VALTIOVARAINMINISTERIÖ

TUVEn turvallisuus-koulutusohje

19/2013 ICT-toiminta

VALTIOVARAINMINISTERIÖ

Hallinnon turvallisuusverkkotoiminnan turvallisuuskoulutuksen toteutusohje

Valtiovarainministeriön julkaisuja

19/2013 ICT-toiminta

441 729
Painotuote

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

Juvenes Print - Suomen Yliopistopaino Oy, 2013

Kuvailulehti

Julkaisija ja julkaisuaika	Valtiovarainministeriö, heinäkuu 2013	
Tekijät	Turvallisuussopimushanke, Ohjausryhmän pj Esko Vainio VM, sihteeri Sami Kilkkilä ERVE	
Julkaisun nimi	Hallinnon turvallisuusverkkotoiminnan turvallisuuskoulutuksen toteutusohje	
Asiasanat	Koulutus, verkko-opetus, verkko-oppimateriaali, turvallisuussuunnittelu, tietoliikenneverkot	
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 19/2013	
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- 952-251-476-9 (nid.) **ISSN** 1459-3394 (nid.) **ISBN** 978-952-251-477-6 (PDF) **ISSN** 1797-9714 (PDF)	**Sivuja** 36	**Kieli** Suomi

Tiivistelmä

Tämän koulutuksen toteutusohjeen tarkoituksena on esittää kootusti kaikille turvallisuusverkon käyttäjätahoille koulutettavat turvallisuusperiaatteet ja tarjota toimijaorganisaatioiden turvallisuusvastuullisille tahoille koulutussuunnitelman runko. Tämä koulutuksen toteutusohje tukee samaan aikaan julkaistavaa ohjetta hallinnon turvallisuusverkon turvallisuusperiaatteista solmitun sopimuksen toimeenpanosta.

Tämä koulutuksen toteutusohje toimii apuvälineenä turvallisuusperiaatteiden käytännön koulutustyössä. Kunkin organisaation on syytä valmistella tämän aineiston opetuspäämäärää tukemaan organisaation omaan toimintaympäristöön ja yksilöllisiin riskienhallinnallisiin toimiin perustuva tarkennettu koulutusosio.

Presentationsblad

Utgivare och datum	Finansministeriet, juli 2013	
Författare	Säkerhetsavtalsprojektet, styrgruppens ordförande Esko Vainio, FM, sekreterare Sami Kilkkilä, ERVE	
Publikationens titel	Hallinnon turvallisuusverkkotoiminnan turvallisuuskoulutuksen toteutusohje	
Publikationsserie och nummer	Finansministeriet publikationer 19/2013	
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 978-952-251-476-9 (hft.) **ISSN** 1459-3394 (hft.) **ISBN** 978-952-251-477-6 (PDF) **ISSN** 1797-9714 (PDF)	**Sidor** 36	**Språk** Finska

Sammandrag

Syftet med denna verkställighetsanvisning för utbildningen är att ge samtliga parter som använder säkerhetsnätet en koncentrerad redovisning över säkerhetsprinciperna som ska läras ut, och att erbjuda aktörsorganisationernas säkerhetsansvariga parter en stomme till utbildningsplanen. Denna verkställighetsanvisning för utbildningen stödjer även anvisningen om verkställandet av säkerhetsprinciperna för förvaltningens säkerhetsnät som ges ut samtidigt.

Denna verkställighetsanvisning för utbildningen fungerar även som ett hjälpredskap vid det praktiska utbildningsarbetet i fråga om säkerhetsprinciperna. Varje organisation bör bereda en på den egna organisationens verksamhetsomgivning och individuella riskhanteringsåtgärder baserad preciserad utbildningsdel som stödjer utbildningsmålet med detta material.

Description page

Publisher and date	Ministry of Finance, July 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	Hallinnon turvallisuusverkkotoiminnan turvallisuuskoulutuksen toteutusohje	
Publication series and number	Ministry of Finance publications 19/2013	
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 978-952-251-476-9 (print.) **ISSN** 1459-3394 (print.) **ISBN** 978-952-251-477-6 (PDF) **ISSN** 1797-9714 (PDF)	**No. of pages** 36	**Language** Finnish

Abstract

The purpose of this training implementation instruction is to present collectively the security principles to be used in the training of all security network users and to offer a training plan framework to the personnel responsible for security in actor organisations. This training implementation instruction supports another instruction, to be published simultaneously, on the implementation of the agreement on the security principles of the public sector security network.

This training implementation instruction shall serve as aid in the practical training of security principles. To support the educational objectives of this material, each organisation should prepare a more detailed training programme based on the organisation's own operating environment and individual risk-management measures.

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

Ohje VM/1448/00.00.00/2013

5.7.2013

Ministeriöille, virastoille, laitoksille ja hallinnon turvallisuusverkkotoiminnan toteutukseen osallistuville

HALLINNON TURVALLISUUSVERKKOTOIMINNAN TURVALLISUUSKOULUTUKSEN TOTETUTUSSUUNNITELMA

Tämän koulutuksen toteutussuunnitelman tarkoituksena on esittää kootusti kaikille turvallisuusverkon käyttäjätahoille koulutettavat turvallisuusperiaatteet ja tarjota toimijaorganisaatioiden turvallisuusvastuullisille tahoille koulutussuunnitelman runko. Tämä koulutuksen toteutussuunnitelma tukee samaan aikaan julkaistavaa suunnitelmaa hallinnon turvallisuusverkon turvallisuusperiaatteista solmitun sopimuksen toimeenpanosta. Kyseisen sopimuksen mukaisesti pääsyoikeus verkkoon ja/tai sen palveluihin voidaan myöntää ainoastaan sellaisille henkilöille, jotka ovat saaneet verkon käyttäjäorganisaation omaan turvallisuusohjeistoon perustuvan turvallisuuskoulutuksen. Turvallisuusohjeistot eroavat toisistaan kustakin käyttö- ja palveluympäristöstä johtuen. Tämä koulutusmateriaali on tehty ottaen huomioon kaikkia verkon toimijoita koskeva lainsäädäntö sekä ne yleisperiaatteet, joista on sovittu edellä mainitussa sopimuksessa.

Tämä koulutuksen toteutussuunnitelma toimii ohjenuorana turvallisuusperiaatteisen käytännön koulutustyössä. Kunkin organisaation on syytä valmistella tämän aineiston opetuspäämäärää tukemaan organisaation omaan toimintaympäristöön ja yksilöllisiin riskienhallinnallisiin toimiin perustuva tarkennettu koulutusosio.

Koulutuksen toteutussuunnitelma on pyritty laatimaan yksinkertaiseen muotoon kuitenkin siten, että soveltamalla sitä omaan toimintaympäristöönsä kukin käyttäjäorganisaatio voi olla varma siitä, ettei mitään keskeisiä turvallisuusverkon turvallisuuteen vaikuttavia elementtejä jää kouluttamatta.

Hallinto- ja kuntaministeri Henna Virkkunen

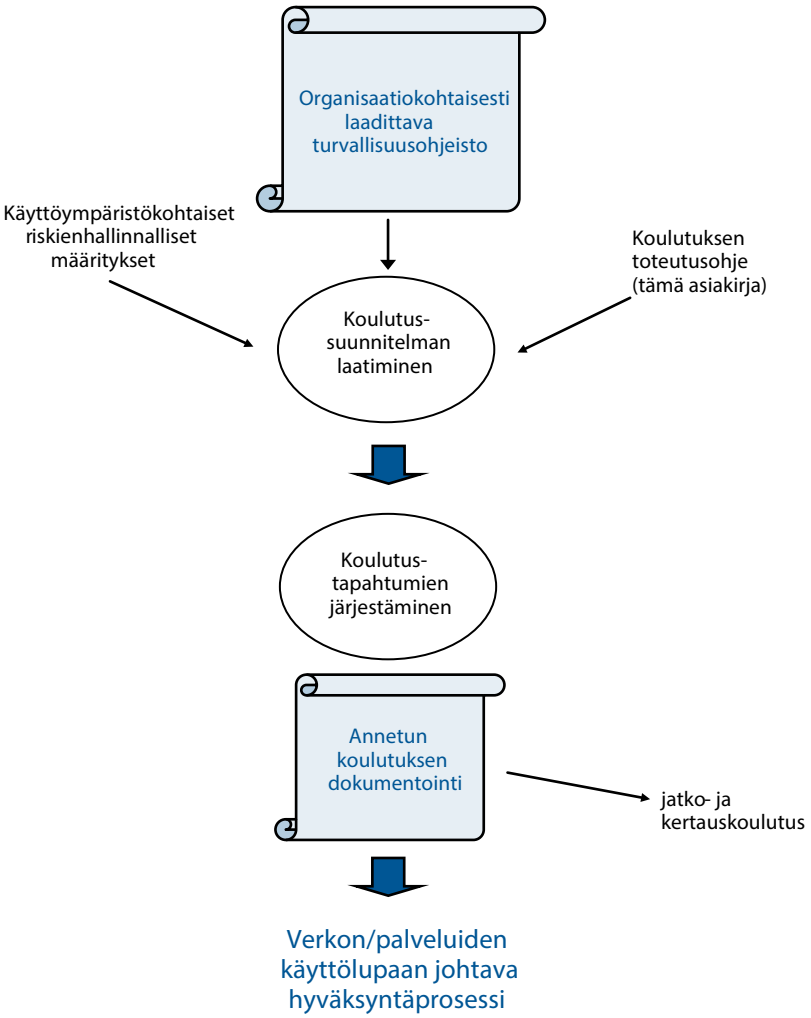
ICT-johtaja Timo Valli

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

Sisältö

1 Hallinnon turvallisuusverkon turvallisuuskoulutuksen toteutusperiaate



2 Hallinnon turvallisuusverkko-toiminnan turvallisuustoimenpiteiden koulutussuunnitelman laatiminen

Kunkin käyttäjä- tai palveluntuottajayksikön turvallisuudesta vastaava taho (turvallisuusvastaava/ turvallisuuspäällikkö tai turvallisuusyksikkö) tuottaa oman toimintansa erityispiirteet huomioon ottavan turvallisuuskoulutussuunnitelman. Koulutussuunnitelmaa laadittaessa keskeistä on määrittää, mikä on opetuksen keskeinen tavoite. Tavoitemäärittelyssä voidaan käyttää apukeinona prioriteettilistan luomista:

- mikä on tärkein opittava asia, jonka ymmärtäminen on ehdoton edellytys verkon käyttöoikeuden myöntämiselle?
- mitä osa-alueita koulutussuunnitelman tulee kattaa, jotta tavoitteen mukainen oppimistulos saavutetaan?
- onko osalle henkilöstöstä järjestettävä syventävää opetusta jonkin yksityiskohdan suhteen?

Tavoitemäärittelyn perusteella koulutuksesta vastaava taho päättää

- miten koulutus on tarkoituksenmukaista toteuttaa?
- mikä on ryhmäkoko?
- miten ryhmä on järkevää kasata?
- voiko osan koulutuksesta toteuttaa tietokoneavusteisesti?

Koulutussuunnitelman on syytä sisältää mekanismi, jolla varmistetaan opetuksen perillemeno. Tavallisin keino on testata oppimistulos perinteisellä kokeella tai tietokoneavusteisesti. Opetettujen asioiden ylläpitämiseksi organisaation turvallisuusohjeisto tai koulutussuunnitelma sisältää kannanoton jatko- tai kertauskoulutuksen järjestämisestä. Tämä otetaan huomioon myös organisaation vuosikellossa.

LIITTEET

Liite 1: turvallisuuden hallintamekanismit omassa työyhteisössä

Liite 2: henkilöstöturvallisuuden hallinta omassa työyhteisössä

Liite 3: fyysisen turvallisuuden hallinta omassa työyhteisössä

Liite 4: salassa pidettävän tiedon turvallinen hallinta omassa työyhteisössä

LIITE 1

Turvallisuuden hallintamekanismit omassa työyhteisössä

KOULUTETTAVAT KOHTEET

1. turvallisuustoimenpiteiden organisointi ja vastuut
2. turvallisuusohjeistotyön suuntaviivat
3. riskienhallintatoimenpiteiden mitoittaminen
4. luokitellun tiedon hallinta
   - 4.1 tietoturvallisuusasetuksen velvoitteet
     - 4.1.1 luokituksen perusteet
     - 4.1.2 valtionhallinnon salassapitomerkinnät
     - 4.1.3 luokitellun tiedon elinkaaren hallinta
   - 4.2 ICT-varautumisen tasomäärittelyt jatkuvuuden hallinnan ja tiedon saatavuuden varmistamiseksi
   - 4.3 hallinnon turvallisuusverkon turvallisuusperiaatteista solmitun sopimuksen keskeiset koulutusvelvoitteet

1 TURVALLISUUSTOIMENPITEIDEN ORGANISOINTI JA VASTUUT

Oppijoille tehdään selväksi oman työyhteisön turvallisuusorganisaatio ja sille annetut vastuut.

1.1 Kuka vastaa turvallisuudesta työyhteisössä?
- turvallisuudesta vastaa loppukädessä aina työyhteisön johto

1.2 Turvallisuustoimet ovat vastuutetut työyhteisön sisällä seuraavasti:
- turvallisuusjohtaminen, turvallisuuspolitiikan hyväksyminen: _____
- henkilöstöturvallisuus:_____
- tietoturvallisuus:_____
- fyysinen turvallisuus:_____.

1.3 Miten turvallisuusvastuut on dokumentoitu?
- työyhteisön intra?
- turvallisuuspolitiikka?
- turvallisuusohjeisto?

2 TURVALLISUUSOHJEISTON SISÄLTÖ

Turvallisuusohjeiston sisällöstä koulutetaan oppijoille
- työyhteisön yleiset turvallisuussäännöt ja
- turvallisuusverkkotoimintaan kohdistuvat erityiset ohjeet ja säännöt

2.1 Miten työyhteisölle mahdollisesti asetetut turvallisuuden tavoitetasot näkyvät oman organisaation turvallisuusohjeistossa?
- tiedon suojaaminen (luottamuksellisuus)
- tiedon käytettävyys ja eheys (varautuminen ja jatkuvuuden hallinta)

2.2 Miten turvallisuusohjeistoa ylläpidetään ja koulutetaan?
- vastuut,
- sitominen vuosikelloon,
- koulutuksen perillemenon varmistaminen,
- koulutuksen dokumentointi.

2.3 Mitä saavutetaan noudattamalla turvallisuusohjeiston linjauksia?
- turvallisuuspoikkeamien hallinta…

3 RISKIENHALLINTATOIMENPITEIDEN MITOITTAMINEN

Oppijoille käydään läpi organisaation toimintaympäristöön kohdistetut riskienhallintatoimenpiteet kunkin työtehtävään riittävällä tasolla. Toimenpiteet perustuvat uhka-arvioon, joka on ”toimivaltaisen viranomaisen tai muun toimijan uhkamallin pohjalta laatima, vastuullaan oleviin tehtäviin ja häiriötilanteisiin liittyvä arvio, jossa konkreettisesti käsitellään uhkan lähdettä, kohdetta, toteutumistapaa, todennäköisyyttä, vaikutuksia tehtävien hoitamiseen sekä vastatoimenpidemahdollisuuksia ja niiden valmisteluun tarvittavaa aikaa” (YTS 2010). Loppukäyttäjien osalta on syytä harkita, milloin ja millä tasolla riskienhallinnallisista toimenpiteistä informoiminen on tarpeen ja milloin informaation jakaminen luo mahdollisesti ylimääräisen riskitekijän.

Yhteiskunnan turvallisuusstrategia vuodelta 2010 jakaa riskienhallinnassa huomioitavat uhkamallit seuraavasti:
- voimahuollon vakavat häiriöt
- tietoliikenteen ja tietojärjestelmien vakavat häiriöt - kyberuhkat
- kuljetuslogistiikan vakavat häiriöt
- yhdyskuntatekniikan vakavat häiriöt
- elintarvikehuollon vakavat häiriöt
- rahoitus- ja maksujärjestelmän vakavat häiriöt

- julkisen talouden rahoituksen saatavuuden häiriintyminen
- väestön terveyden ja hyvinvoinnin vakavat häiriöt
- suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhkat
- terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus
- rajaturvallisuuden vakavat häiriöt
- poliittinen, taloudellinen ja sotilaallinen painostus
- sotilaallisen voiman käyttö.

Yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat voivat esiintyä itsenäisinä, samanaikaisina tai toistensa jatkumoina.

3.1 Mitä seikkoja organisaatiomme riskienhallinnassa on painotettu?
- luokiteltujen (=salassa pidettävien) tai sensitiivisten (=liikesalaisuudet jne.) tietojen suojaamiseksi
- toiminnan jatkuvuuden turvaamiseksi.

3.2 Mitkä kohteet on erityisesti tunnistettu suojautumistoimia vaativiksi turvallisuusverkon turvallisuutta ajatellen?
- kohteiden tärkeimmät tunnistetut uhkat (käydään läpi harkinnan varaisesti)
- kohteiden suojautumistoimien vastuuhenkilöt.

3.3 Miten riskit on priorisoitu?
- riskin konkretisoitumisen todennäköisyys vs. vaikuttavuus organisaation oman toiminnan ja koko turvallisuusverkkoympäristön kannalta.

3.4 Miten alihankkijoiden kautta tulevia riskejä hallitaan?
- mahdollinen turvallisuussopimusmenettely ennen luokitellun / sensitiivisen tiedon luovuttamista
- auditoinnit
- alihankkijalle järjestettävä turvallisuuskoulutus
- palveluiden laatutasomääritys (SLA).

3.5 Toiminta poikkeamatilanteissa
- viestintäkäytännöt havaittaessa tietoturvapoikkeama
- loppukäyttäjän omat toimenpiteet.

4 LUOKITELLUN TIEDON HALLINTA

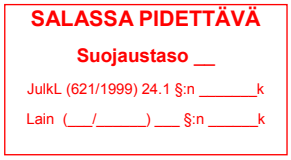
Luokitellun tiedon oikea hallinta on keskeinen turvallisuusverkon turvallisuusperiaate, jolle on syytä varata riittävästi opetusaikaa oman organisaation turvallisuuskoulutusta suunniteltaessa. Koulutuksen toteutuksessa on paikallaan huomioida työtehtävistä riippuvat eroavaisuudet opetuksen syvyydessä. Tämän turvallisuuskoulutusohjeen liitteessä 4 ohjeistetaan yksityiskohtaisemmin salassa pidettävän tiedon hallinnan kouluttamisesta niille työyhteisöille, joille syvempi asiaan perehtyminen on tarpeen.

4.1 Tietoturvallisuusasetuksen ja sitä täydentävän VAHTI 2/2010 –ohjeen keskeiset velvoitteet

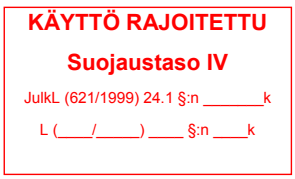
4.1.1 Luokituksen perusteet

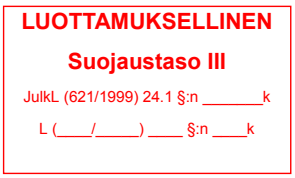
- Ohjaavana pyrkimyksenä julkisuus; ei luokitella ”varmuuden vuoksi”, vaan syystä
- Luokituspäätöksen perusteena
    - tarve salassapitoon tai
    - muu viranomaisen lakiin perustuva harkinta tai
    - tiedon paljastuminen aiheuttaisi haittaa yleiselle tai yksityiselle edulle tai heikentäisi viranomaisen toimintaedellytyksiä (ks. turvallisuussopimuksen toimeenpano-ohje, liitekaavio 3).
- Luokittelu voidaan rajoittaa koskemaan asiakirjan osia tai tiettyjä käsittelyvaiheita

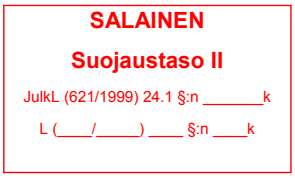
4.1.2 Valtionhallinnon salassapitomerkinnät

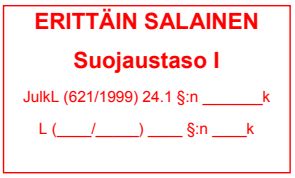


”SALASSA PIDETTÄVÄ” on yleismerkintä,
johon täydennetään suojaustaso ja –suojaamisen/luokittelun perusteena käytettävä laki ja pykälä. Perustelaki ja –pykälä täytetään myös varsinaisella turvallisuusluokitusmerkinnällä varustettuun luokitusmerkintään (käytettävät neljä merkintää alla).





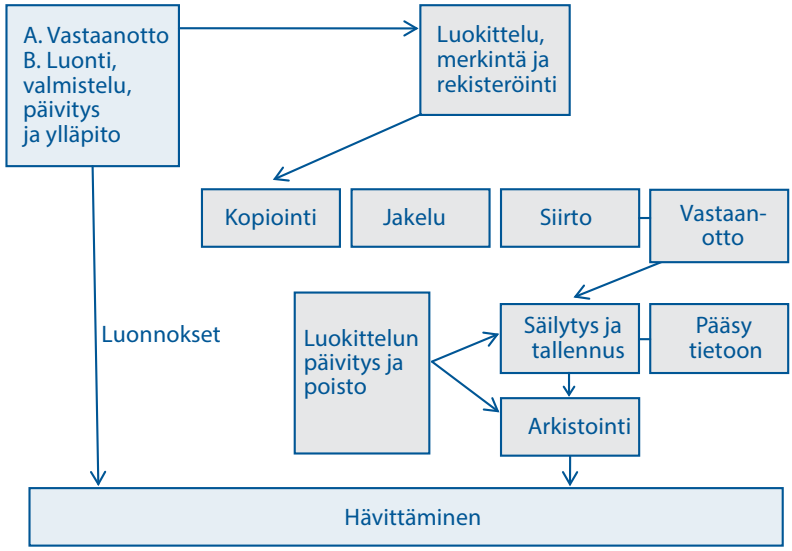




4.1.3 Luokitellun tiedon elinkaaren hallinta

Hallinnon turvallisuusverkkotoiminnan turvallisuusperiaatteista solmittu sopimus koskee turvallisuusverkkotoiminnan kaikkia elinkaaren vaiheita. VAHTI 2/2010 –ohjeen mukaan luokitellun tiedon hallinta tulee suunnitella siten, että se kattaa seuraavat tapahtumat

- Laatiminen
- Vastaanottaminen
- Arkistointi
- Hävittäminen
- Luovuttaminen
- Siirtäminen
- Käsittelyn valvonta
- Ulkoisten palveluiden käyttö



4.2 ICT-varautumisen tasomäärittelyt jatkuvuuden hallinnan ja tiedon saatavuuden varmistamiseksi

Turvallisuusverkon toimijoiden – sekä käyttäjätahojen, että palveluntarjoajien - on varauduttava erilaisiin yhteiskunnallisiin tiloihin (normaali aika, normaaliajan häiriötilanteet, poikkeustila, sotatila) laatimalla varautumisvaatimukset huomioiva ohjeisto ja toteuttamalla sen mukaiset toimenpiteet, mukaan luettuna henkilöstön koulutus. VAHTI-ohje 3/2012 antaa toimijoille perusteet eri varautumistasojen (perustaso, korotettu taso, korkea taso, erityistaso) mukaiselle toiminnalle nimenomaan ICT-varautumisen kannalta. Sisäverkko-ohje (VAHTI 3/2010) antaa lisätietoja tietojärjestelmien suojaamis- ja varautumisaspektin käytännön toteutuksesta ja yksityiskohtaisista vaatimuksista.
ICT-varautumisen osalta turvallisuuskoulutus keskittyy hallinnon turvallisuusverkon suunnittelusta ja ylläpidosta vastaaviin toimijoihin.

4.3 Hallinnon turvallisuusverkon turvallisuusperiaatteista solmitun sopimuksen keskeiset koulutusvelvoitteet

Hallinnon turvallisuusverkon turvallisuusperiaatteista solmittu sopimus edellyttää, että verkon toiminnassa huomioidaan suojaustasonluokittelun osalta tietoturvallisuusasetuksen ja sitä välittömästi täydentävien ohjeiden (ks. luku 4.1) käsitteitä ja termejä. Sopimus edellyttää myös turvallisuusverkkotoiminnassa käsiteltävän tiedon, tietojärjestelmien sekä käsittely- ja säilytystilojen luokittelemista ICT-varautumisen tasoihin (ks. luku 4.2). Sopimuksessa osapuolet sitoutuvat siihen, että verkon turvallisuushallintaan voidaan osoittaa riittävät ja ammattitaitoiset henkilöresurssit (ks. luku 1), jotka kykenevät reagoimaan verkon turvallisuustapahtumiin.

Kaikki edellä mainitut velvoitteet edellyttävät henkilöstön turvallisuushallintaa ja -koulutusta, mukaan luettuina ne alihankkijat, joihin kohdistuu turvallisuusvaatimuksia. Työskenneltiinpä kaupallisten toimijoiden kanssa tai virkamieskunnan kesken, on suositeltavaa käyttää verkon turvallisuushallinnassa tiedon luokittelumatriisia, jossa esitetään selkeästi turvallisuusverkkohankkeen - palvelut mukaan lukien – tiedon luokittelu hanke-elementeittäin (vast.) eroteltuina. Turvallisuusluokittelumatriisin kutakin toimijaa koskevat osat koulutetaan kohdehenkilöstölle (ks. sopimuksen liite 2; luku 5).

LIITE 2

Henkilöstöturvallisuuden hallinta omassa työyhteisössä

KOULUTETTAVAT KOHTEET

1. henkilöstöturvallisuuden käsitteet
2. henkilöstöturvallisuuden organisointi ja vastuut

1 HENKILÖSTÖTURVALLISUUDEN KÄSITTEET

Oppijoille käydään läpi henkilöstöturvallisuuden peruskäsitteistö.

Yleisiä periaatteita

- salassa pidettäviä asiakirjoja tai henkilörekisteriin talletettuja henkilötietoja saavat käsitellä vain ne henkilöt, joilla on oikeus kyseisten asiakirjojen käyttöön.
- henkilön luotettavuus on tarvittaessa selvitetty asiaan kuuluvalla tavalla, esim. turvallisuusselvitysmenettelyn avulla. Tämä vaatimus koskee erityisesti suojaustasoa I ja II edellyttävän tietoaineiston käsittelyä

Perustason vaatimuksia

- Suojaustason IV osalta jokaisella virkamiehellä on oikeus käsitellä tietoa työtehtäviensä tarpeiden mukaisesti viranomaisen johdon päätöksiin perustuen (Tietoturvallisuusasetus 13 §).

1.1 Mitä keinoja käytetään henkilöstön turvallisuudesta huolehtimiseksi tietoturvan näkökulmasta?

- henkilöstön turvallisuusselvitykset (taustatarkastukset)
  - turvallisuusselvitysten edellytyksenä on työtehtäviin perustuva tarve voida käsitellä salassa pidettävää tietoa
  - kansainvälinen turvallisuustodistus
    - hakumenettely (ulkoministeriön johdolla)
    - hallintamenettely (sisäiset vastuujärjestelyt)
  - kansalliseen käyttöön laadittu turvallisuusselvitys
    - hakumenettely (työyhteisö hakee vastuuviranomaisilta)
    - hallintamenettely (sisäiset vastuujärjestelyt)
- henkilöstön turvallisuuskoulutus ja sen ylläpitomenettely
  - keskeinen turvallisuustoimenpide, jota ennen ei voida myöntää pääsyä salassa pidettävään tietoon
- henkilöstön työhyvinvoinnista huolehtiminen on turvallisuusasia!
- salassapitovelvoitteen säilymisen korostaminen työsuhteen päättyessä.

1.2 Turvallisuustietoisuus

- yleisen varovaisuusperiaatteen korostaminen
- varoitus laittoman tiedustelun ja yritysvakoilun esiintymisestä
- matkustusturvallisuuden perusteet.

2 HENKILÖSTÖTURVALLISUUDEN ORGANISOINTI JA VASTUUT

Oppijoille tehdään selväksi, miten omassa työyhteisössä henkilöstön turvallisuudesta huolehditaan (tietoturvanäkökulma)

2.1 Kuka määrittää työyhteisössä, missä tehtävissä joudutaan käsittelemään salassa pidettävää tietoa?

- työyhteisön johto alempia johtoportaita ja turvallisuusjohtoa kuultuaan
- päätös ei ole staattinen, vaan mukautuu muuttuviin tilanteisiin.

2.2 Mistä löytyy kirjallisessa muodossa olevaa tietoa henkilöstöturvallisuuden periaatteista ja käytänteistä?

- organisaation oma turvallisuuspolitiikka
- organisaation oma turvallisuusohjeisto

2.3 Turvallisuusselvitysten hakeminen

- hakuprosessi
  - ° tyypillisesti turvallisuusvastaava valmistelee, organisaation johto allekirjoittaa, toimivaltainen viranomainen (poliisi tai puolustusvoimat) laatii selvityksen
  - ° kansainvälisissä todistuksen kyseessä ollessa maiden vastuuviranomaiset huolehtivat tietojen vaihdosta saatuaan indikaation todistuksen tarpeesta, kunkin maan toimivaltainen viranomainen laatii selvityksen maiden välisen sopimuksen mukaisesti

2.4 Turvallisuusselvitysten hallinta

- ° turvallisuusselvitykset ovat voimassa määräajan
- ° organisaation turvallisuusvastuiden mukainen taho/henkilö pitää kirjaa haetuista turvallisuusselvitystä ja huolehtii niiden pysymisestä voimassa, mikäli kyseessä olevan henkilön tarve käsitellä salassa pidettävää tietoa jatkuu

2.5 Turvallisuustodistuksen evääminen

- mikäli erityistä syytä ilmenee, turvallisuustodistuksen voimassaolo lopetetaan viranomaisen päätöksellä, mahdollisesti organisaation hakemuksesta. Henkilöltä evätään välittömästi pääsy sellaiseen salassa pidettävään tietoon, jonka käsittelyn edellytyksenä todistus oli.

LIITE 3

Fyysisen turvallisuuden hallinta omassa työyhteisössä

KOULUTETTAVAT KOHTEET

1. fyysisen turvallisuuden käsitteet
2. fyysisen turvallisuuden organisointi ja vastuut

1 FYYSISEN TURVALLISUUDEN KÄSITTEET

Oppijoille käydään läpi fyysisen turvallisuuden peruskäsitteet.

- fyysisen turvallisuuden tarkoituksena on suojata henkilöstöä, tietoja ja materiaalia
- fyysisen turvallisuuden kokonaiskäsite sisältää tilaturvallisuuden lisäksi reagointikyvyn (mm. vartiointijärjestelyt)
    - tilaturvallisuudella tarkoitetaan kaikkia niitä rakenteellisia ja valvonnallisia järjestelyjä, joilla varmistetaan tilojen pysyminen vain oikeutettujen hallinnassa ja käytössä sekä käyttötarkoituksen edellyttämässä kunnossa.
    - rakenteilla tarkoitetaan seiniä, kattoja, ikkunoita, ovia, paloturva- ja kassakaappeja sekä muita mekaanisia ratkaisuja.
    - valvontajärjestelmillä tarkoitetaan yleensä kulunvalvonta-, tunkeutumisen ilmaisu-, kameravalvonta- ja olosuhdevaroitusjärjestelmiä. Sähköisiin valvontajärjestelmiin kuuluvat myös kiinteistöautomaatiojärjestelmät, joilla valvotaan ja ohjataan tilan käyttöolosuhteita.
- kutakin tietoturvallisuuden suojaustasoa vastaa jokin turvallisuusvyöhyke. Niihin kohdistuvat viranomaisvaatimukset on esitetty yksityiskohtaisesti VAHTI 2/2013 –ohjeessa ”Toimitilojen tietoturvaohje”
    - Viranomaisen on määriteltävä toimi- ja laitetilojensa turvallisuusratkaisut. Tällaisia ovat rakenteelliset ratkaisut, tarvittavat valvontajärjestelmät ja mahdollisesti tilan käyttöoikeuksiin liittyvät asiat.
    - Viranomainen vastaa tietotyössä käytettävien tilojen turvallisuudesta.
    - Kiinteistöautomaatiojärjestelmien turvalliseen hallintaan tulee kiinnittää erityishuomiota.

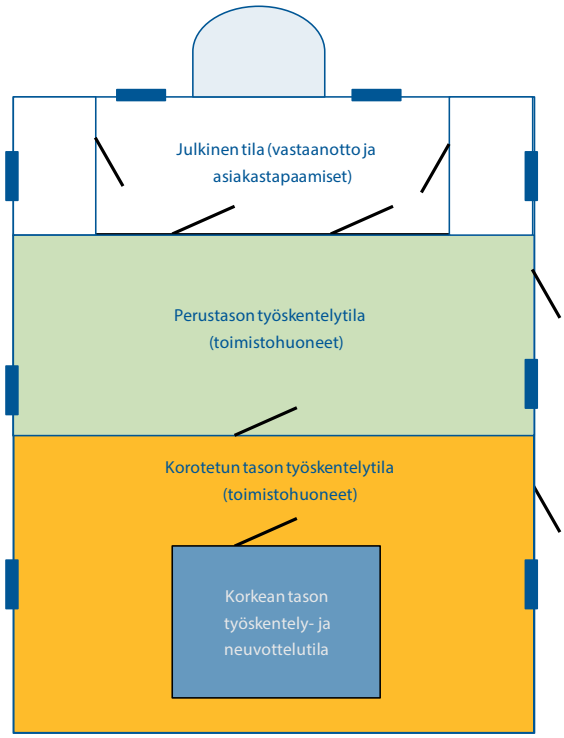
2 FYYSISEN TURVALLISUUDEN ORGANISOINTI JA VASTUUT

Oppijoille tehdään selväksi, miten omassa työyhteisössä huolehditaan fyysisestä turvallisuudesta (tietoturvanäkökulma)

2.1 Mitä fyysisen turvallisuuden käsite sisältää omassa työyhteisössä?
- toimitilaturvallisuuden ja vartioinnin vastuut sekä niiden organisointi työyhteisössä
- organisaation turvallisuusohjeiston linjaukset fyysisen turvallisuuden osalta
- kaaviokuva fyysisen turvallisuuden järjestelyistä siltä osin, kuin ne koskettavat koulutuksen kohteena olevaa henkilöstöä

2.2 Miten turvallisuusverkon käyttötilat on luokiteltu (turvallisuusvyöhykkeet) ja mitä turvallisuustoimenpiteitä eri vyöhykkeet edellyttävät?

Esimerkki valtionhallinnon turvallisuusvyöhykkeistä (lähde: VAHTI 2/2013)



LIITE 4

Salassa pidettävän tiedon turvallinen hallinta omassa työyhteisössä

KOULUTETTAVAT KOHTEET

- salassa pidettävän tiedon turvallisen käsittelyn määritelmistä
- salassa pidettävän tiedon turvallisuuden organisointi ja vastuut

1 SALASSA PIDETTÄVÄN TIEDON TURVALLISEN KÄSITTELYN MÄÄRITELMISTÄ

Oppijoille käydään läpi salassa pidettävän tiedon turvaamisen peruskäsitteet sen lisäksi, mitä tämän ohjeen liitteessä 1 (kappale 4) on opetettu tiedon luokittelusta.

- tiedon turvaamistoimenpiteiden tarkoituksena on suojata luokiteltuja tai muita salassa pidettäviä tietoja oikeudettomalta paljastumiselta silloin, kun tietoa käsitellään tai säilytetään turvallisuusverkkoympäristössä sähköisessä muodossa
- tietoturvallisuuden kokonaiskäsite sisältää kaikki sellaiset toimenpiteet, joiden avulla salassa pidettävä tieto suojataan oikeudettomalta paljastumiselta. Silloin kun tietoturvallisuuden kokonaiskäsitteen alla ei käsitellä tiedon turvaamiseen liittyviä henkilöstöturvallisuuden (liite 2) tai fyysisen turvallisuuden (liite 3) toimia, tietoturvallisuuden käsite jaetaan yleensä kahteen osaan
    - hallinnolliseen tietoturvallisuuteen, jolloin tarkastellaan tiedon turvallisen hallinnan periaatteita (liite 1)
    - tekniseen tietoturvallisuuteen, jolloin tarkastellaan tiedon luottamuksellisuuden takaavia teknisiä toimenpiteitä (liite 4)
- termillä ”asiakirja” käsitetään tietoturvallisuudesta puhuttaessa tietoa missä tahansa muodossa; esim. paperimuotoisena tai sähköisenä

2 SALASSA PIDETTÄVÄN TIEDON KÄSITTELYN ORGANISOINTI JA VASTUUT

Oppijoille tehdään selväksi, miten omassa työyhteisössä huolehditaan salassa pidettävän tiedon turvallisuudesta koko tiedon elinkaari huomioon ottaen:

2.1 Asiakirjan laatiminen ja muokkaaminen

2.1.1 Tietoaineistojen valmistelutyössä tulee alusta alkaen kiinnittää huomio siihen, onko kysymyksessä julkinen vai salassa pidettävää tietoa sisältävä aineisto. Valmistelussa oleva aineisto on laatijan ja valmisteluun osallistuvien vastuulla. Valmistelijataho päättää valmistelussa olevan asiakirjan jakelusta. Valmistelussa oleva asia ei pääsääntöisesti ole ulkopuolisille tarkoitettua, olipa kyseessä julkista tai salassa pidettävää tietoa sisältävä asiakirjaluonnos. Kun asiakirja saavuttaa tason, jossa siitä syntyy viranomaisen asiakirja, se otetaan osaksi viranomaisen tietovarantoa.

2.1.2 Luokiteltua tietoa sisältävää asiakirjaa on käsiteltävä sen valmistelun aikana samalla tavalla kuin viranomaisen muitakin asiakirjoja. Tiedon käsittely ei riipu siitä, missä muodossa tieto on talletettu.

2.1.3 Asiakirjoissa voidaan viitata ylemmän suojaustason sisältämään asiakirjaan. Tämä koskee myös julkisia asiakirjoja.

2.1.4 Asiakirjojen laadinnassa tulee ottaa huomioon asiakirjan käyttötarkoitus sekä pyrkiä hyvään julkisuus- ja salassapitorakenteeseen, mikä merkitsee vaatimusta eriyttää mahdollisuuksien mukaan salassa pidettävät tiedot julkisesta tiedosta. Myös eri suojaustasoihin kuuluva tieto tulee ensisijaisesti esittää eri asiakirjoissa. Näillä menettelyillä turvataan asiakirjojen käytettävyysvaatimukset.

2.2 Asiakirjan tallettaminen

2.2.1 Julkinen ja luokiteltu asiakirja-aineisto (tieto) tulee pitää erillään. Luokiteltua tietoa sisältävät asiakirjat tulee säilyttää siten, että vain käyttöoikeuden omaava henkilöstö pääsee käsittelemään kyseistä aineistoa. On erittäin suositeltavaa, ettei ylimpiin suojaustasoihin kuuluvaa tietoa esitetä tai talleteta viranomaisen asiakirja-aineiston ulkopuolella.

2.2.2 Luokitellun tiedon säilytyksen valvonta on järjestettävä.

2.2.3 Luokitellut (suojaustasot I – III) paperimuotoiset asiakirjat on säilytettävä vähintään Euro II SFS-EN 1143-1 -normin mukaisessa data- tai kassakaapissa sen mukaan, mikä asiakirjan suojaustaso on. Luonnokset eivät tee poikkeusta tästä. Suojaustasoon IV kuuluvat asiakirjat tulee säilyttää lukitussa paikassa.

2.2.4 Sähköisissä järjestelmissä tulee käyttää suojaustasokohtaiset vaatimukset täyttäviä ratkaisuja.

2.2.5 Muisteille talletettavat luokitellut tiedot on suojattava käyttämällä hyväksi suojaustason mukaisia, hyväksyttyjä salausratkaisuja.

2.2.6 Salassa pidettävää tietoa saa siirtää ja taltioida vain viranomaisen hyväksymillä salausmenetelmillä (vast.) suojattuna. Riittävän vahvasti salattua asiakirjaa voidaan käsitellä kuten julkista asiakirjaa.

2.2.7 Suojaustasoon I kuuluva tieto tulee aina olla vahvasti salattu tai muutoin vahvasti suojattu, kun sitä taltioidaan tai käsitellään ainoastaan valvotuissa erillisverkoissa. Suojaustasoon II kuuluva tieto tulee olla vahvasti salattu kun sitä siirretään tai käsitellään perus- tai korotetun tason tietojenkäsittely-ympäristössä. Suojaustasoon III kuuluva tieto voidaan tallettaa selväkielisessä muodossa valvotuissa korotetun tai korkean tietoturvallisuustason verkon palvelimilla. Muissa verkkoympäristöissä suojaustason III tietoa saadaan siirtää ja tallettaa vain asianmukaisesti salattuna. Myös suojaustasoon IV kuuluva tieto tulee salata, kun sitä siirretään ja taltioidaan yleisessä verkossa ja sen palvelimilla, ellei lähettäjän ja vastaanottajan kesken ole sovittu muusta turvallisesta järjestelystä.

2.3 Asiakirjan kopiointi

2.3.1 Luokitelluista asiakirjoista voidaan myös ottaa sekä sähköisiä että paperimuotoisia kopioita ottamalla huomioon suojaustasokohtaiset rajoitukset ja käsittelysäännöt. Kopioita tulee käsitellä kuten alkuperäisiä asiakirjoja.

2.3.2 Kopiot on merkittävä kuten alkuperäiset asiakirjat sekä varmistuttava, että kopion saajalla on työtehtäviin perustuva oikeus salassa pidettävän tietoaineiston käsittelyyn.

2.3.3 Kopiointisäännöt yksinkertaistettuina (TTA):

- ST I –luokiteltu asiakirja: ei saa kopioida ilman laatijan lupaa
- ST I ja ST II –luokitellut asiakirjat: reaaliaikainen seurantavaatimus jokaisen otetun kopion suhteen
  - ° Kopiossa on oltava alkuperäistä vastaava suojaustasomerkintä
- ST III ja ST IV –luokitellut asiakirjat: suojaustasomerkintä ei ole välttämätön, jos asiakirjaa ei luovuteta ulkopuolisille ja käsittelijät tiedostavat suojaustarpeen.

2.4 Asiakirjan välittäminen

2.4.1 asiakirjan välittämisellä tarkoitetaan tässä yhteydessä asiakirjan toimittamista vastaanottajalle muuten kuin tietoverkon välityksellä

2.4.2 ST I ja ST II -asiakirjat toimitetaan fyysisesti perille henkilökohtaisesti tai muulla viranomaisen hyväksymällä tavalla, kuten valtuutetun kuriirin välityksellä. Asiakirjojen lähettäminen ja vastaanottaminen on kirjattava.

2.5 Asiakirjan siirtäminen tietoverkossa

2.5.1 ST I ja ST II –luokiteltua tietoa saa siirtää vain sellaisessa viranomaisen tietoverkossa, joka

- on suljettu ja
- kaikilta osiltaan erityisvalvottu.

Käsittelyn on lisäksi oltava vahvasti suojattua.

2.5.2 ST II –luokiteltua tietoa saa siirtää edellisen lisäksi, kun

- kyseessä on viranomaisen käyttörajoitteinen tietoverkko,
- asiakirja on vahvasti salattu tai vahvasti suojattu ja
- käyttöympäristö kokonaisuudessaan täyttää korkean tietoturvallisuustason vaatimukset..

2.6 Kirjaaminen

2.6.1 Viranomaisen asiakirjarekisteristä tulisi käydä ilmi, mitä suojaustasoa asiakirjat edellyttävät. Korkeimman suojaustason edellyttämien asiakirjojen rekisteri voidaan tarvittaessa luokitella ja se tulee käyttöoikeuksin rajata asiakirjarekisterin muista tiedoista.

2.6.2 Luokitellun asiakirjan vastaanottaja kirjaa vastaanotetun aineiston asiakirjan suojaustasoa vastaavaan diaariin tai rekisteriin. Jos asiakirja tulee suoraan vastaanottajalle, hänen on huolehdittava asiakirjan kirjaamisesta.

2.6.3 Asiakirjan vastaanottaja tarkastaa, että käsittelystä vastaavalla henkilöllä on oikeus käsitellä luokiteltua asiakirjaa.

2.6.4 Asiakirjan vastaanottaja lähettää asiakirjan edelleen asian käsittelijälle käyttäen esim. suljettua kuorta, jos kyseessä on luokiteltu asiakirja, ja muutenkin huomioiden asiakirjojen siirtoon liittyvät menettelytavat.

2.6.5 Salassa pidettävää tietoaineistoa ei saa jättää esille tai valvomatta työtilasta poistuttaessa.

2.6.6 Asiakirjan vastaanottaja vastaa kaikista asiakirjan käsittelyyn liittyvistä velvollisuuksista käsittely- ja käyttöoikeuksineen.

2.6.7 Vastaanotettaessa kansainvälistä turvallisuusluokiteltua tietoa (esim. EU, NATO) sähköisesti tai muilla menetelmillä tulee erikseen varmistua, mitä kahdenkeskisissä turvallisuussopimuksissa (vast.) asiasta on sovittu. Ulkomaiset asiakirjat merkitään tarvittaessa myös kotimaisilla suojaustaso/turvallisuusluokitusmerkinnöillä.

2.6.8 ST I—III sekä ST IV kuuluvien arkaluonteisia henkilötietoja tai biometrisiä tietoja sisältävien henkilörekisteriin talletettujen asiakirjojen käsittely tulee kirjata

- sähköiseen lokiin,
- tietojärjestelmään,
- asianhallintajärjestelmään,
- manuaaliseen diaariin tai asiakirjaan.

Em. ei koske vain laatijan käytössä olevia asiakirjaluonnoksia.

2.7 Arkistointi ja hävittäminen

2.7.1 Arkistoinnin tulee pohjautua arkistonmuodostussuunnitelmissa määriteltyihin rakenteisiin ja vaatimuksiin.

2.7.2 Arkistoinnissa on otettava huomioon suojaustason ja sopimusten käsittelylle asettamat ehdot.

2.7.3 Kansainväliseen toimintaan liittyvät asiakirjat tulee arkistoida sopimuksissa määritellyin tavoin.

2.7.4 Pysyvästi arkistoitavien asiakirjojen osalta noudatetaan Arkistolaitoksen määräyksiä.

2.7.5 Tarpeettomat asiakirjakopiot tulee hävittää käyttötarpeen päätyttyä. Hävittämisen suorittaa organisaation siihen valtuuttama henkilö. Asiakirjan valmistelija vastaa valmistelussaan olevien luonnosvaiheen asiakirjojen hävittämisestä.

2.7.6 Aineiston hävittämisessä on varmistauduttava, ettei se joudu oikeudettomien haltuun.

2.7.7 Paperiasiakirjat tuhotaan suojaustasolle asetetut vaatimukset täyttävää menettelyä käyttäen.

2.7.8 Sähköiset tiedostot tuhotaan tietovälineiltä, työasemilta ja palvelimilta sekä muilta laitteilta suojaustason edellyttämällä tavalla. Tietojärjestelmien käytön yhteydessä syntyvät väliaikaistiedostot on poistettava käyttötarpeen päätyttyä tietohallinnon antamien ohjeiden mukaisesti.

2.7.9 Viranomaisen tulee varmistaa, ettei tietojärjestelmä käsittelyn yhteydessä tallenneta luokitusta edellyttävää tietoa työaseman tai palvelinympäristön muistialueeseen, jonne kyseisen tiedon kannalta asiattomilla on pääsymahdollisuus. Tämä vaatimus koskee myös väliaikais- ja muita tallenteita.

2.7.10 Salassa pidettävät paperiasiakirjat on hävitettävä joko polttamalla, silppuamalla tai keräämällä ne lukittuun astiaan, jonka sisältö hävitetään auditoidussa ja valvotussa ympäristössä.

Käsittelyvaatimukset yksinkertaistetusti	PERUSTASO ST IV (KÄYTTÖ RAJOITETTU)	KOROTETTU TASO ST III (LUOTTAMUKSELLINEN)	KORKEA TASO ST II (SALAINEN)	KORKEIN TASO ST I (ERITTÄIN SALAINEN)
Käsittelyoikeus	Myönnetty käsittely-oikeus	Myönnetty käsittelyoikeus	Myönnetty käsittely-oikeus	Jakelussa mainittu, myönnetty käsittely-oikeus
Jakelu	Työtehtävien mukaisesti	Työtehtävien mukaisesti	Laatija määrittelee, perustuu työtehtäviin	Laatija määrittelee henkilöjakelun
Käsittelyn kirjaaminen	Henkilörekisterissä olevien tietojen tai biometristä tietoa sisältävien asiakirjojen käsittelytapahtumien kirjaaminen	Arkaluonteisten henkilörekisterissä olevien tietojen tai biometristä tietoa sisältävien asiakirjojen käsittelytapahtumien kirjaaminen. Muiden asiakirjojen osalta suositellaan .		
Jäljitettävyys	Ei seurantaa	Ei seurantaa	Asiakirjakopiokohtainen jäljitettävyys	Asiakirjakopiokohtainen jäljitettävyys
Siirto avoimissa verkoissa	Salattuna tai muutoin suojattuna	Salattuna tai muutoin suojattuna	Ei sallittu	Ei sallittu
Siirto viranomaisen verkoissa	Selväkielisenä perustietoturvallisuustason ja sitä korkeamman tietoturvallisuustason verkoissa	Selväkielisenä valvotuissa korotetun tai korkean tietoturvallisuustason verkoissa	Selväkielisenä valvotuissa korkean tietoturvallisuustason verkoissa	Vahvasti salattuna tai muutoin vahvasti suojattuna valvotuissa erillisverkoissa
Käsittely avoimeen verkkoon liitetyssä työasemassa	Sallittu perus-, korotetun ja korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu korotetun tai korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu korkean tietoturvallisuustason käsittely-ympäristöissä	Ei sallittu
Käsittely viranomaisen verkkoon liitetyssä työasemassa	Sallittu perus- ja sitä korkeamman tietoturvallisuustason käsittely-ympäristöissä	Sallittu valvotuissa korotetun ja korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu valvotuissa korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu korkean tietoturvallisuustason erillisverkossa, johon ei ole yhteyttä muista tietoverkoista.
Tallentaminen muistivälineelle (kiintolevy, siirrettävä muisti)	Suojattuna	Salattuna tai muutoin suojattuna	Vahvasti salattuna tai muutoin vahvasti suojattuna	Vahvasti salattuna tai muutoin vahvasti suojattuna
Tallentaminen verkon palvelimelle	Suojattuna käyttäjätunnuksilla	Salattuna tai muutoin suojattuna, jos järjestelmä täyttää korotetun tietoturvallisuustason vaatimukset	Salattuna tai muutoin suojattuna, jos järjestelmä täyttää korkean tietoturvallisuustason vaatimukset.	Vahvasti salattuna tai muutoin vahvasti suojattuna, jos järjestelmä täyttää korkean tietoturvallisuustason vaatimukset.

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 09 160 01
Telefaksi 09 160 33123
www.vm.fi

19/2013
Valtiovarainministeriön julkaisuja
Heinäkuu 2013

ISSN 1459-3394 (nid.)
ISBN 978-952-251-476-9 (nid.)
ISSN 1797-9714 (pdf)
ISBN 978-952-251-477-6 (pdf)