvallisuuspolitiikan määritelmien lisäksi vaatimustietämystä täydennetään keskustelemalla suunnitteilla olevista ratkaisumalleista vastuuviranomaisten kanssa etukäteen. Täten varmistutaan vaatimustenmukaisuudesta kustannustehokkaalla tavalla.

Havaittaessa jo tehtyjen ratkaisujen suhteen kehittämistarpeita, nämä priorisoidaan toisiinsa nähden tarvittaessa turvallisuusviranomaisnäkemystä hyödyntäen. Mikäli puutteiden korjaamisen vastuiden tai muiden seikkojen osalta esiintyy epätietoisuutta, ratkaisee valtiovarainministeriö epäselvyydet turvallisuusverkkotoiminnan neuvottelukunnan esittelystä.

Lähteitä:

- Suomen kyberturvallisuusstrategia, VNp 24.1.2013
- Johdon tietoturvaopas, VAHTI 2/2011
- ISO/IEC 27002
- PCI DSS 12
- COBIT 4.1
- Kansallinen turvallisuusauditointikriteeristö

2.20

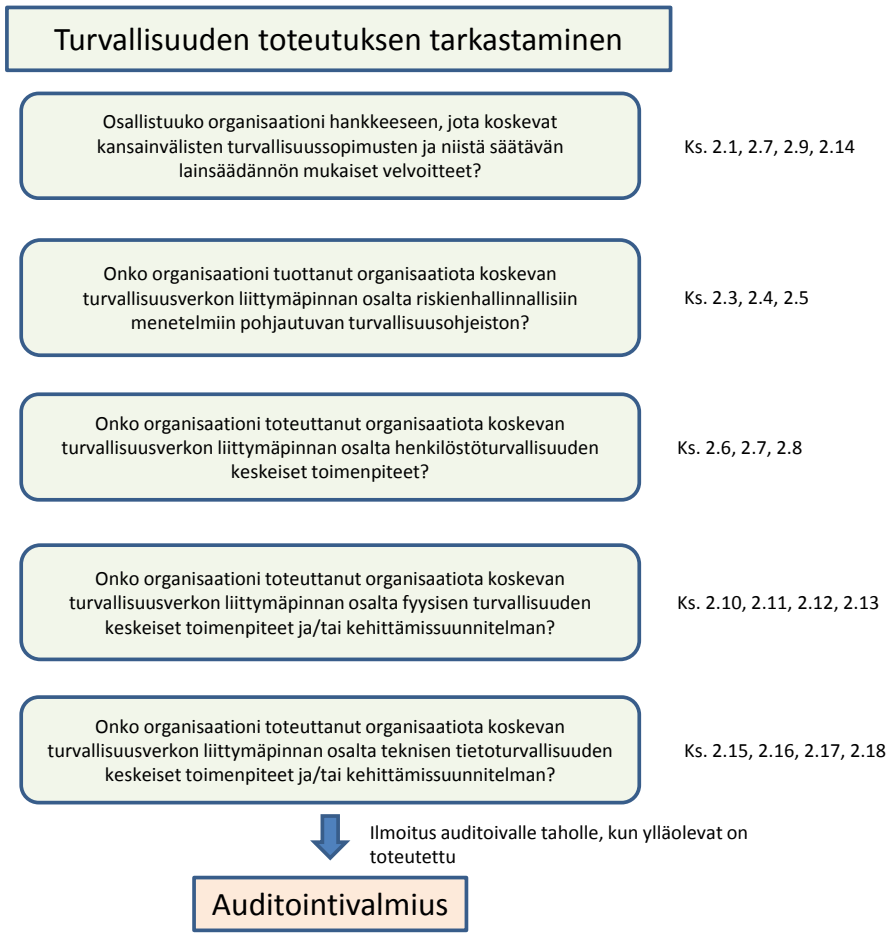
Turvallisuusverkon teknisen tietoturvallisuuden kehittäminen (toimenpidesuunnitelma)

Hallinnon turvallisuusverkon teknistä tietoturvallisuutta kehitetään sen mukaisesti, mitä on sovittu turvallisuusverkon turvallisuusperiaatteista (HE54/2013/TuveL 16§). Valtiovarainministeriö vastaa hallinnon turvallisuusverkkotoiminnan tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta. Tieto- ja tietoliikenneturvallisuuden jatkuva kehittäminen ja ajantasaisuus ovat verkon yleisen luotettavuuden kannalta ensiarvoisessa asemassa. Jotta tietoturvallisuuden jatkuva kehittäminen olisi mahdollista vaaditulla tasolla, noudatetaan verkon hallinnasta vastaavien viranomaistahojen ja palveluntuottajien kesken jatkuvan kehityksen periaatetta siten kuin valtiovarainministeriö ja turvallisuusverkkotoiminnan neuvottelukunta erikseen linjaavat.

Muita lähteitä:
- Sopimus hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista (liite 2: luku 1)
- Hallinnon turvallisuusverkon politiikka
- Hallinnon turvallisuusverkon varautumispolitiikka
- Hallinnon turvallisuusverkon tietoturvapolitiikka
- Hallinnon turvallisuusverkon tietoliikennepolitiikka
- ISO/IEC 27002
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010
- Kansallinen turvallisuusauditointikriteeristö, A500-A600 osiot.

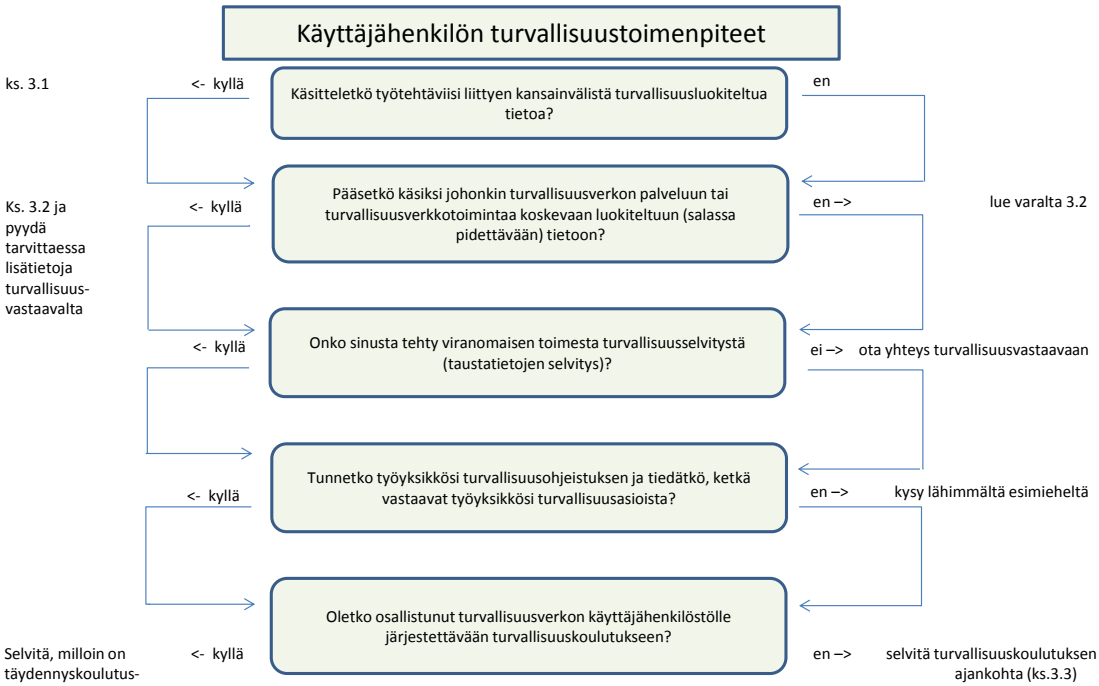
TUVE-KÄYTTÄJIEN JA -PALVELUNTARJOAJIEN TURVALLISUUDEN TOTEUTUS

KAAVIO 2.5



Liite 3

Verkon loppukäyttäjien turvallisuuden toteutus



Loppukäyttäjän turvallisuustoimien toteutus turvallisuusverkkoympäristössä

3. Yleistä

Hallinnon turvallisuusverkon käyttäjiä ja palveluntarjoajia sitovat turvallisuusverkkotoiminnan turvallisuuden toteutuksesta solmitun sopimuksen mukaiset velvoitteet. Sopimus, joka välillisesti koskee siis myös verkon toteutukseen osallistuvia kaupallisia toimijoita, määrittää kokonaisturvallisuuden näkökulmasta ne vähimmäistoimet, jotka turvallisuusverkkoon tavalla tai toisella liittyvän organisaation tulee täyttää. Työyksikön turvallisuusvastaava kouluttaa sopimuksen mukanaan tuomat velvoitteet ja muut turvallisuusvaatimukset jokaiselle verkon loppukäyttäjälle.

Tällä lyhyellä ohjeella pyritään helpottamaan turvallisuustoimien sisällön ymmärtämistä verkon loppukäyttäjien keskuudessa.

3.1

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Kansainvälisellä tietoturvallisuusvelvoitteella tarkoitetaan sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä.

Kansainvälisessä tietoturvalaissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

Loppukäyttäjän osalta on merkittävää, että hänelle on myönnetty kirjallisesti lupa päästä käsiksi kansainväliseen luokiteltuun tietoaineistoon ja että hänestä on tehty asianmukainen turvallisuusselvitys. Se salassa pidettävä tieto, minkä työntekijä saa tietoonsa työtehtäviinsä liittyen, tulee pitää salassa myös sen jälkeen kun työsuhde on päättynyt (Julkisuuslaki).

3.2. Luokittelu

Tietoturvallisuusasetus
Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Tietoturvallisuusasetuksen mukaisesti valtionhallinnon salassa pidettävä tieto voidaan luokitella neljään suojaustasoon ja erityisistä syistä (valtion turvallisuus, kansainväliset suhteet, maanpuolustus jne.) johtuen varustaa turvallisuusluokitusmerkinnällä. Tämän mukaisesti luokittelun periaate on yksinkertaistettuna seuraava:

Suojaustaso	Turvallisuusluokitusmerkintä	Mitä tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa?
Suojaustaso IV	KÄYTTÖ RAJOITETTU	Haittaa yleiselle tai yksityiselle edulle, viranomaisen toimintaedellytysten heikentymistä
Suojaustaso III	LUOTTAMUKSELLINEN	Vahinkoa yleiselle tai yksityiselle edulle
Suojaustaso II	SALAINEN	Merkittävää vahinkoa yleiselle edulle
Suojaustaso I	ERITTÄIN SALAINEN	Erityisen suurta vahinkoa yleiselle edulle

3.3

Henkilöstön turvallisuuskoulutus

Hallinnon turvallisuusverkkohankkeen turvallisuusperiaatteet koulutetaan vastuuhenkilöiden toimesta koko sille henkilöstölle, joka toimii verkon palveluiden käyttäjänä tai palveluiden tuottajana. Hyväksytysti läpikäyty koulutus on edellytys turvallisuusverkon eritasoisten pääsyoikeuksien myöntämiselle. Alihankkijoiden turvallisuuskoulutus toteutetaan toimeksiantajan turvallisuusohjeiston mukaisesti ja sen laajuisena kuin alihankintatyö edellyttää (pääsy tiloihin/pääsy tietoon). Koulutustapahtumien ajankohta ja sisältö dokumentoidaan. Lisä- tai päivityskoulutustarvetta arvioidaan organisaation turvallisuusdokumentaatiossa määritetyin väliajoin, kuitenkin vähintään vuosittain.

Lähteitä:

- Johdon tietoturvaopas, VAHTI 2/2011
- Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- ISO/IEC 27002
- PCI DSS 12.6
- COBIT 4.1
- Kansallinen turvallisuusauditointikriteeristö: A100, A400, A700, A800, P100, P500.

VM:N JULKAISUSARJAN TEEMAT:

Budjetti

Hallinnon kehittäminen

ICT-toiminta

Kunnat

Ohjaus ja tilivelvollisuus

Rahoitusmarkkinat

Taloudelliset ja talouspoliittiset katsaukset

Valtion työmarkkinalaitos

Verotus

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 16001
Telefaksi 09 160 33123
www.vm.fi

18/2013
Valtiovarainministeriön julkaisuja
Elokuu 2013

ISSN 1459-3394 (nid.)
ISBN 978-952-251-474-5 (nid.)
ISSN 1797-9714 (pdf)
ISBN 978-952-251-475-2 (pdf)