

Valtiontalouden tarkastusviraston määräys



**Valtiontalouden tarkastusviraston
toimintakäsikirja**

**Määräys tietoturvallisuudesta
tarkastusvirastossa**
(sisältää muutokset 17.10.2011)

Valtiontalouden tarkastusviraston määräys tietoturvallisuudesta

Dnro 179/01/11

Tämä määräys liitetään osaksi Valtiontalouden tarkastusviraston toimintakäsikirjaa.

Helsingissä 24. päivänä toukokuuta 2011

Pääjohtaja Tuomas Pöysti

Tietojohtaja Jaakko Hamunen

Sisällys

1	Määräyksen rakenne ja keskeiset määritelmät	5
2	Tietoturvapoliittikka	6
3	Tietoturvallisuuden hallintajärjestelmä	8
4	Hallinnollinen turvallisuus	10
5	Henkilöstöturvallisuus	13
6	Tietoaineistoturvallisuus	16
6.1	Asiakirjojen luokittelu ja merkinnät	16
6.2	Käsittelyoikeudet	18
6.3	Tietoaineiston käsittely	19
6.4	Tiedon antaminen salassa pidettävästä tietoaineistosta	21
6.5	Tietoaineiston toimittaminen vastaanottajalle ja vastaanottaminen	22
6.6	Tietoaineistojen hävittäminen	23
7	Fyysinen turvallisuus	24
8	Tietotekninen turvallisuus	26
8.1	Tietoliikenne	26
8.2	Työasemat, oheislaitteet ja matkapuhelimet	27
8.3	Siirrettävät tietovälineet	28
8.4	Järjestelmien ja ohjelmistojen käyttö	29
8.5	Sosiaalinen media	30
9	Toiminta poikkeustilanteissa	32
10	Toimenpiteet	33
	Litteet:	35
	Liite 1. Työaseman käyttäjän tietoturvaohje	
	Liite 2. Sitoumus tietoteknisten laitteiden käytöstä ja vaitiolosta	
	Liite 3. Käyttöoikeuksien hakulomake tarkastusviraston tietojärjestelmiin	
	Liite 4. Kooste luokitellun tiedon käsittelystä	

1 Määräyksen rakenne ja keskeiset määritelmät

Tämä määräys sisältää Valtiontalouden tarkastusviraston tietoturvapoliittikan sekä määräykset tarkastusvirastossa käytettävästä tietoturvallisuuden hallintajärjestelmästä, hallinnollisesta turvallisuudesta, henkilöstöturvallisuudesta, tietoaineistoturvallisuudesta, fyysisestä turvallisuudesta, tietoteknisestä turvallisuudesta sekä määräyksen toimenpanemiseksi tarvittavista ensimmäisistä toimenpiteistä.

Tietoturvallisuudella tarkoitetaan tietojen käytettävyyden, eheyden ja luottamuksellisuuden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä.

Käytettävyydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat niihin oikeutettujen esteettä hyödynnettävissä silloin, kun niitä tarvitaan.

Luottamuksellisuudella tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.

Eheydellä tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

2 Tietoturvapoliittikka

Tietoturvapoliittikassa kuvataan tarkastusviraston tietoturvallisuuden yleiset perusteet, tavoitteet ja periaatteet.

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:n mukaan viranomaisten tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä. Henkilötietolain (533/1999) 32 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämislä taikka muulta laittomalta käsittelyltä.

Tarkastusvirasto tuottaa eduskunnalle, valtioneuvostolle ja sen alaiselle hallinnolle hyödyllistä ja luotettavaa valvonta- ja tarkastustietoa. Tuotettavat tiedot ja niiden tuottamiseksi tarvittavat tiedot tulee suojata tarkoituksenmukaisella tavalla tarkastusviraston tehtävien onnistumisen takaamiseksi. Tämän kokonaisuuden toimivuus edellyttää riittävää tietoturvallisuuden tasoa.

Tarkastusvirastolla on perustuslaissa säädetty oikeus saada viranomaisilta ja muilta valvontansa kohteina olevilta tehtävänsä hoitamiseksi tarvitsemansa tiedot. Osa näistä tiedoista voi olla salassa pidettäviä tai arkaluonteisia. Tarkastusviraston on pystyttävä käsittelemään vastaanottamiin tietoja vähintään yhtä turvallisesti kuin tietoja omistavat organisaatiot niitä käsittelevät.

Valtionhallinnossa noudatetaan tietoturvallisuudesta valtionhallinnossa annettua asetusta (681/2010; jäljempänä tietoturvallisuusasetus). Valtionhallinnon kanssa tapahtuvan tietojen vaihdon turvaamiseksi ja yhdenmukaistamiseksi tarkastusvirastossa noudatetaan asetusta tässä määräyksessä ja erillisissä tietoturvaohjeissa kuvatulla tavalla. Tarkastusvirastossa noudatetaan vähintään asetuksen mukaista tietoturvallisuuden perustasoa. Tarkastusviraston tietoturva-asiakirjoja laadittaessa huomioidaan soveltuvin osin valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) antama ohjeistus.

Tarkastusvirasto eduskunnan yhteydessä olevana virastona saa osan tietoteknisistä palveluistaan eduskunnan kautta. Näiden palvelujen tietoturvallisuuteen liittyvissä asioissa tarkastusvirasto tekee yhteistyötä eduskunnan kanssa ja sopii, tulisiko palveluja koskevia tietoturvaohjeita soveltaa tarkastusvirastossa sellaisenaan vai muutettuna. Tarkastusvirasto pitää

eduskunnan ja muut keskeiset sidosryhmät tietoisina tietoturvatilanteestaan niitä koskevilta osin.

Tarkastusviraston henkilöstö osallistuu tietoturvakoulutukseen, noudattaa tietoturvaohjeita, tietoturvallisia toiminta- ja työskentelytapoja sekä tunnistaa ja ehkäisee tietoturvariskejä ja raportoi havaitsemistaan tietoturvallisuuden puutteista. Esimiehet tukevat, ohjaavat työntekijöitään ja varmistavat, että vastuualueeseensa sisältyvät tietoturvamenettelyt suoritetaan asianmukaisesti.

Mikäli tarkastuskohteissa, niiden tietojärjestelmissä tai omistamien tietojen käsittelyssä vaaditaan korkeampaa tietoturvallisuutta, noudatetaan näiltä osin kohteen antamia tietoturvaohjeita ja -määräyksiä, mikäli ne eivät ole este tarkastuksen suorittamiselle. Tarkastusviraston ulkopuolisilta palveluntuottajilta edellytetään vähintään samaa tietoturvallisuustasoa kuin tarkastusvirasto itsekin noudattaa.

3 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan tietoturvallisuus-toiminnan yleistä toimintaperiaatetta ja -kehystä, joka koostuu mm. seuraavista toimintamalleista ja dokumenteista:

- tietoturvamääräys sisältäen tietoturvapoliitiikan
- tietoturvaohjeet ja -koulutus
- riskien arviointi ja hallinta
- tietoturvallisuuden kehittämissuunnitelmat
- tietoturvaraportointi johdolle
- seuranta ja auditointi

Tietoyksikkö järjestää koko henkilöstölle tietoturvakoulutusta vähintään joka toinen vuosi.

Koska tarkastusviraston kaikissa tehtävissä on oikeus käsitellä salassa pidettävä tietoa, jokaisella on velvollisuus huolehtia tietoturvaosaamisestaan. Jokaisen on osallistuttava tietoturvakoulutukseen. Tietoturvaosaaminen arvioidaan kehityskeskustelujen yhteydessä.

Tietoturvallisuuden riskien arviointi on osa tarkastusviraston yleistä riskien arviointia. Riskien arviointi käsittää tietoturvallisuuden riskianalyysin ja riskien vaikutusten arvioinnin. Riskianalyysissä tunnistetaan ja määritellään tarkastusvirastoon kohdistuvat tietoturvallisuusuhkat ja arvioidaan niihin liittyvien riskien suuruudet toteutumisen todennäköisyyksien ja mahdollisten vaikutusten perusteella. Riskien vaikutusten arvioinnissa määritetään riskien hyväksyttävyyks eli määritetään jatkotoiminnan pohjaksi vaihtoehtoja arvioitujen riskien siirrettävyydestä, pienentämisestä tai kokonaan poistamisesta. Riskien hallinta käsittää riskien vähentämiseen liittyvän päätöksenteon, päätöksien toimeenpanon sekä seurannan. Tietoturvaryhmä tekee riskien arvioinnin vähintään joka toinen vuosi siten, että sen tulokset, toimenpide-ehdotukset ja edellisen arvioinnin toimenpiteiden seuranta on esiteltävissä viraston johtoryhmälle määräaikaisen tietoturvaraportin yhteydessä.

Tietoturvallisuuden hallinnan kehittämistoimenpiteet sisällytetään tarkastusviraston toiminta- ja taloussuunnitelmaan ja sekä vuosittain vahvistettavaan tulostavoitteet ja tarkastussuunnitelmaan ja ne suunnitellaan kyseisten suunnitelmien laatimisen yhteydessä. Suunnitelmien toteutumista raportoidaan osana tarkastusviraston raportointia. Kehittämistoimenpiteiden täytäntöönpanosta tehdään tarvittaessa erilliset suunnitelmat ja pää-

tökset. Yksiköt sisällyttävät kehityskeskusteluissa kehittämistoimenpiteet henkilöstön tavoitteisiin ja pysyvät tietoturvavastuut tehtäväkuvauksiin.

Tietoturvallisuusraportointi jakaantuu säännöllisesti annettavaan tietoturvaraporttiin ja erillisraportointiin. Yksiköt raportoivat tietoturvasuosituksensa mukaisista asioista tietoturvapäälikölle aina havaitessaan tietoturvapoikkeamia tai -riskejä. Tietoturvapäälikkö kokoaa tiedot tietoturvaraporttiin yksiköiltä ja henkilöstöltä saamiensa ilmoitusten sekä omien seuranta- ja valvontatoimenpiteiden perusteella vuosittain elokuussa ja tammikuussa. Tietoturvaraportti käsitellään tietoturvaryhmässä ja sen jälkeen viraston johtoryhmässä. Elokuussa koostettava raportti käsitellään viraston johtoryhmässä syyskuussa ja tammikuussa koostettava raportti sisäisen valvonnan arviointi- ja vahvistuslausuman yhteydessä helmikuussa. Erillisraportointia tehdään tilanteen ja tarpeen mukaisesti. Erillisraportointi painottuu havaittuihin vakaviin tietoturvallisuusrikkeisiin ja -rikkomuksiin sekä muihin mahdollisiin tietoturvallisuuteen liittyviin vakaviksi luokiteltuihin vaaratilanteisiin tai puutteisiin.

Tietoturvallisuuden seuranta ja valvonta on osa normaalia esimiesasemassa olevien johtamistoimintaa. Arvio tietoturvallisuuden riskienhallinnan asianmukaisuudesta ja riittävydestä sekä olennaisimmista kehittämistarpeista sisällytetään tarkastusviraston toimintakertomukseen. Tietoyksikkö tilaa vähintään joka toinen vuosi ulkoisen auditoinnin yhdelle tietoturvallisuuden osa-alueelle. Kriittiset ja kiireelliset tulokset ja toimenpide-ehdotukset käsitellään viraston johtoryhmässä välittömästi auditoinnin valmistuttua. Muut auditoinnin tulokset käsitellään tietoturvaraportin yhteydessä. Auditoinnin toteutuksesta ja sen toimenpidesuositusten seurannasta vastaa tietoturvapäälikkö, ja tietoturvaryhmä osallistuu sen toteuttamiseen. Seuranta ja auditointi liitetään osaksi viraston laatujärjestelmää.

4 Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella tarkoitetaan tietoturvallisuuteen tähtääviä hallinnollisia keinoja, kuten organisaatiojärjestelyjä, tehtävien ja vastuiden määrittelyä sekä henkilöstön ohjeistusta ja valvontaa.

Tarkastusviraston pääjohtaja vahvistaa vuosittain tulostavoitteet ja tarkastussuunnitelmassa tietoturvallisuustoiminnan tavoitteet, linjaukset ja voimavarat sekä vahvistaa tietoturvallisuutta koskevat viraston määräykset.

Tietoyksikön päällikkö voi antaa tietoturvallisuutta koskevia hallinnollisia määräyksiä ja ohjeita tarkastusviraston työjärjestyksen 24 §:n perusteella sekä esittelee tietoturvallisuutta koskevat asiat pääjohtajalle ja johtoryhmässä.

Tarkastusviraston johtoryhmä toimii tarkastusviraston työjärjestyksen mukaisesti myös tietoturvallisuusasioissa pääjohtajan ja tarkastuksen toimintayksiköiden, hallintoyksikön ja tietoyksikön johdon yhteistyö- ja valmisteluelimänä johtamisessa ja toiminnan suunnittelussa, kehittämisessä sekä toiminnan arvioinnissa. Johtoryhmä käsittelee tietoturvallisuustilanteen vähintään kaksi kertaa vuodessa.

Tietoyksikkö vastaa

- tarkastusviraston työjärjestyksen 6 §:n mukaisesti tarkastusviraston tietoturvallisuuden hallintajärjestelmästä sekä huolehtii tietoturvallisuustoiminnan yhteensovittamisesta, tietoturvallisuuteen liittyvien asioiden valmistelusta ja tietoturvallisuushankkeiden sisällyttämisestä viraston suunnitteluasiakirjoihin
- tietoteknisen turvallisuuden ja tietoaineistoturvallisuuden ohjeistuksesta, seurannasta ja valvonnasta sekä näihin liittyvien poikkeamien tiedottamisesta
- tietoturvallisuusraportoinnista eduskunnalle ja muille sidosryhmille tarvittavilta osin
- omistamiensa tietojärjestelmien käytön tietoturvallisuudesta
- tekemiensä hankintojen ja tehtäviinsä liittyvien kumppanuuksien tietoturvallisuudesta
- tietoturvamääräyksen ja -ohjeiden menettelytapojen noudattamisesta yksikön työskentelyssä
- työntekijöidensä osallistumisesta tietoturvakoulutukseen ja työntekijöiden tietoisuudesta tietoturvamääräyksen ja ohjeiden menettelytapoista.

Tietoturvapäällikkö

- valmistelee tietoturvallisuutta koskevat määräykset, ohjeet, raportit ja koulutuksen
- huolehtii tietoturvallisuuden hallintamallin kehittämisestä
- ylläpitää ja kehittää tarkastusviraston hankintasopimuksissa käyttämää turvallisuusliitettä
- seuraa ja valvoo tietoturvallisuudesta annettujen määräysten ja ohjeiden noudattamista.

Apunaan hänellä on tietoturvaryhmä.

Hallintoyksikkö vastaa

- fyysisen turvallisuuden ja henkilöstöturvallisuuden ohjeistuksesta, seurannasta ja valvonnasta, näihin liittyvien poikkeamien tiedottamisesta ja näitä koskevien kehittämistoimenpiteiden sisällyttämisestä viraston suunnitteluasiakirjoihin
- omistamiensa tietojärjestelmien käytön tietoturvallisuudesta
- tekemiensä hankintojen ja tehtäviinsä liittyvien kumppanuuksien tietoturvallisuudesta
- tietoturvamääräyksen ja -ohjeiden menettelytapojen noudattamisesta yksikön työskentelyssä
- työntekijöidensä osallistumisesta tietoturvakoulutukseen ja työntekijöiden tietoisuudesta tietoturvamääräyksen ja ohjeiden menettelyta-voista.

Tarkastusviraston toimintayksiköt vastaavat

- omistamiensa tietojärjestelmien käytön tietoturvallisuudesta
- tekemiensä hankintojen ja tehtäviinsä liittyvien kumppanuuksien tietoturvallisuudesta
- tietoturvamääräyksen ja -ohjeiden menettelytapojen noudattamisesta yksikön työskentelyssä tietoturvallisuuden edellyttämien toimenpiteiden sisällyttämisestä tarkastusohjeisiin
- työntekijöidensä osallistumisesta tietoturvakoulutukseen ja työntekijöiden tietoisuudesta tietoturvamääräyksen ja ohjeiden menettelyta-voista.

Jokainen tarkastusviraston henkilöstöön kuuluva vastaa oman toimintansa tietoturvallisuudesta. Henkilöstön tulee välttää tietoturvallisuutta vaarantavia toimenpiteitä ottaen huomioon, mitä vaitiolovelvollisuudesta, viranomaisten toiminnan julkisuudesta, asiakirjojen salassa pitämisestä, henki-

lötietojen käsittelystä sekä tietojen luovuttamisesta säädetään ja mitä ylimpien tarkastusviranomaisten kansainvälisen järjestön vahvistama ISSAI -tarkastusstandardin 30 Code of Ethics perustuva ulkoisen tarkastajan tarkastusetiikka edellyttää.

Henkilöstö perehtyy tietoturvallisuusmääräykseen ja ohjeisiin, noudattaa niitä, tunnistaa ja ehkäisee tietoturvallisuusriskejä omassa toiminnassaan sekä tekee aloitteita toiminnan kehittämiseksi. Henkilöstö raportoi havaitsemistaan tietoturvallisuuspoikkeamista omalle esimiehelleen tai tietoturvapäällikölle.

Esimiehet tukevat ja ohjaavat työntekijöitään sekä varmistavat, että työntekijöillä on tehtäviinsä nähden riittävä tietoturvaosaaminen ja että työntekijöiden tehtävät suoritetaan asianmukaisesti. Tietoturvallisuuden huomiointi on osa esimiestyötä.

Palveluja, ohjelmistoja tai laitteita hankittaessa hankinnan valmistelijan on varmistettava hankinnan kohteen, toimittajan ja toiminnan tietoturvallisuus. Mikäli hankittavan tavaran tai palvelun toimittamisessa on tarve käsitellä salassa pidettävää tai arkaluonteista tietoa tai toimittajan henkilöstöllä on tarve liikkua sellaisissa tarkastusviraston tiloissa, joissa käsitellään salassa pidettävää tai arkaluonteista tietoa, on otettava yhteyttä hallintoyksikköön ja sovittava toimittajan kanssa turvallisuusmenettelyistä. Lisäksi toimittajan henkilöstöstä on haettava ennen työn aloittamista turvallisuusselvityksistä annetun lain (177/2002) mukainen suppea tai perusmuotoinen turvallisuus selvitys, mikäli laissa määritellyt selvityksen edellytykset täyttyvät.

5 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien tietoriskien hallintaa henkilöstön soveltuvuuksien, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.

Henkilöstöturvallisuuden tavoitteena on vähentää suojattaviin tietoi-neistöihin kohdistuvia inhimillisen eli henkilön aiheuttaman virheen riskiä sekä erilaisia väärinkäytösriskejä. Henkilöstöturvallisuuden tavoitteena on lisäksi varmistaa, että käyttäjät ovat tietoisia tietoturvallisuuteen liittyvistä uhkista ja niiden merkityksistä ja että heillä on tarvittava tietotaito ja kei-not tukea tarkastusviraston turvallisuutta työskennellessään.

Uusien työntekijöiden rekrytoinnin yhteydessä kaikista valittavaksi esi-tettävistä haetaan perusmuotoista turvallisuusselvitystä ja heidät voidaan velvoittaa toimittamaan huumausainetestiä koskeva todistus, ellei ole pe-rusteltua syytä jättää selvitystä hakematta tai huumausainetestiä koskevaa todistusta toimittamatta. Rekrytoitaessa tärkeimpien tutkinto- ja työtodis-tusten oikeellisuus tarkistetaan kohtuullisin käytettävissä olevin keinoin.

Viraston työntekijästä voidaan hakea perusmuotoista turvallisuusselvi-tystä työntekijän tehtävän olennaisesti muuttuessa. Lisäksi viraston työn-tekijä voidaan velvoittaa toimittamaan huumausainetestiä koskeva todistus yksityisyyden suojasta työelämässä annetun lain 7 §:n 3 momentin nojal-la, jos työntekijän työtehtävät muuttuvat työsuhteen aikana siten, että ne täyttävät laissa säädetty edellytykset työnantajan oikeudesta käsitellä huumausainetestiä koskevaan todistukseen merkittäviä tietoja.

Turvallisuusselvitysten teosta on säädetty laissa turvallisuusselvityksistä (177/2002). Huumausainetestiä koskevan todistuksen toimittamisesta vir-kaan nimittämisen edellytyksenä säädetään lain eduskunnan virkamiehistä (1197/2003) 14 §:ssä. Huumausaineiden käyttöä koskevien tietojen käsit-telystä on säädetty laissa yksityisyyden suojasta työelämässä (759/2004).

Ennen tietokoneen, matkapuhelimen ja näiden käyttäjätunnusten luovut-tamista tietohallintohenkilöstö antaa jokaiselle uudelle työntekijöille tä-män tietoturvamääräyksen, opastaa käyttäjää työvälineiden käytössä, näyt-tää mistä työntekijä löytää tietoturvamääräyksen ja -ohjeet sekä ottaa vas-taan liitteenä 2 olevan sitoumuksen.

Uuden henkilöstön perehdyttämiskoulutukseen sisällytetään tietoturva-koulutusta. Koulutuksessa käydään läpi henkilöstön tietoturvallisuuteen liittyvät yleiset velvollisuudet sekä esitellään tietoturvamääräys ja -ohjeet ja niiden saatavilla olo. Tietoturvapäällikkö varmistaa, että jokainen uusi työntekijä osallistuu perehdyttämiskoulutuksessa tietoturvaosioon ja jär-

jestää poissaolleille uutta koulutusta, kunnes kaikki uudet työntekijät ovat osallistuneet koulutukseen. Työntekijän tietoturvallisuutta koskevat erityiset vastuut ja velvollisuudet määritellään henkilön tehtäväkuivissa. Työntekijöiden tulee myös tuntee hänelle määrätyt tehtävät ja vastuut mahdolliset sijaisjärjestelyt mukaan lukien.

Tarkastusvirastoon henkilöstön samoin kuin tarkastusviraston toimeksiannosta toimivan ja tämän palveluksessa olevan vaitiolovelvollisuudesta sekä siihen liittyvästä tietojen hyväksikäyttökiellosta on voimassa, mitä julkisuuslaissa säädetään (JulKL 22 ja 23 §). Vaitiolovelvollisuus ja tietojen hyväksikäyttökielto on voimassa myös virkasuhteen tai tehtävän päätyttyä.

Esimiehen tulee todeta työntekijän tarve tietojärjestelmien käyttöön ja käyttöoikeuksien laajuus työtehtävistä tulevaa tarvetta vastaavaksi. Esimies taltioi kopion työntekijän käyttöoikeushakemuksesta tai muulla tavoin seuraa työntekijöidensä hakemia käyttöoikeuksia ja vähintään kerran vuodessa esimerkiksi kehityskeskustelujen yhteydessä toteaa käyttöoikeuksien tarpeen jatkumisen. Käyttöoikeuksien hakemisessa tarvittava lomake on liitteenä 2.

Virka- tai palvelussuhteen päättyessä työntekijä vastaa ilmoituksista tietoteknisten järjestelmien käyttöoikeuksien poistamiseksi sekä tarkastusviraston omaisuuden, luokitellun tietoaineiston, avainten ja kulkukorttien palautuksista. Virkasuhteen päättymisestä sekä tehtävää hoitavasta uudesta henkilöstä tulee tarvittaessa ilmoittaa keskeisille sidosryhmille. Esimies varmistaa, että edellä mainitut toimenpiteet on tehty tarkastamalla työntekijän täyttämän tarkistuslistan. Esimies ja työntekijä varmistuvat yhdessä työntekijän hallussa olevan tietoaineiston käytettävyydestä sekä kertaavat vaitiolo- ja salassapitovelvoitteet. Esimies vastaa työntekijän tietoturvallisuuden ylläpitoon tai valvontaan liittyvien tehtävien siirrosta ja jatkumisesta.

Tarkastusviraston tietoturvallisuutta vaarantavista epäilyistä rikoksista ja rikkomuksista, kuten varkaudesta, luvattomasta käytöstä, vaaran aiheuttamisesta tietojenkäsittelylle, vahingonteosta ja tieto- ja viestintärikoksista sekä tietoturvallisuutta vaarantavista tahattomista vahingoista tulee viiveettä raportoida esimiehelle ja tietoturvapäällikölle.

Hankinnan valmistelija vastaa hankinnan turvallisuustoimenpiteiden toteuttamisesta. Ostopalveluiden tietoturvallisuusvaatimukset on arvioitava hankinnan valmistelun yhteydessä. Mikäli palveluntuottaja voi joutua käsittelemään salassa pidettävää tietoaineistoa tai palveluntuottajan henkilöstö liikkuu tarkastusviraston toimitiloissa, joissa käsitellään salassa pidettävää tietoaineistoa, tarjouspyyntöön on sisällytettävä turvallisuusvelvoitteet. Turvallisuusvelvoitteissa tulee velvoittaa palveluntoimittaja hyväksyttämään työntekijänsä tarkastusvirastolla ennen työn aloittamista,

toimittamaan työhön osallistuvan henkilöstön henkilökohtaiset vaitiolositoumukset sekä mahdolliset kirjalliset suostumukset turvallisuusselvitysten teettämistä varten.

Mikäli palveluntuottaja voi joutua käsittelemään salassa pidettävää tietoaaineistoa, sen henkilöstöstä haetaan perusmuotoista turvallisuusselvitystä. Mikäli palveluntuottajan henkilöstö liikkuu tarkastusviraston tiloissa, joissa käsitellään salassa pidettävää tietoaaineistoa, henkilöstöstä haetaan suppeaa turvallisuusselvitystä lain turvallisuusselvityksistä (177/2002) edellytysten täytyessä.

Suppeaa turvallisuusselvitystä ei tarvitse pyytää, jos kyseessä on kertaluontoinen tai muuten satunnainen kulkuoikeuden järjestäminen tarkastusviraston tiloihin, kuten esimerkiksi lyhytkestoinen huoltotyö työhuoneessa tai muussa tilassa. Tällaisissa tapauksissa vierailun valvonta on oltava tarkastusviraston työntekijänä toimivan isännän vastuulla.

Vaitiolositoumukset säilytetään asianomaisten palvelusopimusten yhteydessä. Sitoumusten tulee olla voimassa myös sopimuksen päättymisen tai työsuhteen purkautumisen jälkeen.

Turvallisuusvelvoitteiden on katettava myös palvelun tuottajan mahdolliset aliurakoitsijat.

6 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan asiakirjojen, tiedostojen ja muiden tietojen ja niitä sisältävien järjestelmien tunnistusta, luokittelua, säilytystä, hävittämistä ja valvontaa käsittelyn eri vaiheissa. Asiakirjalla ymmärretään tässä määräyksessä julkisuuslain (621/1999) 5 §:n mukaista asiakirjaa.

6.1 Asiakirjojen luokittelu ja merkinnät

Salassa pidettävien asiakirjojen luokittelussa tarkastusvirastossa käytetään seuraavia luokkia:

1. suojaustaso I (ST I), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle;
2. suojaustaso II (ST II), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle;
3. suojaustaso III (ST III), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle;
4. suojaustaso IV (ST IV), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle. Samaan suojaustasoon voidaan luokitella muukin kuin salassa pidettäväksi säädetty asiakirja, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Kansainvälisiä suhteita, valtion turvallisuutta tai esimerkiksi maanpuolustusta käsittelevissä valtionhallinnon asiakirjoissa voi olla myös turvallisuusluokittelumerkintä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisalan piiriin kuuluva aineisto luokitellaan kansainvä-

listen velvoitteiden mukaisesti. Kansainvälisten järjestöjen ja Suomen turvallisuusluokitukset vastaavat suojaustasoja alla olevan taulukon mukaisesti.

Suojaustaso	Turvallisuusluokka	EU	NATO
Suojaustaso I	ERITTÄIN SALAINEN, ERSAL, E	TRÉS SECRET UE/ EU TOP SECRET	COSMIC TOP SECRET
Suojaustaso II	SALAINEN, SAL, S	SECRET UE/ EU SECRET	NATO SECRET
Suojaustaso III	LUOTTAMUKSELLINEN, LUOT, L	CONFIDENTIEL UE/ EU CONFIDENTIAL	NATO CONFIDENTIAL
Suojaustaso IV	KÄYTTÖ RAJOITETTU, RAJ, R	RESTREINT UE/ EU RESTRICTED	NATO RESTRICTED

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin julkisuuslain 24 § 1 momentin 2, 7–10 kohtiin tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen vuoksi.

Henkilörekistereiden ja niihin sisältyvien tietojen julkisuus- ja salassapitoerusteet sekä luokitusta koskevat vaatimukset ovat samoja kuin muis-
sakin asiakirjoissa. Mikäli salassa pidettävän asiakirjan sisällöstä ei muuta johdu, arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan suo-
jaustasolle III. Henkilötunnuksen sisältäviä asiakirjoja käsitellään suojaus-
tason IV mukaisesti, ellei asiakirjan sisällön perusteella asiakirjaa kuulu
käsitellä korkeamman suojaustason vaatimusten mukaisesti. Salassa pidet-
tävä tietoaineisto varustetaan alla olevalla leimalla tai sähköisessä käsitte-
lyssä merkinnällä, jossa ilmenee salassa pidettävyys. Leima sijoitetaan en-
simmäisen sivun oikeaan yläkulmaan. Asiakirjaan kirjataan merkintä sa-
lassapidon perusteesta sekä selvitys sen mahdollisesta julkisesta osuudes-
ta. Salassa pidettävän asiakirjan sivut numeroidaan ja sivujen lukumäärä
merkitään asiakirjaan.

SALASSA PIDETTÄVÄ

Suojaustaso __

JulkL (621/1999) 24.1 §:n _____k

L (____/____) __ §:n _____k

Suojaustasoon I ja II kuuluvissa asiakirjoissa leima sijoitetaan asiakirjan kaikille sivuille ja lisäksi tulostettaessa käytetään punaisella poikkiviivalla merkittyä paperia tai vastaavan merkinnän toteuttavaa tulostustapaa.

Luokiteltuun tietoaaineistoon tehdään sen suojaustasoa osoittavat merkinnät jo luonnosvaiheessa. Tiedon käsittely ei riipu siitä, missä muodossa tieto on talletettu.

Salassa pidettävä tietoaaineisto voi sisältää myös alemman salattavuusasteen tai julkisia liitteitä tai osia. Liitteet merkitään kunkin liitteen suojaustason mukaisesti. Asiakirjan suojaustaso valitaan sen sisältämän korkeimman suojaustason mukaisesti. Tällöin pääasiakirjasta tulee käydä ilmi sekä pääasiakirjan että liitekohtainen suojaustaso, mikäli nämä poikkeavat toisistaan. Myös muusta asiakirjasta poikkeavaa luokiteltua tietoa sisältävän kappaleen alkuun voidaan merkitä sulkuihin suojaustasomerkintä osoittamaan kappaleeseen sisältyvän tiedon käsittelyn tasoa.

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

Jos salassapito päättyy tietyssä hetkenä tai tietyn tapahtuman johdosta, tästä voidaan tehdä merkintä salassapitoa osoittavan leiman alapuolelle. Tiedon salassa pitäminen lakkaa, kun asiakirjan antamisesta ei aiheudu salassapidon edellytyksenä olevia vaikutuksia tai kun julkisuuslain 31 §:ssä säädetty salassapitoaika on kulunut umpeen.

JulkL 31 §:n mukaan viranomaisen salassa pidettävien asiakirjojen salassapitoaika on pääsääntöisesti 25 vuotta. Mikäli salassapitotarve on edellä mainitussa laissa määritettyä aikaa lyhyempi tai pidempi, tehdään tästä merkintä asiakirjaan. Merkintä tehdään salassapitoleiman alapuolelle tai muuten sopivaan kohtaan. Salassapidon päättymisestä tulee tehdä merkintä myös asiakirjojen luovutusluetteloon sekä diaariin.

Tietoaaineiston suojaustason ratkaisee asiakirjan allekirjoittaja esittelijän tai valmistelijan esittelystä. Viranomaiselle toimitetun asiakirjan (esimerkiksi kantelut tai tarjoukset) suojaustason ratkaisee asian käsittelystä vastaava virkamies. Valmistelija tekee valmisteltavana olevaan asiakirjaan tai muuhun tietoaaineistoon suojaustasoa osoittavan merkinnän. Tietojärjestelmissä käsiteltävän tietoaaineiston suojaustason ratkaisee järjestelmän omistava yksikkö.

6.2 Käsittelyoikeudet

Asiakirjasta saa antaa tietoja vain niille henkilöille, joille on myönnetty oikeus käsitellä asiakirjan edellyttämän suojaustason mukaisia asiakirjoja

ja joilla on asiakirjan sisältämää tietoa edellyttävä, työtehtäviin pohjautuva käsittelytarve.

Suojaustasoon I kuuluvien tietoaineistojen pysyvä käsittelyoikeus tarkastusvirastossa on pääjohtajalla sekä tietoturvallisuuskoulutuksen ja perusmuotoisen turvallisuusselvityksen teon jälkeen toimintayksiköiden päälliköillä sekä asiakirjahallintoon ja arkiston hoitoon liittyvissä tehtävissä tietoyksikön päälliköllä ja hänen ensimmäisellä sijaisellaan. Mikäli suojaustasoon I kuuluvan asiakirjan käsittelyoikeuksien laajentaminen on tarpeen ja mahdollista, pääjohtaja tai hänen sijainen voi myöntää tietoturvallisuuskoulutuksen sekä perusmuotoisen turvallisuusselvityksen teon jälkeen tilapäisen, tiettyä asiaa tai asiakirjaa koskevan käsittelyoikeuden työntekijälle, jonka työtehtävät sitä edellyttävät. Tilapäinen käsittelyoikeus merkitään kyseiseen asiakirjaan.

Suojaustasoon II kuuluvien tietoaineistojen pysyvä käsittelyoikeus tarkastusvirastossa on suojaustasoon I kuuluvien tietoaineistojen pysyvän käsittelyoikeuden omaavilla sekä tietoyksikön päälliköllä, hallintoyksikön päälliköllä, laatu- ja kantelupäälliköllä, tuloksellisuustarkastusjohtajalla, tilintarkastusjohtajalla, tilintarkastuspäälliköllä, tuloksellisuustarkastuspäälliköllä, tarkastusta ohjaamaan määrätyllä muulla virkamiehellä, omistajaohjausta tarkastavalla virkamiehellä, asiakirjahallinnon suunnittelijalla sekä tietoturvapäälliköksi määrätyllä virkamiehellä tietoturvallisuuskoulutuksen sekä perusmuotoisen turvallisuusselvityksen teon jälkeen. Pääjohtaja tai yksikön päällikkö voi myöntää tietoturvallisuuskoulutuksen sekä perusmuotoisen turvallisuusselvityksen teon jälkeen tilapäisen, tiettyä asiaa tai asiakirjaa koskevan käsittelyoikeuden työntekijälle, jonka työtehtävät sitä edellyttävät. Tilapäinen käsittelyoikeus merkitään kyseiseen asiakirjaan.

Suojaustasoihin III ja IV kuuluvien tietoaineistojen käsittelyoikeus on tarkastusvirastossa kaikilla tietoturvallisuuskoulutuksen suorittaneilla tarkastusviraston työntekijöillä heidän työtehtäviensä mukaisissa asioissa.

6.3 Tietoaineiston käsittely

Tarkastusvirastossa suojaustasoon III ja IV kuuluvat viranomaisen asiakirjat rekisteröidään samaan diaariin ja arkistoidaan samaan arkistoon julkisten asiakirjojen kanssa. Diaaritiedoista tulee käydä ilmi asiakirjan suojaustaso tai turvallisuusluokka. Asiakirja arkistoidaan ja säilytetään lukitussa tilassa erillään julkisista asiakirjoista. Tarkastustoiminnan yhteydessä laadittavista tai vastaanotettavista suojaustasoon III tai IV kuuluvista asiakirjoista on pidettävä tarkastuskohtaista luetteloa. Luettelo voi olla esimer-

kiksi sähköisen työtilan käyttöoikeuksin rajoitettu dokumenttikirjasto, jonka asiakirjaluetteloon merkitään suojaustasotieto.

Suojaustasoon II kuuluvat asiakirjat rekisteröidään omaan diaariinsa ja arkistoidaan omaan arkistoonsa. Samoin suojaustasoon I kuuluvat asiakirjat rekisteröidään omaan diaariinsa ja arkistoidaan omaan arkistoonsa.

Luokitelluista asiakirjoista voidaan ottaa sekä sähköisiä että paperimuotoisia kopioita. Kopiot tulee merkitä ja niitä tulee käsitellä kuten alkuperäisiä asiakirjoja. Kopion saajalla on oltava työtehtäviin perustuva oikeus salassa pidettävän tietoaineiston käsittelyyn.

Suojaustasoihin I ja II luokitellut paperimuotoiset asiakirjat säilytetään vähintään Euro II -normin mukaisessa data- tai kassakaapissa. Luonnokset eivät tee poikkeusta tästä. Suojaustasoon III ja IV kuuluvat asiakirjat tulee säilyttää lukitussa paikassa.

Suojaustasoihin I ja II kuuluvien asiakirjojen käsittelijän on merkittävä päivämäärä ja nimikirjoituksensa asiakirjaan tai sen kopioon käsitellessään sitä ensimmäistä kertaa. Suojaustasoihin I ja II kuuluvien asiakirjojen kopioinnista on tehtävä merkintä alkuperäiseen asiakirjaan ja kopiot on leimattava punaisella leimalla. Suojaustason I asiakirjan kopiointi on sallittu ainoastaan sen laatijan luvalla.

Suojaustason I tietoaineiston käsittelyä varten tietoyksikkö varaa erilliset vain tätä tarkoitusta varten tarkoitetut työasemat ja tulostimet. Työasemat on lainattavissa tietoyksiköstä. Työskentelyn päätyttyä työstetyt tiedostot poistetaan ja työasema palautetaan tietoyksikköön. Tietoyksikkö valmistelee työaseman seuraavaa käyttöä varten tarvittaessa ylikirjoittamalla koneen muistin ja säilyttää työaseman kassakaapissa.

Suojaustason II tietoaineiston tulostamiseen käytetään työasemakohtaista oheistulostinta. Verkkotulostimien käyttäminen on kielletty. Oheistulostin tulostusta varten on lainattavissa tietoyksiköstä.

Suojaustasoihin I ja II kuuluvia asiakirjoja ei saa tallentaa eikä käsitellä tarkastusviraston tietojärjestelmissä, tietoverkossa eikä niitä koskevia asioita saa käsitellä puhelimessa.

Suojaustasoihin III ja IV kuuluvaa tietoaineistoa saa käsitellä ja tallentaa tietoverkkoon kytketyssä työasemassa ja tulostaa verkkotulostimella, jos käyttäjä asettaa henkilökohtaisen turvatulostuskoodin tulosteiden noutamiseksi tai pystyy valvomaan, ettei kukaan muu saa tulosteita verkkotulostimesta käsiinsä. Tietoaineistoa saa tallentaa levyalueille ja tietojärjestelmiin siten, että tietoa voivat käsitellä vain siihen oikeutetut henkilöt.

Suojaustasoihin I ja II luokiteltua tietoaineistoa, tai niitä sisältäviä tietovälineitä, ei saa viedä virkapaikan ulkopuolelle ilman erillistä päätöstä tai lupaa.

Suojaustasoihin III ja IV kuuluvaa tietoaainestoa tai niitä sisältäviä tietovälineitä saa kuljettaa virkapaikan ulkopuolella työtehtäviin liittyen. Sähköiselle tietovälineelle tallennetut tiedot on oltava salattuja.

Liikuttaessa valtion virastojen ulkopuolella, julkisissa kulkuvälineissä tai tiloissa, joissa on läsnä tietoaaineston käytön kannalta ulkopuolisia henkilöitä, ei saa käsitellä salassa pidettävää tietoaainestoa missään muodoissa.

Salassa pidettävää tietoa saa siirtää ja taltioida vain viranomaisen hyväksymillä salausmenetelmillä suojattuna. Luokitellun tiedon siirtämisen, taltioinnin ja muun käsittelyn vaatimuksia on koottu tämän määräyksen liitteeseen 1.

Jokainen tarkastusviraston tietojärjestelmiä käyttävä henkilö vastaa omalla käyttäjätunnuksella tapahtuneesta tietojen käsittelystä. Käyttäjätunnuksen saamisen ehtona on sitoutuminen tarkastusviraston tietoturvalisuusohjeistuksen noudattamiseen. Käyttäjille luovutetut käyttäjätunnukset, salasana, tunnistuskortit, PIN ja PUK -koodit ja muut vastaavat tunnistet ovat henkilökohtaisia, ellei näitä luovutettaessa erikseen ole toisin määritelty. Edellä mainittua henkilökohtaiseksi tarkoitettua materiaalia ei saa luovuttaa muulle taholle tai toiselle henkilölle edes tilapäiseen käyttöön.

6.4 Tiedon antaminen salassa pidettävästä tietoaainestosta

Asiakirjan antamisesta päättää yleisen säännön mukaan se viranomainen, jonka hallussa asiakirja on. Viranomainen voi kuitenkin siirtää tiedonsaantipyynnön sille viranomaiselle, joka on laatinut asiakirjan tai jonka käsiteltävään asiaan se kuuluu. Kansainvälisistä tietoturvalisuusvelvoitteista annetun lain mukaan turvalisuusluokitellun asiakirjan saantia koskeva pyyntö on aina siirrettävä sille viranomaiselle, jolle sopimuspuoli on asiakirjan toimittanut.

Salassa pidettävästä asiakirjasta tai sen sisältämästä tiedosta saa antaa tiedon vain, jos niin on erikseen julkisuuslaissa tai muussa laissa säädetty. Tiedon antamisen salassa pidettävästä asiakirjasta ratkaistaan tarkastusviraston työjärjestyksen 27 ja 28 §:n mukaisesti.

6.5 Tietoaineiston toimittaminen vastaanottajalle ja vastaanottaminen

Asiakirjan allekirjoittaja määrää jakelun ja käsittelyprosessin. Lähettäjän on varmistettava, että salassa pidettävä asiakirja luovutetaan vain sellaiselle henkilölle, jolla on tehtäviinsä liittyvä oikeus käsitellä kyseistä asiakirjaa.

Suojaustasoon I luokitellun asiakirjan vastaanottajana on aina henkilö. Toimipisteestä lähetettävä aineisto toimitetaan vastaanottajalle lähettäjän tai vastaanottajan henkilökuntaan kuuluvan kuriirin välityksellä. Asiakirja pakataan mustaan läpinäkymättömään kirjekuoreen ja sen jälkeen tavalliseen kirjekuoreen. Kirjekuoret liimataan toisiinsa. Päällimmäinen kirjekuoren sulkemisen jälkeen se sinetöidään kulumista. Päällimmäiseen kirjekuoreen merkitään vastaanottaja, asiakirjan koodi (= vastaanottajan kappaleen numero), lähettäjä ja merkintä ”KURIIRIPOSTI”. Mustan kirjekuoren sijasta voidaan käyttää myös tähän tarkoitukseen valmistettua mustaa muovista asiakirjapussia.

Pakattu ja lähetettävä aineisto merkitään tämän jälkeen erilliseen kuriiripostiluetteloon. Luettelon ensimmäinen kappale annetaan kuriirille, joka toimittaa sen vastaanottajalle. Vastaanottaja palauttaa ensimmäisen kappaleen lähettäjälle joko kuriirin mukana tai postitse tarkastettuaan ensin, että vastaanotettu aineisto on täydellinen (ei puutu sivuja tai tiedostoja). Luettelon toinen kappale jää postin lähettäjälle varmistuskappaleeksi. Kuriiripostiluetteloita säilytetään yksi kalenterivuosi.

Suojaustasoon II kuuluva asiakirja voidaan kuriirin lisäksi toimittaa vastaanottajalle myös kirjattuna kirjeenä. Asiakirja pakataan kuten suojaustasoon I asiakirja. Postitusta ei saa suorittaa perjantaisin eikä juhla- tai vapaapäivien aattona. Suojaustasoon II kuuluva asiakirjan vastaanottaja voi olla henkilö tai organisaatio. Suojaustasoon II kuuluvaa aineistoa saa lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai -verkon välityksellä. Mikäli sähköisessä muodossa olevaa suojaustasoon II tietoaineistoa lähetetään manuaalisesti (esim. postin tai kuriirin välityksellä), tulee aineisto lähettää tallennettuna käyttämättömälle tietovälineelle ja vahvasti salattuna.

Suojaustasoon III kuuluvan tietoaineiston vastaanottaja voi olla henkilö tai organisaatio. Suojaustasoa III edellyttävän asiakirjan luovutus on oltava jäljitettävissä. Asiakirjan postitus merkitään diaariin tai tarkastuskoh- taiseen luetteloon. Asiakirja voidaan postittaa läpinäkymättömässä ja suljetussa kirjekuoreessa.

Suojaustasoa IV oleva asiakirja voidaan postittaa läpinäkymättömässä ja suljetussa kirjekuoreessa.

Asiakirjan vastaanottaja vastaa kaikista asiakirjan käsittelyyn liittyvistä velvollisuuksista käsittely- ja käyttöoikeuksineen. Jos asiakirja tulee suoraan vastaanottajalle, hänen on huolehdittava asiakirjan kirjaamisesta. Asiakirjan vastaanottaja tarkastaa, että käsittelystä vastaavalla henkilöllä on oikeus käsitellä luokiteltua asiakirjaa.

Vastaanotettaessa kansainvälistä turvallisuusluokiteltua tietoa (esim. EU, NATO) sähköisesti tai muilla menetelmillä tulee erikseen varmistua, mitä kahdenkeskisissä turvallisuussopimuksissa (vast.) asiasta on sovittu.

6.6 Tietoaineistojen hävittäminen

Tarpeettomat asiakirjakopiot ja tiedostokopiot tulee hävittää käyttötarpeen päätyttyä. Arkistoissa olevat asiakirjat hävittää kyseisen arkiston hoitaja. Asiakirjan valmistelija vastaa valmistelussaan olevien luonnosvaiheen asiakirjojen hävittämisestä. Sähköiset tiedostot tuhotaan tietovälineiltä, työasemilta ja palvelimilta sekä muilta laitteilta suojaustason edellyttämällä tavalla.

Suojaustasoon III ja IV kuuluvat asiakirjat on hävitettävä jättämällä ne tarkastusviraston valvotussa ja lukitussa tilassa olevaan lukittuun astiaan. Suojaustasoon I ja II kuuluvat asiakirjat voidaan hävittää vain silppuamalla. Suojaustasoon II kuuluvat asiakirjat voidaan hävittää silppurissa, jonka silpun koko on enintään 1,9 x 15 mm. Suojaustasoon I kuuluvat asiakirjat voidaan hävittää silppurissa, jonka silpun koko on enintään 0,78 x 11 mm. Astiat ja silppurit varustetaan merkinnällä, josta selviää, minkä suojaustason asiakirjoja astiaan voidaan jättää tai silppurilla hävittää.

Tarpeettomat tietovälineet on palautettava tuhottavaksi atk-tukeen, joka säilyttää niitä lukitussa tietosuojalaatikossa ja hävittää ne suojaustason III edellyttämällä tavalla. Suojaustasojen I ja II aineistoja sisältävät tarpeettomat tietovälineet on palautettava suojaustasojen I ja II arkistonhoitajalle, joka säilyttää niitä lukitussa kassakaapissa ja hävittää ne aina korkeimman suojaustason edellyttämällä tavalla.

7 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilavalvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan.

Fyysisen turvallisuuden tavoitteena on estää luvaton tunkeutuminen toimitiloihin ja siellä käytettäviin tai säilytettäviin tietoaineistoihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen. Tarkastusviraston toimitilaturvallisuuden päämääränä on suojata rakenteellisten ratkaisujen sekä teknisen valvonnan keinoin tarkastusviraston käytössä olevat tilat ja alueet niihin kohdistuvilta uhkilta ja minimoida vahingot.

Tarkastusviraston toimitilaturvallisuuden suunnittelun ja toteutuksen lähtökohtana on kansallinen turvallisuusauditointikriteeristö (KATAKRI) soveltuvin osin. Toimitilojen suojausluokan määräytymiseen vaikuttaa niihin sijoitettujen tietoteknisten järjestelmien tärkeysluokitus sekä niissä käsiteltävien tietoaineistojen turvallisuusluokitus.

Tarkastusviraston tilat jaetaan

1. asiakaspalvelu- ja neuvottelutiloihin
2. työhuoneisiin sekä
3. erityistiloihin.

Eryityksiä ovat tietotekniset laitetilat sekä arkistotilat.

Tarkastusviraston henkilökunnan tulee pitää henkilökorttia näkyvillä liikkueessaan tarkastusviraston tiloissa.

Jokaisen henkilöstöön kuuluvan veloitteena on osaltaan huolehtia siitä, ettei turvaluokiteltu tai arkaluonteinen aineisto ole vieraiden saatavilla tai nähtävissä asiakaspalvelu- tai neuvottelutiloista. Neuvottelutilan varaajan on tarkistettava ennen tilan käyttöä ja sen jälkeen, ettei neuvottelutiloihin ole jätetty muistivälineitä, salassa pidettävää aineistoa tai sinne kuulumattomia kannettavia tietokoneita. Vieraat tulee saattaa ulko-ovelta tai rappukäytävän ovelta asiakaspalvelu- ja neuvottelutiloihin ja sieltä pois tarkastusviraston henkilökuntaan kuuluvan valvonnassa. Vierailun isännän ei tarvitse ilmoittaa asiakaspalvelu- ja neuvottelutiloihin saapuvia vieraita etukäteen kulunvalvontaan eikä heillä tarvitse olla vierailajakorttia, mikäli isäntä on sopinut itse ottavansa vieraat vastaan ulko-ovella tai rappukäytävän ovelta.

Vierailun isännän on ilmoitettava Antinkadun toimipisteen työhuoneisiin ja erityistiloihin vietävistä vieraista etukäteen virastomestarille ja vie-

railun isännän on noudettava vieraat työhuoneisiin tai erityistiloihin 5. kerroksen aulasta. Turun ja Oulun toimipisteissä vierailun isännän on noudettava vieraat tarkastusviraston tilojen ulkopuolelta. Vierailun päättyessä isännän on saatettava vieras tarkastusviraston toimitilojen ulkopuolelle.

Työhuoneisiin saa päästää ulkopuolisia henkilöitä vain tarkastusviraston henkilökuntaan kuuluvan valvonnassa. Ulkopuolisen palveluntuottajan henkilöstö voi käydä työhuoneissa ilman valvontaa tehtäviinsä (esim. siivous) liittyen. Ulkopuolisen palveluntuottajan henkilöstöllä tulee olla esillä työnantajansa antama henkilökortti tarkastusviraston tiloissa työskennellessään. Työhuoneen ovi on lukittava sieltä poistuttaessa.

Erityistilojen tulee olla fyysisesti suojattuja luvattoman käytön, vahinkojen ja häiriöiden varalta. Ulkopuolisten pääsy (ml. siivous-, asennus- ja huoltotyöt) erityistiloihin, on sallittu vain tarkastusviraston henkilökuntaan kuuluvan valvonnan alaisena.

Suojaustasoihin I–II kuuluvan tiedon säilytystiloissa tulee olla jatkuva kulunvalvonta, rikosilmoitinjärjestelmä sekä dokumentoitu lukitusjärjestely.

8 Tietotekninen turvallisuus

8.1 Tietoliikenne

Tarkastusviraston ja eduskunnan lähiverkkoihin tai niihin kytkettyihin laitteisiin ei saa olla kytkettynä ylimääräisiä ulkoisia yhteyksiä, radiolaitteita eikä niitä saa kytkeä ristiin muiden verkkojen kanssa. Tietoliikenneverkoissa käytetään ainoastaan eduskunnan tai tarkastusviraston hyväksymiä päätelaitteita, verkkokomponentteja ja muita aktiivilaitteita. Hyväksyminen tehdään tietoliikenneverkosta riippuen joko järjestelmän käyttöönottopäätöksensä tai hankintapäätöksensä.

Salassa pidettävää tai arkaluonteista tietoaineistoa sisältävien tietojärjestelmien tietoliikenne tulee salata. Salaus tulee toteuttaa soveltuvalla tavalla siten, että tietoliikenne salataan palvelusta palvelua käyttävälle työasemalle saakka.

Eduskunta tuottaa tarkastusvirastolle Internet-yhteydet. Tämän vuoksi tarkastusvirastossa noudatetaan samoja periaatteita kuin eduskunnan virkamiesten internetin käytössä. Internet -yhteydet on tarkoitettu työhön liittyvään tiedonhakuun ja muuhun työtehtävien hoitamiseen liittyvään käyttöön. Lisäksi internetiä voi käyttää tavanomaisiin palveluihin kuten pankkipalveluihin. Työtehtäviin kuulumattoman materiaalin lataaminen internetistä ei ole sallittua, koska lataaminen saattaa estää viraston tehtäviin tarvittavan tietoliikennekaistan käyttöä. Tällaista materiaalia ovat muun muassa elokuvat ja ohjelmat.

Puhelut tai viestit ajanviete- ja aikuisviihdepalveluihin estetään Viestintäviraston teleliikenteen estoluokan P3 mukaisesti (35 O/2010 M, 6.9.2010).

Etäkäytöllä tarkoitetaan tilapäistä liittymistä tarkastusviraston tai eduskunnan palvelujen käyttäjäksi tavanomaisen toimipisteverkon ulkopuolelta. Tarkastusviraston etäkäyttö toteutetaan vain eduskunnan hyväksymiä etäkäyttöratkaisuja hyödyntäen.

Tietoyksikkö ohjeistaa, toteuttaa ja valvoo tietoliikenneyhteyksien rakentamisen ja varmentamisen. Tietoliikenneturvallisuutta valvotaan muun muassa verkonvalvonta-ohjelmistojen, tietoliikennelaitteiden lokitiedostojen, laskutusraporttien sekä käytön seurannan avulla.

8.2 Työasemat, oheislaitteet ja matkapuhelimet

Käyttäjät saavat käyttää vain tietohallinto henkilöstön heille käyttöön luovuttamia työasemia ja matkaviestimiä. Kaikki verkkoon liitettävät työasemat ja muut päätelaitteet liitetään verkkokäyttöjärjestelmään, järjestelmänhallintaohjelmistoon, keskitettyyn haittaohjelmien torjuntajärjestelmään ja keskitettyyn tietoturvapäivitysjärjestelmään. Käyttöön oton yhteydessä poistetaan työaseman käytön kannalta tarpeettomat ohjelmistot ja palvelut. Työasemiin määritellään ryhmäkäytäntöjen avulla käyttäjien kirjautumisten seuranta, joka kirjaa työaseman lokiin onnistuneet ja epäonnistuneet kirjautumiset. Kirjautumisia seurataan luvattomien käyttöyritysten paljastamiseksi.

Henkilökohtaisiin kannettaviin työasemiin asennetaan aina käyttöön hyväksytty kiintolevyn salausohjelma. Salausohjelman on käytettävä vahvan salauksen määrittelyä täyttävää algoritmia. Käyttäjä on erikseen pyydettyessä velvollinen palauttamaan työaseman tietohallinto henkilöstölle tarkastusta tai päivitystä varten. Kannettaviin työasemiin asennetaan aina etäyhteysohjelmisto, joka on varustettu palomuurilla ja johon on määritetty säännöt keskitetysti. Käyttäjä ei saa pystyä kytkemään etäyhteysohjelmistoa pois päältä.

Työasemia, joilla käsitellään suojaustason I aineistoja, ei saa kytkeä mihinkään verkkoon, ja niiden tietoturva- ja haittaohjelmapäivitykset asennetaan ilman verkkoyhteyttä.

Tietohallinto henkilöstö pitää työasemista ja oheislaitteista luetteloa, josta ilmenee työaseman sijoituspaikka, sen sarjanumero ja sen haltija. Materiaaliin laitetaan merkintä sen kuulumisesta tarkastusviraston omaisuuteen tai hallintaan.

Käyttäjän on säilytettävä kannettavaa työasemaa siten, että muilla ei ole mahdollisuutta saada työasemaa haltuunsa. Jos työasema joutuu ulkopuolisen käsiin tai katoaa, on asiasta viipymättä ilmoitettava lähimmälle esimiehelle sekä tietohallinto henkilöstölle.

Ellei liikenteen turvallisuusmääräyksistä muuta johdu, kannettava työasema on aina matkustettaessa kuljetettava käsimatkatavarana. Matkaliput on tilattava siten, että työaseman kuljetus käsimatkatavarana on mahdollista. Kannettavan työaseman kuljetuslaukussa ei saa kuljettaa salasanoja tai käyttäjätunnuksia. Työaseman tulee olla aina niiden haltijan valvonnassa. Tarkastusviraston työasemiin saa kytkeä ainoastaan tarkastusviraston hyväksymiä laitteita.

Poistuttaessa työtilasta, johon ulkopuoliset voivat päästä, käyttäjä kirjautuu ulos työasemaltaan ja lukitsee työtilan oven. Etätyössä on huoleh-

dittava, että perheenjäsenet ja muut ulkopuoliset eivät pääse käsiksi asiakirjoihin tai muihin tietoihin. Tiloissa, joissa on tai joihin voi nähdä tarkastusviraston ulkopuoliset henkilöt, on käytettävä näyttöjen suojana tietoturvasuojia. Työasemat määritellään keskitetysti lukittumaan 15 minuutin kuluessa siitä, kun työasemaa on lakattu käyttämästä.

Käyttäjä luovuttaa käytöstä poistettavat ja huoltoon lähetettävät työasemat, matkaviestimet ja oheislaitteet tietohallintohenkilöstölle. Tietoyksikkö ohjeistaa tietohallintohenkilöstön niiden käyttöönottamista, massamuistien tyhjentämistä tai poistamista, oletusasetusten palauttamista sekä huoltoon lähettämistä varten tehtäviksi toimenpiteiksi.

Jokainen matkaviestimen haltija on vastuussa sen asianmukaisesta käytöstä, myös luovuttaessaan matkaviestimen tilapäisesti tehtävän suorittamiseen osallistuvien muiden virkamiesten käyttöön. Muille matkaviestintä ei saa luovuttaa. Käyttäjän tulee erityisesti huolehtia matkaviestimen kuljetuksessa siitä, ettei laite pääse katoamaan. Matkaviestintä tulee pitää luotettavasti suljettuna erilliseen koteloon tai taskuun.

Omien SIM -korttien käyttö (myös tilapäinen) virkakäyttöön tarkoituisissa matkaviestimissä on kielletty. Matkaviestimien PIN -koodikysely ja suojakoodikysely on oltava päällä, ja käyttäjän tulee muuttaa ne oletusasetuksesta. Käyttäjän tulee muuttaa myös vastaajapalvelun tunnus oletuksesta.

Mikäli haittaohjelmien torjuntaohjelmisto ilmoittaa poikkeamasta, tai epäillään työasemassa tai matkaviestimessä olevan haittaohjelmia, on käyttäjän otettava välittömästi yhteyttä tietohallintohenkilöstöön.

Tietoyksikkö järjestää virka-aikana jatkuvasti käytettävissä olevan sen tasoisen käyttäjätuen, että käyttäjiä pystytään neuvomaan tavallisimmissa työasemien ja ohjelmistojen käyttöön liittyvissä ongelmissa. Tietoyksikkö vastaa laitteiden, ohjelmistojen ja tietoturvapäivitysten päivitys- ja muutostarpeen seurannasta ja toteuttamisesta.

8.3 Siirrettävät tietovälineet

Siirrettävät tietovälineet, pois lukien levykkeet, CD ja DVD -levyt merkitään tarkastusviraston omaisuudeksi. Mikäli tietoväline ei itsessään sisällä yksilöivää tunnistetta (sarjanumero), sisällytetään se edellä mainittuun merkintään. Tietohallintohenkilöstö pitää siirrettävistä tietovälineistä lueteloa, josta ilmenee tietovälineen yksilöivä tunniste ja henkilö kenelle tietoväline on luovutettu.

Tarkastusviraston työtehtäviin käytetään tarkastusviraston omistamia siirrettäviä tietovälineitä. Mikäli tarkastusviraston työasemaan täytyy väli-

aikaisesti liittää muu kuin tarkastusviraston omistama siirrettävä tietoväline, käyttäjän on varmistuttava siitä, että tietovälineellä ei ole haitta- tai vakoiluohjelmia.

Tarkastusviraston omistamia siirrettäviä tietovälineitä saa kytkeä ulkopuoliseen työasemaan vain silloin, kun tietovälineissä on kirjoitussuojaus päällä. Jos siirrettävä tietoväline on ollut kytkettynä ulkopuoliseen työasemaan, käyttäjän on varmistuttava siitä, että tietovälineellä ei ole haitta- tai vakoiluohjelmia ennen sen käyttöä tarkastusviraston työasemissa.

Automaattinen ohjelmien käynnistäminen siirrettävältä tietovälineeltä estetään keskitetyllä ryhmäkäytännöllä.

Siirrettäviä tietovälineitä säilytetään sen mukaisesti, mitä niille tallennettujen tietoaineistojen säilytysmääräykset edellyttävät. Siirrettävien tietovälineiden turvallinen käyttö koulutetaan henkilöstölle laitteen luovuttamisen yhteydessä.

8.4 Järjestelmien ja ohjelmistojen käyttö

Tarkastusvirastossa käytetään vain eduskunnan tai tarkastusviraston käyttöön hyväksymiä ohjelmistoja ja järjestelmiä. Tietohallinto säilyttää ohjelmistojen alkuperäismediat, lisenssiasiakirjat ja lisenssikoodit palo- ja varkausturvallisessa tilassa tai säilytyspaikassa.

Jokaisella tarkastusviraston virkamiehellä on oltava henkilökohtainen käyttäjätunnus kaikkiin tietojärjestelmiin, joissa on käyttäjän tunnistus. Salasanoja tulee säilyttää huolellisesti, eikä niitä saa luovuttaa toisen henkilön tai tahon käyttöön.

Salasanan tai asiointikortin luovuttaminen toisen henkilön käyttöön on kielletty. Käyttäjän tulee säilyttää asiointikorttiin kuuluvia PIN- ja PUK -koodit lukitussa paikassa erillään kortista. Käyttäjän tulee vaihtaa kaikkien laitteiden ja järjestelmien oletussalasanat käyttöönoton yhteydessä.

Tietojärjestelmien tekninen ylläpitäjä huolehtii järjestelmän käyttöön liittyvän tiedon siirron kontrolloinnista sekä dokumentaation ja lähdekoodin turvallisesta säilyttämisestä.

Internetin kautta saatavissa oleviin palveluihin rekisteröitymiseen ja niiden käyttöön on saatava tietoyksikön lupa, mikäli palvelun käyttö edellyttää tietoliikenneyhteyksien avaamista tai erillisen ohjelmiston asentamista tai tarkastusvirastolle voi kohdistua maksuja, vastuita tai velvollisuuksia rekisteröitymisestä tai käytöstä. Internet-palveluihin rekisteröidyttyessä ei saa käyttää samoja käyttäjätunnuksia ja salasanoja kuin työasemalle, verkkoon tai tietojärjestelmiin kirjauduttaessa käytetään.

Tietohallintohenkilöstö vastaa palvelimille tallennettujen tietoaineistojen säännöllisestä varmennuksesta.

8.5 Sosiaalinen media

Tarkastusviraston sähköisen työpöydän (Auditori) yhteydessä olevat sosiaalisen median työkalut ovat käyttöönottopäätöksen mukaisesti käytettävissä viraston sisäisesti. Tarkastusviraston www-sivuja käytetään ulkoiseen viestintään. Www-palvelun yhteydessä toimivia käyttöoikeuksin rajattuja työryhmätiloja (extranet) voidaan käyttää tarkastusviraston ja ulkopuolisten työryhmätyöskentelyyn. Muihin sosiaalisiin medioihin tarkastusviraston profiilin luomisesta päätetään tapauskohtaisesti erikseen.

Tarkastusviraston pääjohtaja, esikuntapäällikkö sekä viestintähenkilöstö esikuntapäällikön tai pääjohtajan toimeksiannosta voivat luoda virkatehtävien hoitamista varten profiilin sosiaalisen median palveluihin ja osallistua niissä tapahtuvaan viestintään käyttäen kirjautumisessa työnantajan tarjoamaa sähköpostiosoitetta, työpaikalta ja työaikana. Viestittäessä sosiaalisessa mediassa käsitellään vain julkista tietoa. Julkaistu aineisto sekä käytävät keskustelut tulee olla luonteeltaan objektiivisia, neutraaleja ja asiallisia. Tällöin ei osallistuta väittelyihin eikä oteta kantaa mahdollisiin omiin tai muiden ristiriitatilanteisiin. Provokatiivisiin tarkastusvirastolle osoitettuihin viesteihin ei reagoida. Laittomat, siveettömät, aggressiiviset sekä loukkaavat viestit pyritään poistamaan palvelusta siitä erikseen tiedottamatta. Tarkastusviraston viestintä valmistelee tarvittaessa tarkemman ohjeen viestinnästä sosiaalisessa mediassa.

Tarkastusviraston työntekijät voivat kirjautua yksikön päällikön tapauskohtaisesti myöntämällä luvalla sosiaalisen median palveluihin työ sähköpostiosoitteellaan ja käyttää palvelua työaikana työpaikalta seuratakseen työtehtäviinsä liittyvää keskustelua tai materiaalia. Keskusteluihin osallistuminen on mahdollista vain yksikön päällikön luvalla. Keskusteluissa esitettävät asiat on perustuttava tarkastuskertomuksissa esitettyihin havaintoihin tai kannanottoihin. Muunlainen sisällön julkaisu ei ole sallittua. Yksikön päällikön tulee ottaa lupaa koskevassa harkinnassaan huomioon palvelusta saatavat hyödyt, palvelun välttämättömyys, palvelun sopimusehdot, yksityisyyden suoja, käyttäjän osaaminen, tietoturvallisuus ja tarkastusviraston maineen hallinta.

Muu sosiaalisen median käyttö on tapahduttava vapaa-ajalla eikä siinä saa käyttää työnantajan tarjoamaa sähköpostiosoitetta tai laitteita, ohjelmistoja tai yhteyksiä. Tällöin on huomattava, että virkavastuu on voimassa myös vapaa-ajalla ja riippumatta siitä, mainitaanko tarkastusvirasto

työnantajana samassa yhteydessä vai ei. Muiden käyttäjien voi olla vaikea erottaa, milloin virkamies toimii verkossa yksityishenkilönä ja milloin virkamiehenä. Tämän vuoksi tulee harkita tarkkaan verkkoon tuotetun sisällön vaikutukset sidonnaisuuksien tai jääviyden syntymiseen sekä virkatehtävien asianmukaiseen hoitamiseen.

9 Toiminta poikkeustilanteissa

Hallintojohtaja tai hänen sijaisensa vastaa fyysisen turvallisuuden ja henkilöstöturvallisuuden tietoturvapoikkeamien selvittämisestä, tiedottamisesta ja tarkastusviraston muun johdon ja tietoturvapäällikön informoinnista.

Tietoturvapäällikkö tai tietojohtaja hänen sijaisenaan vastaa tietotekni- sen turvallisuuden ja tietoaineistoturvallisuuden tietoturvapoikkeamien selvittämisestä, tiedottamisesta, tarkastusviraston johdon informoinnista sekä kaikkien tietoturvapoikkeamien kirjaamisesta.

Tarkastusvirastossa on päätetty tietoteknisten järjestelmien omistajista, pääkäyttäjistä ja vastuuhenkilöistä (Dnro 324/09/2010, 18.2.2011). Kyseiset tahot ja henkilöt toimivat tarvittaessa tietoturvapoikkeamiin reagoinnissa järjestelmäkohtaisina avustajina ja yhteyshenkilöinä.

Järjestelmän pääkäyttäjä tai tekninen vastuuhenkilö voi reagoida virka- aikana poikkeamaan itse. Poikkeamasta on ilmoitettava esimiehelle ja tietoturvapäällikölle. Merkittävässä ja vakavimmissa tietoturvapoikkeamissa tietoturvapäällikkö, hallintojohtaja ja tarvittavat muut henkilöt kokoontuvat tietojohtajan johdolla arvioimaan tilannetta ja sen vaatimia toimenpiteitä. Virka-ajan ulkopuolella poikkeamiin reagoi ja toiminnan käynnistää tietojohtaja tai hallintojohtaja. Vakavista tietoturvapoikkeamista ilmoitetaan viraston muulle johdolle viivytyksettä.

Tietoyksikkö laatii tarkastusviraston tärkeimpien järjestelmien osalta toipumissuunnitelman ja ylläpitää sitä.

10 Toimenpiteet

Tämän määräyksen mukaiset tietoturvaliikkeitä, raportointi ja toiminta poikkeustilanteissa otetaan käyttöön välittömästi. Muilta osin määräyksen mukaiset menettelyt otetaan käyttöön 1.11.2011.

Tällä määräyksellä kumotaan

- VTV:n tietoturvaliikkeitä 30.4.2008
- VTV:n sähköpostin ja internetin käyttöliikkeitä 421/01/2002, 1.6.2003 (kumoutuu 31.10.2011)
- Työhuoneiden ovien lukitseminen 377/01/2001 (kumoutuu 31.10.2011)
- Henkilökortit 1.4.2002 lukien 197/01/2002 (kumoutuu 31.10.2011)
- Vierailijakortti 197/01/2002 (kumoutuu 31.10.2011).

Tietoyksikkö järjestää esimiestehtävissä toimiville ja koko henkilöstölle tietoturvaliikkeitä koulutuksen. Esimiesten on suoritettava koulutus 16.9.2011 mennessä ja jokaisen viraston henkilökuntaan kuuluvan 31.10.2011 mennessä. Mikäli henkilökuntaan kuuluva on virkavapaalla, on hänen suoritettava koulutus kuukauden kuluessa virkavapaan päättymisestä. Koulutuksen suorittamista seurataan.

Tietoyksikkö hankkii määräyksen edellyttämät kannettavien tietokoneiden näyttöjen tietoturvasuojat, matkaviestinten suojakotelot sekä uudet muistitikut 31.10.2011 mennessä. Käyttäjät vaihtavat vanhat muistitikut uusiin 31.10.2011 mennessä tietoyksikön antamien ohjeiden mukaan.

Hallintoyksikkö merkitsee lukitut asiakirjojen hävitysasiat ja silppurit suojaustasoluokilla sekä hankkii suojaustasojen I ja II hävittämiseen tarvittavan silppurin 31.10.2011 mennessä.

Hallintoyksikkö pyytää 16.9.2011 mennessä perusmuotoiset turvallisuusselvitykset henkilöistä, joille on tarkoitus antaa suojaustason I ja II pysyvät käsittelyoikeudet.

Tietoyksikkö laati tietoturvaliikkeitä perustason saavuttamiseksi tarvittavat kirjalliset ohjeet tietohallintohenkilöstöltä vaadittavista toimenpiteistä tietoteknisen ympäristön ylläpitämiseksi 15.12.2011 ja toipumissuunnitelman tärkeimpien järjestelmien osalta 15.2.2012 mennessä.

Tietoyksikkö valmistelee arkistosäännön ja arkistonmuodostussuunnitelman muutokset siten, että ne on uusittuina otettavissa käyttöön 1.1.2012.

Hallintoyksikkö hankkii yhdessä tietoyksikön kanssa tehdyn suunnitelman mukaisesti

- tarvittavat Euro II -normin kassakaapit sekä lukittavat kaapit arkistotiloihin
- erityistilojen kulunvalvonta-, lukitus- ja rikosilmoitusjärjestelmän muutokset

31.10.2011 mennessä.

Tarkastuksen toimintayksiköt päivittävät tarkastusohjeensa ja saattavat tarkastusaineistoarkistonsa tietoaineiston säilytyksen tämän määräyksen mukaiseksi 30.6.2012 mennessä.

Tämä määräys on käsitelty tarkastusviraston henkilöstöjärjestöjen kanssa 23.3.2011 sekä tarkastusviraston yhteistoimintakokouksissa 4.5.2011 ja 23.5.2011.

JAKELU

VTV henkilöstö

TIEDOKSI

Eduskunnan kanslia

Eduskunnan oikeusasiamiehen kanslia

Ulkopoliittinen instituutti

Liite 1. Työaseman käyttäjän tietoturvaohje

1. Säilytä salasanasi ja PIN -koodisi turvallisessa paikassa siten, että muut eivät voi saada niitä käsiinsä. Käytä salasanoissa vähintään 8 merkkiä, joista vähintään yksi on iso kirjain, yksi pieni kirjain ja yksi numero.
2. Älä päästä ketään muuta käyttämään tietoteknisiä järjestelmiä omilla käyttäjätunnuksellasi tai asiointikortillasi. Älä käytä toisen käyttäjätunnuksia tai asiointikorttia.
3. Älä asenna itse ohjelmia koneeseesi, äläkä tee muutoksia siihen jo asennettuihin ohjelmistoihin.
4. Tarkista vieraat tietovälineet (muistit) sekä vieraisissa koneissa käyttämäsi omat tietovälineet haittaohjelmien torjuntaohjelmalla ennen niiden käyttöä VTV:n koneessa. Säilytä tietovälineesi turvallisessa paikassa.
5. Säilytä tiedostosi palvelimella. Mikäli säilytät tiedostojasi muualla, ota niistä varmuuskopiot säännöllisesti. Tallenna tekemäsi työ poistuessasi koneelta.
6. Valmistellessasi tai vastaanottaessasi salassa pidettävää tietoaaineistoa, varmistu miten sitä tulee käsitellä.
7. Havaittuasi tietoturvasuutta vaarantavan seikan, ilmoita siitä esimiehellesi ja tietoturvapäälikölle.
8. Kirjautu ulos aina käyttämästäsi järjestelmästä ohjeiden mukaan. Lukitse työasema ja ovi poistuessasi työhuoneestasi.
9. Nouda tulosteet tulostimelta välittömästi tulostettuasi.
10. Muista, että tarpeeton Internetin selailu on tietoturvariski. Internetissä oleva tieto ei aina ole oikeaa ja se voi olla tekijänoikeuksin suojattua. Internetin käyttöä seurataan ja voidaan tarvittaessa rajoittaa. Käytä Internet -palveluissa eri salasanoja kuin viraston järjestelmissä.

Liite 2. Sitoumus tietoteknisten laitteiden käytöstä ja vaihtolosta

Tämän sitoumuksen allekirjoittamisella vakuutan noudattavani

1. tarkastusviraston tietoturvamääräystä
2. kannettavan tietokoneen ja sen etäyhteyden sekä matkapuhelimen ja matkapuhelinliittymän 5.11.2008 voimaan tulleita käyttöehtoja, jotka kuittaamalla saaduiksi.

Vakuutan, etten ilman lupaa tai toimeksiantoa tarkastusviraston virassa ollessani enkä sen jälkeenkään ilmaise asiaan kuulumattomille mitään tarkastusvirastoa tai sen toimintaa koskevaa asiaa enkä sellaista, minkä olen tehtävässäni saanut tietää, mikäli se on lain tai erityisen määräyksen mukaan nimenomaan taikka asian laadun vuoksi ilmeisesti salassa pidettävä.

Tarkastusvirastossa ___ päivänä _____kuuta 201___

Nimen selvennys

Allekirjoitus

Liite 3. Käyttöoikeuksien hakulomake tarkastusviraston tietojärjestelmiin

Järjestelmä (pääkäyttäjä)		
<input type="checkbox"/> AdeEko+(ARS)	<input type="checkbox"/> Basware (ARS)	<input type="checkbox"/> Credita (REK)
<input type="checkbox"/> Diaari (ANR)	<input type="checkbox"/> Esmikko/hallinta (ARH)	<input type="checkbox"/> Finlex/määr.kok (ANR)
<input type="checkbox"/> Hansel extranet (MIK)	<input type="checkbox"/> Heli (TIP)	<input type="checkbox"/> MobileServant (JEK)
<input type="checkbox"/> Oma Elisa (JEK)	<input type="checkbox"/> PrettyCirc (ANR)	<input type="checkbox"/> Prima (TIP)
<input type="checkbox"/> PVR (HEB)	<input type="checkbox"/> QPR Process Guide (PES)	<input type="checkbox"/> Rondo/VTV (ARS)
<input type="checkbox"/> Tahti (TIP)	<input type="checkbox"/> Webropol (TEK, HEB)	
Automaattisesti kaikille tulevat oikeudet: Active Directory, sähköposti, Esmikko/työaika, Komppi, Auditori, Citrix - etätyöpöytä, tekstiarkiston haku		
Käyttäjä		
<input type="checkbox"/> Käyttöoikeuden haku	<input type="checkbox"/> Käyttöoikeuden poisto	
Nimi	Rooli	
_____	_____	
<p>Käyttäjänä sitoudun käyttämään tietojärjestelmää vain työtehtävieni hoitamiseen. Olen lukenut järjestelmän käyttöohjeen ja VTV:n tietoturvamääräyksen ja sitoudun noudattamaan niitä. Ymmärrän, että järjestelmän väärinkäytökset voivat johtaa käyttöoikeuksien poistamiseen ja mahdollisesti rikosoikeudellisiin seuraamuksiin tai vahingonkorvauksiin. Minulla käyttäjänä on oikeus päästä käsiksi vain sellaisiin tietoihin, tietovälineisiin, järjestelmiin, tietoliikenneverkon osiin ja muihin resursseihin, joihin minulle on työtehtävien suorittamista varten annettu käyttöoikeus.</p> <p>Jonkun resurssin tekninen suojaamattomuus sellaisenaan ei anna käyttäjälle oikeutta tämän resurssin käyttöön. Vastaavasti tietoturvasuosohjeisiin liittyviä määräyksiä esimerkiksi salasanojen vaihtamisesta on noudatettava silloinkin, kun käytettävä tekniikka ei tähän erityisesti pakota. Jokainen tietojärjestelmiä käyttävä henkilö vastaa omalla käyttäjätunnuksellaan tietojärjestelmiin tehdyistä kyselyistä, syötöistä ja muutoksista.</p> <p>Tietojärjestelmään kirjautumisesta ja siinä tehdyistä toimenpiteistä voidaan tallentaa käyttäjän tiedot ja toimenpiteen tekoaika tietojärjestelmän lokiin.</p> <p>Päiväys _____ Allekirjoitus ja nimenselvennys _____</p>		
Esimies		
<p>Esimiehenä vakuutan varmistuneeni käyttäjän tarvitsevan haettavaa järjestelmää ja sen tietoja työtehtäviensä suorittamiseksi. Olen varmistunut siitä, että käyttäjä on perehtynyt järjestelmän käyttöohjeeseen ja VTV:n tietoturvamääräykseen. Valvon hakijan tietojärjestelmän käyttöä ja opastan häntä tietoturvasuuteen liittyvissä asioissa. Käyttäjän työtehtävien muuttuessa huolehdin siitä, että työtehtävien kannalta tarpeettomien tietojärjestelmien käyttöoikeudet poistetaan tai muutetaan uusiin työtehtäviin sopiviksi.</p> <p>Päiväys _____ Allekirjoitus, asema ja nimenselvennys _____</p>		
VTV:n pääkäyttäjä		
<p>Olen tarkistanut, että käyttöoikeushakemus on täytetty oikein ja haettu käyttöoikeus vastaa järjestelmän käyttöoikeusperiaatteita. Olen luonut käyttäjälle järjestelmään käyttöoikeudet ja informoinut häntä siitä.</p> <p>Päiväys _____ Allekirjoitus _____</p>		

Pääkäyttäjä säilyttää hakulomakkeen ja hävittää sen 5 vuoden kuluttua siitä, kun käyttäjän työsuhde on päättynyt. Ulkopuolisten omistamiin tietojärjestelmiin haetaan käyttöoikeuksia omistajan ohjeiden mukaan.

Liite 4. Kooste luokitellun tiedon käsittelystä

Käsittely	S U O J A U S T A S O			
	IV	III	II	I
1. Käsittely, laatiminen				
Tietoverkosta erillään oleva tarkastusviraston työasema	Kyllä	Kyllä	Kyllä	Kyllä
Tietoverkkoon kytketty tarkastusviraston työasema	Kyllä	Kyllä	Kyllä	Ei
Tarkastusviraston mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Etäkäyttö	Kyllä	Kyllä	Ei	Ei
2. Tulostus ja kopiointi				
Verkkotulostin tai verkkoon kytketty monitoimilaite, kun käytetään koodilla varustettua tulostusta	Kyllä	Kyllä	Ei	Ei
Verkosta erillään oleva tulostin tai monitoimilaite	Kyllä	Kyllä	Kyllä	Kyllä
3. Kirjaaminen				
Julkinen diaari	Kyllä	Kyllä	Ei	Ei
Suojaustason II asiakirjojen diaari	Ei	Ei	Kyllä	Ei
Suojaustason I asiakirjojen diaari	Ei	Ei	Ei	Kyllä
4. Lähettäminen				
Kirjaamaton kirje	Kyllä	Kyllä	Ei	Ei
Kirjattu kirje	Kyllä	Kyllä	Kyllä	Ei
Kuriiripostina	Kyllä	Kyllä	Kyllä	Kyllä
Salaamattomana sähköpostina tarkastusviraston ulkopuolelle	Ei	Ei	Ei	Ei
Salaamattomana sähköpostina tarkastusviraston sisällä	Kyllä	Ei	Ei	Ei
Salattuna sähköpostina, kun käytetään eduskunnan salattua sähköpostia tai salataan virkakortilla	Kyllä	Kyllä	Kyllä	Ei
Fax, vastaanottaja varmistettava	Kyllä	Ei	Ei	Ei
5. Hävittäminen				
Paperinkeräys	Ei	Ei	Ei	Ei
Lukittu tietosuojalaatikko	Kyllä	Kyllä	Ei	Ei
Silppuri, huomioitava silppurin luokitus (taso merkittävä silppuriin)	Kyllä	Kyllä	Kyllä	Kyllä
6. Säilyttäminen, tallentaminen				
Murtosuojattu tila, kuten kassakaappi tai holvi	Kyllä	Kyllä	Kyllä	Kyllä
Lukittu kaappi tai muu vastaava tila	Kyllä	Kyllä	Ei	Ei
Työtehtävien perusteella käyttöoikeuksin rajattu tiedostokansio tai sähköisen työpöydän työtila	Kyllä	Kyllä	Ei	Ei
Tietoverkkoon kytketty tarkastusviraston työasema	Kyllä	Kyllä	Kyllä	Ei
Tietoverkosta erillään oleva tarkastusviraston työasema	Kyllä	Kyllä	Kyllä	Kyllä
Tarkastusviraston omaisuudeksi merkityt salatut tallennusmediat ja muistilaitteet	Kyllä	Kyllä	Kyllä	Kyllä
Tarkastusviraston mobiililaitteet	Kyllä	Kyllä	Ei	Ei