



VALTIOVARAINMINISTERIÖ

# HENKILÖSTÖN TIETOTURVAOHJE

10/2006



VALTIONHALINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

# **HENKILÖSTÖN TIETOTURVAOHJE**

10/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN  
JOHTORYHMÄ

VAHTI

**VALTIOVARAINMINISTERIÖ**

Snellmaninkatu 1 A

PL 28

00023 VALTIONEUVOSTO

**Puhelin**

(09) 160 01

**Telefaksi**

(09) 160 33123

**Internet**

[www.vm.fi](http://www.vm.fi)

**Julkaisun tilaukset**

Sähköposti:

[asiakaspalvelu.prima@edita.fi](mailto:asiakaspalvelu.prima@edita.fi)

Puh. (09) 160 33287

ISSN 1455-2566

ISBN 951-804-664-6 (nid.)

ISBN 951-804-665-4 (pdf)

Edita Prima Oy

HELSINKI 2006



Ministeriöille, virastoille ja laitoksille

**HENKILÖSTÖN TIETOTURVAOHJE**

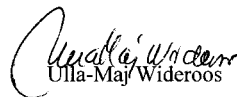
Valtiovarainministeriön ohessa antaman tietoturvaohjeen (jäljempänä ohje) tavoitteena on kehittää ja tukea hallinnon henkilökunnan tietoturvatyötä. Ohje korvaa valtiovarainministeriön aiemmin antaman Käyttäjän tietoturvaohjeen (VAHTI 5/2003). Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on ohjannut ohjeen uudistamista osana valtion tietoturvallisuuden kehitysohjelmaa (VAHTI-julkaisu 1/2004).

Ohjeen tarkoituksena on toimia hallinnon henkilöstön tietoturvatyötä koskevana yleisohjeena ja se soveltuu kaikille hallinnon työntekijöille. Ohjeessa on tiiviisti kuvattu tietoturvallisuuden perusasiat ja siinä annetaan käytännön neuvoja tietoturvallisuuden toteuttamiseen osana hallinnon perustyötä ja tehtävien hoitamista.

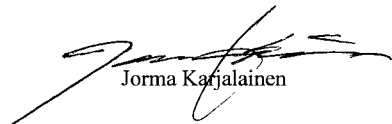
Valtionhallinnon yksiköissä tulee huolehtia henkilökunnan tietoturvatietoisuuden ylläpidosta, kehittämisestä ja kouluttamisesta sekä siitä, että koko henkilökunnalla on tietoturvallisuuden perustuntemus. Valtiovarainministeriö suosittelee ohjeen jakamista hallinnon kaikille työntekijöille osana hallinnon tietoturvatyötä ja -koulutusta.

Ohje tulee VAHTIn Internet-sivuille ([www.vm.fi/vahti](http://www.vm.fi/vahti)). Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle ([hko@vm.fi](mailto:hko@vm.fi)). Lisätietoja antaa neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kiviniemi ([etunimi.sukunimi@vm.fi](mailto:etunimi.sukunimi@vm.fi))

Toinen valtiovarainministeri

  
Ulla-Maj Wideroos

Ylijohtaja

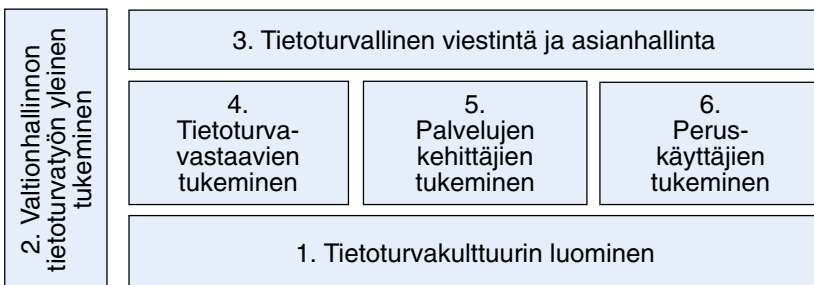
  
Jorma Karjalainen**Liite** Henkilöstön tietoturvaohje (VAHTI 10/2006)

## ESIPUHE

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) on yli kymmenvuotisen toimintansa aikana vakiinnuttanut asemansa hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimenä.

Valtiovarainministeriön johtamalla ja Valtion tietoturvallisuuden johtoryhmän VAHTI koordinoimalla valtion tietoturvallisuuden kehitysohjelmalla (VAHTIn julkaisu 1/2004) kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Seuraavassa kuvassa esitetyissä kuudessa kehitysohjelman osa-alueessa on yhteensä 29 laajaa kehittämiskohdetta.

### ***Kaavio valtion tietoturvallisuuden kehitysohjelmasta ja sen hankealueista***



Kehitysohjelman aikana merkittävää kehitystyötä on toteutunut kaikilla ohjelman hankealueilla ja yhteensä 26:ssä kehittämiskohteessa. Toteuttamiseen osallistuvat laajasti kaikki hallinnonalat ja osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä muita asiantuntijoita. Valtionhallintotasolta nimettyjä osallistujia hankkeissa on ollut yli 300.

Tämän ohjeen on laatinut VAHTIn alainen peruskäyttäjien tietoturvatyön jaosto. Ohje on hyväksytty VAHTIn kokouksessa marraskuussa 2006. Ohje korvaa valtionhallinnon aiemman peruskäyttäjien tietoturvaohjeen (VAHTI 5/2003).

## Sisällysluettelo

1	JOHDANTO .....	9
1.1	Keskeiset ohjeet .....	9
1.2	Mitä tietoturvallisuudella tarkoitetaan? .....	10
1.3	Miksi tietoturvallisuus on tärkeää? .....	11
1.4	Lainsäädäntö tietoturvallisuuden perustana .....	11
2	ASIANHALLINTA JA TIETOJEN KÄSITTELY .....	13
2.1	Työhön liittyvät tiedot .....	13
2.2	Haastattelut, kyselyt, tutkimukset ja tietojen luovutus .....	15
2.3	Omat tiedot ja yksityisyys .....	15
3	TYÖPAIKALLA .....	17
3.1	Tietokoneen käyttö .....	17
3.2	Käyttöoikeudet ja salasana .....	17
3.3	Internet ja sähköposti .....	18
3.4	Toimitilojen turvallisuus .....	20
4	LIIKKUVA TYÖ, ETÄTYÖ JA MATKATYÖ .....	23
4.1	Liikkuva työ ja mobiililaitteet .....	23
4.2	Etätyö ja etäkäyttö .....	23
4.3	Kotikoneella .....	24
4.4	Matkatyö .....	25
5	ONGELMATILANTEET .....	27
5.1	Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa .....	27
5.2	Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa .....	27
5.3	Seuraamukset .....	28
6	MISTÄ SAA LISÄTIETOJA? .....	29
	Liite 1: Tietoturvallisuuteen keskeisesti liittyvät säädökset .....	31
	Liite 2: Voimassa olevat VAHTI-julkaisut .....	33

# 1 JOHDANTO

Tietoturvallisuus perustuu lainsäädäntöön ja normiohjaukseen. Vastuu tietoturvavallisuudesta ja siihen liittyvä osaaminen kuuluu omalta osaltaan jokaiselle, myös sinulle. Tämä tietoturvaohje on tarkoitettu koko julkishallinnon henkilöstölle, sen toimeksiantonosta työskenteleville (esim. palvelutoimittajat) ja sen tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. opiskelijat). Ohjetta voidaan soveltaa käyttäen myös muissa kuin julkishallinnon organisaatioissa.

Ohjeeseen on koottu keskeisimmät tietoturvallisuuden perusasiat. Se antaa neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa. Teksti on pyritty kirjoittamaan siten, että se sopii mahdollisimman moneen organisaatioon. Kussakin organisaatiossa voi kuitenkin olla toiminnan erityisluonteesta johtuen tätä ohjetta koskevia poikkeuksia, lisäyksiä ja täsmennyksiä, joita luonnollisesti tulee noudattaa. Ja kun saat hyvän idean parantaa tietoturvallisuutta, tee siitä aloite.

## 1.1 Keskeiset ohjeet

1. Seuraa tietoturvallisuuteen liittyviä tiedotteita, tutustu ohjeisiin ja osallistu sinulle tarjottuun koulutukseen. Toimi saamiesi ohjeiden mukaisesti.
2. Tue osaltasi organisaation kulunvalvontaa ja käytä organisaation toimitiloissa kuvallista henkilökorttiasi (mikäli sellainen on annettu).
3. Älä jätä vierasta yksin tai valvomatta työhuoneeseesi tai muihin organisaation tiloihin.
4. Älä anna ulkopuolisen käyttää tietokonettasi.
5. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydällä salassa pidettäviä aineistoa.
6. Käsittele tietoja huolellisesti välineestä riippumatta – olipa tiedon välittäjänä siten henkilö, tietokone, paperi, puhelin tai telekopio.
7. Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön käyttöön – älä edes tietohallintohenkilöstölle, koska he eivät niitä tarvitse.
8. Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluontoista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja.
9. Vaihda salasanat riittävän usein ja heti, kun epäilet niiden paljastuneen.



10. Käytä tietoaineistoja ja työvälineitä vain työtehtäviesi hoitamiseen.
11. Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei tämä kuulu työtehtäviisi.
12. Tallenna tekemäsi työ verkkopalvelimen levyille, mistä tiedot varmistetaan keskitetysti.
13. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
14. Muista, että organisaation laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnytt tietoverkossa aina – tahtomattasikin – organisaation edustajana.
15. Käytä aina asianmukaista salausta, mikäli sinun on siirrettävä Internetin kautta salassa pidettävää tietoa.
16. Mikäli siirrät aineistoa muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.
17. Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi.
18. Työpäivän päättyessä kirjaudu tietojärjestelmästä ulos ja sammuta työasemasi organisaatiokohtaisen ohjeen mukaisesti.
19. Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi tietoturvavastaavalle, tietohallinto-organisaatioon tai omalle esimiehellesi. Heidän velvollisuutenaan on ryhtyä tarvittaaviin toimenpiteisiin.
20. Pyydä tarvittaessa neuvoa organisaatiosi asiantuntijoilta.

## 1.2 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvajärjestelyjen tarkoituksena on, että tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyvät riskit ovat hallinnassa. Tietoturvallisuus on osa organisaation toiminnan laatua.

Käytännössä tämä merkitsee mm. sitä, että osa tiedoista ja tietojärjestelmistä pidetään vain niiden käyttöön oikeutettujen saatavilla. Tällöin sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään. Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, häittäohjelmien, laitteisto- tai ohjelmistovikojen tai muidenkaan vahinkojen ja tapahtumien seurauksena. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin kun niitä tarvitaan. Sähköisen asioinnin yleistyttyä on lisäksi entisestään korostunut vaatimus, että asioinnin osapuolet tunnistetaan luotettavasti ja että asiointitapahtumien olemassaolo ja sisältö voidaan jälkikäteenkin todistaa.

## 1.3 Miksi tietoturvallisuus on tärkeää?

Tietoturvatoinenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Tietoturvalisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Yhteiskunnan toiminnot ovat nykyään suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta. Verkottuneessa toimintaympäristössä harva organisaatio on enää vastuussa yksinomaan omasta tietoturvallisuudestaan.

Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki – ei siis vain tekniikka vaan myös jokapäiväiset toimintatapamme ja asenteemme. Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta.

## 1.4 Lainsäädäntö tietoturvallisuuden perustana

Julkishallinnossa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Suomen lainsäädännössä on laajasti tietoturvavelvoitteita – toisin sanoen myös lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain ja asetuksen lisäksi useisiin muihinkin lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Julkisuuslainsäädännön mukaan tieto on julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole salassa pidettävää. Tietojen lain mukaisesta käsittelystä on aina huolehdittava.

“Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä.” (Laki viranomaisten toiminnan julkisuudesta 18§ , Hyvä tiedonhallintatapa)

“Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalla tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelylvä.” (Henkilötietolaki 32§ , Tietojen suojaaminen)

Tietoturvallisuuteen keskeisesti liittyvien säädösten luettelo on koottu tämän ohjeen liitteeksi.

## 2 ASIANHALLINTA JA TIETOJEN KÄSITTELY

Asianhallinta tarkoittaa organisaation toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia sekä asiakirjamuodossa olevien tietojen (asiakirjalliset tiedot) hallintaa.

Asiakirjalliset tiedot ovat osa organisaation pääomaa, jolloin niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen.

Tiedolla puolestaan tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai matkapuhelimen muistissa, ääni- tai kuvanauhassa tai vaikkapa yksittäisen ihmisen muistissa. Tietoa on tarkasteltava tiedon koko elinkaaren ajalla, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen.

Tietoja käsiteltäessä tulee huomioida, että käsiteltävät tiedot ovat usein merkittävästi arvokkaampia kuin tietojen käsittelyyn mahdollisesti liittyvä tekninen väline.

### 2.1 Työhön liittyvät tiedot

- Selvitä itsellesi tietojen ja asiakirjojen luokittelu ja siihen liittyvät käyttöä, luovutusta ja käsittelyä koskevat säännöt ja rajoitukset. (VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 2/2000 Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 4/2002 Arkaluonteiset kansainväliset tietoaineistot).
- Mikäli laadit salassa pidettävää asiakirjaa, vastaat tehtäviesi mukaisesti myös sen luokittelusta ja merkinnästä. Osa salassa pidettävästä aineistosta kuuluu turvluokittelun piiriin.

- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo myös syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Tallenna tekemäsi työ mahdollisuuksien mukaan palvelimelle, jonka varmuuskopiointista tietohallinto-organisaatio huolehtii. Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella laitteella tai tietovälineellä, jonka varmuuskopiointi on epäsäännöllistä.
- Mikäli aineistoa siirretään muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti. Varo tilannetta, jossa omalla tietovälineelläsi olisi siirrettävän tiedoston lisäksi muuta aineistoa salaamattomana.
- Varo toimistojärjestelmäsovelluksilla (esim. tekstinkäsittely, esitysgrafiikka, taulukkolaskenta) tehtyjen tiedostojen piiloon jääviä tietoja (ns. meta-, jäännös- ja piilotiedot) erityisesti organisaation ulkopuolelle tiedostoja lähettäessäsi tai tietovälineellä siirtäessäsi. Tiedosto voi sisältää siinä aiemmin ollutta tietoa tai muuta järjestelmässä olevaa tietoa, vaikka se ei näytöllä näkyisikään.
- Tarkista organisaatiosi ulkopuolelta tuotu muistitikku, CD-/DVD-levy tai muu tietoväline virustorjuntaohjelmalla ennen käyttöä organisaatiokohtaisen ohjeen mukaan.
- Mikäli joudut lähettämään salassa pidettävää aineistoa, lähetä se salattuna. Varmistu, että vastaanottaja on oikeutettu sen saamaan ja että lähetys on mennyt perille. Telekopiota voi vain poikkeustapauksissa käyttää salassa pidettävän aineiston lähettämiseen. Varmistu tällöin, että vastaanottaja on paikalla.
- Vältä turhaa tulostamista ja kopiointia, koska ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet (kustannus- ja ympäristövaikutusten ohella) lisäävät tiedon väärin käsiin joutumisen vaaraa ja siten turvaamistehtäviä erityisesti säilyttämisen tai hävittämisen osalta.
- Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkotulostimesta heti tulostuksen jälkeen.
- Käytä salassa pidettäviä tietoja hävittäessäsi suojausluokituksen mukaisia silppureita tai hävittämispalveluun kuuluvia keräyssäiliöitä.

## 2.2 Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation tiedotuspolitiikan mukaisesti.
- Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa salassa pidettävistä ja yksityisyyden suojan piiriin kuuluvista tiedoista.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt aineiston vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Mikäli aineisto luovutetaan tietovälineellä sähköisessä muodossa, tulee käytettävän tietovälineen ehdottomasti olla uusi ja aiemmin käyttämätön.

## 2.3 Omat tiedot ja yksityisyys

- Käytä henkilökohtaiseen viestintääsi yksityistä (itse hankittu, työnantajasta riippumaton) sähköpostiosoitettasi.
- Omia henkilökohtaisia tiedostoja ei pidä tarpeettomasti tallentaa työpaikan matkapuhelimeen, työasemaan tai palvelimelle.
- Kaikki ovat vaitiolovelvollisia toisten viesteistä, jotka on työtehtävissään vahingossa saanut tietoonsa.
- Tukahduta juurut.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, myös sähköpostiliikenteestä ja Internet-selauksesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäyttöksiin voidaan puuttua. Ks. tarkemmin organisaatiokohtaisesta ohjeistuksesta.

## 3 TYÖPAIKALLA

### 3.1 Tietokoneen käyttö

Tietokoneen käyttö sisältää sekä oman työaseman että verkon kautta käytettävien palveluiden käytön.

- Vastaat käyttäjänä omasta koneestasi. Ole siis huolellinen.
- Vain tietohallinto-organisaatio saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia.
- Kirjautu koneelle aina omilla käyttöoikeuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (Windows-työasemalla paina Ctrl+Alt+Del ja valitse Lukitse tietokone) aina kun poistut työpisteestäsi. Lisävarmistuksena voit myös käyttää salasanasuojattua näytönsäästäjää. Toimi organisaatiokohtaisen ohjeistuksen mukaisesti.
- Tallenna työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut työpisteestäsi.
- Tallenna kaikki tärkeä tieto sellaisen verkkopalvelimen levyille, josta tietohallinto-organisaatio ottaa säännöllisesti varmuuskopiot.
- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku tai CD-/DVD-levy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Huolehdi hävittämisestä organisaation ohjeistuksen mukaisesti tai toimita tallennusväline tietohallinto-organisaatioon hävitettäväksi.
- Kirjautu ulos sekä ohjelmistoista että koneeltasi ja sammuta tietokoneesi työpäivän päättyessä organisaation ohjeistuksen mukaisesti.

### 3.2 Käyttöoikeudet ja salasanat

Tietojärjestelmiin tarvitaan käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on yhdistetty juuri sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön – älä edes tietohallinnolle. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja välttävät jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa voi olla pieniä ja isoja kirjaimia, numeroita ja jopa erikoismerkkejä. Kaikkiin järjestelmiin ei kuitenkaan käy erikoismerkit. Hyvä salasana on sinun helppo muistaa, mutta vaikea ulkopuolisen arvata.
- Älä kirjoita salasanoja muistiin – ainakaan sellaiseen paikkaan, mistä ne ovat helposti löydettävissä.
- Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa Internetin palveluihin rekisteröityessäsi.
- Mikäli joissain tilanteissa tai järjestelmissä on pakko käyttää yhteistunnuksia, siitä päättää järjestelmän tai tietojen omistaja. Yhteistunnusten käyttö on sallittu vain omistajan luvalla. Yhteistunnuksen salasana täytyy vaihtaa aina, kun jonkun käyttäjän käyttöoikeus siihen lakkaa tai epäillään jonkun ryhmään kuulumattoman saaneen sen tietoonsa. Salasana tulee muutoinkin vaihtaa riittävän usein.

## 3.3 Internet ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä sekä tiedon hakuun että yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa tai Internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Sähköpostin ja Internetin käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi.
- Käytä vain sellaisia palveluita, jotka tiedät asiallisiksi.
- Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista vahvaa salausta. Tällaiset viestit ja liitetiedostot on salattava tietohallinto-organisaation hyväksymillä tuotteilla.
- Opettele salaustuotteiden oikea käyttö, jotta tieto ei vahingossa lähde salaamattomana.
- Ohjelmien lataus Internetin kautta voi olla organisaatiossasi kokonaan kiellettyä. Tällöin tietohallinto-organisaatio asentaa kaikki tarvittavat ohjelmat. Mikäli organisaatiokohtaisen ohjeistuksen ja työtehtäviesi perusteella lataat ohjelmia, pyri aina varmistumaan ohjelmiston ja lähteen luotettavuudesta.
- Jos käytät julkisia päätteitä tai tilapäisesti toisen henkilön hallussa olevaa tietokonet-

ta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies). Pyydä tarvittaessa tietohallinnolta apua.

- Muista, että viranomaisella on velvollisuus käsitellä virkasähköposti.
- Virkasähköpostia saa käsitellä vain oman organisaation tai mahdollisesti muun julkishallinnon organisaation omistamilla laitteilla.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan oman organisaation sähköpostijärjestelmään. Sitä ei saa ohjata tai jatkolähetetään organisaation sähköpostijärjestelmän ulkopuolelle.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat, vireille saateutut asiat organisaation määrittelemään sähköpostiin.
- Muista, että vastaat henkilökohtaiseen sähköpostiin tulevasta työpostista virkavelvollisuuksien mukaisesti.
- Muiden kuin virkasähköpostin (esimerkiksi Internetin ilmaissähköpostiohjelmat tai kotisähköposti) käyttö töissä on sallittua vain oman organisaation luvalla.
- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana virkavelvollisuuksien mukaisesti.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä, vaan toimi ohjeistuksen mukaisesti. Tarvittaessa voit ilmoittaa asiasta tietohallintoon.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se kannattaa tuhota heti. Jos viestiin vastaa, tietää roskapostittaja sähköpostiosoitteesi toimivaksi ja jatkaa roskapostien lähettämistä ja lisäksi välittää osoitteesi myös muille roskapostittajille.
- Älä anna työ sähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Ole terveen epäluuloinen sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös virukset voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä. Varo ns. ”kalasteluviestejä”, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin.
- Älä välitä ketjukirjeitä eteenpäin.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaihtolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa ja se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiointoa, jos haluat estää jakelulistalla olevien osoitteiden näkymisen vastaanottajille.



- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä. Esimerkiksi joulutervehdysten lähettäminen kuormittaa sekä sähköpostijärjestelmää että vastaanottajan sähköpostilaatikkoo.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä virkapostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit.

## 3.4 Toimitilojen turvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaisteja sisältävien lähetysten turvallisuuden.

- Suuntaa asiakaspalvelupisteessä ja -tilanteessa tietokoneesi näyttö harkitusti – onko tarkoitus, että tiedot näkyvät asioijalle vai ei?
- Noudata kulunvalvonnasta annettuja ohjeita. Käytä organisaation toimitiloissa kuivallista henkilökorttiasi (mikäli sellainen on annettu).
- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Jokaisella vieraalla tulee olla isäntä. Isäntä vastaa vieraidensa oleskelusta ja kulemisesta toimitiloissa.
- Pyri käyttämään vierailuihin neuvottelutiloja.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaankuulumatonta materiaalia. Vastaavasti neuvottelun päättyessä huolehdi, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä luottamuksellisia aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvassa, mahdollisuuksien mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitteita lukitussa tilassa. Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperituloiteiden ym. asianmukaisesta säilyttämisestä.
- Noudata “puhtaan pöydän” periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin toimitiloihin.
- Kuvaaminen organisaation tiloissa voi olla kiellettyä – noudata organisaatiokohtaista ohjeistusta. Valvo myös vieraidesi toimintaa ja esim. kamerakännyköiden käyttöä.

- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.
- Ohjaa vieraat tai “eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten suljettuina pidettäväksi tarkoitettuja ovia auki.

## 4 LIIKKUVA TYÖ, ETÄTYÖ JA MATKATYÖ

### 4.1 Liikkuva työ ja mobiililaitteet

Monet liikkuvan työn välineet voivat vastata ominaisuuksiltaan ja sisällöltään työpaikan työasemia. Laitteet eivät enää ole esim. pelkkiä puhelimia. Liikkuvan työn välineisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteämmin asennettuihin, joten kyseeseen tulevat soveltuvien osin samat turvallisuusohjeet. Kun välineitä lisäksi kuljetetaan ja käytetään työpaikan toimitilojen tarjoamien turvatoimien ulkopuolella, tarvitaan erityistä huolellisuutta.

- Huolehdi työnteossa käyttämiesi kannettavien tietokoneiden, matkapuhelinten, kommunikaattoreiden ja kämmentietokoneiden turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin (mm. PIN-kyselyt, Bluetooth-asetukset, sovellusten lataaminen).
- Huolehdi, että matkapuhelimessasi on päällä PIN-kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat PIN-koodit.
- Älä lataa ja asenna laitteisiin mitään työhön kuulumatonta.
- Käytä tietojen salausta mahdollisuuksien mukaan.
- Huolehdi tietojen varmuuskopioinnista ja/tai tarvittaessa synkroinnista muuhun tietojärjestelmään organisaatiokohtaisen ohjeen mukaisesti.

### 4.2 Etätö ja etäkäyttö

Etätöillä tarkoitetaan muualla kuin organisaation vakituksessa toimipisteessä suoritettavaa työtä. Tyypillinen etätö on kotoa tehtävää toimistotyötä. Etätöitä voidaan

tehdä myös muusta vakituisesta paikasta (esim. organisaation järjestämä etätyöpaikka) tai matkoilla (esim. hotelli tai toisen organisaation tilat), jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys. Etäyhteys on tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknisten palvelujen käyttöä etäyhteyden avulla. Langattomien verkkoyhteyksien yleistyessä etätyöntekijän on entistä useammin kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallesiin menettelytapoihin. Erityisen tärkeää tämä on toimittaessa vakituisten toimistotilojen ulkopuolella. Etätyössä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi organisaation varsinaisissa toimitiloissa.
- Etätyö on sallittua vain, jos siitä on tehty erillinen sopimus. Etäkäytön osalta tarkista asia organisaatiokohtaisesta ohjeistuksesta.
- Muista, että kaikkea organisaatiossa tehtävää työtä ei voida tehdä tietoturvallisesti etätyönä. Tunnista nämä työt. Joidenkin järjestelmien etäkäyttö voi olla kielletty tai estetty.
- Pääsääntöisesti työnantaja hoitaa etäkäytössä vaadittavien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien hankinnan ja asentamisen.
- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
- Huolehdi, että käyttämäsi käyttäjätunnukset, salasana, mahdolliset toimikortit ja muut todennusvälineet ovat vain sinun hallussasi ja tiedossasi.
- Käytä sovittuja suojausohjelmia ja varmista, että ne ovat ajan tasalla.
- Kuljeta mukana vain välttämätön määrä tietoaineistoa ja varmista aina aineiston asianmukaisesta suojauksesta.
- Asiakirjojen käsittelyssä on noudatettava samoja periaatteita kuin normaalisti, etätyön erityisriskit huomioon ottaen. Etätyö on rajattava aineistoon, jonka paljastuminen ei vaaranna tietoturvallisuutta. Myös etätyössä on otettava huomioon aineiston luokittelu ja siihen liittyvät käytösäännöt sekä luovutusta, käyttöä ja käsittelyä koskevat rajoitukset.
- Huolehdi tietoaineistosi varmuuskopioinnista sekä turvallisesta säilytyksestä ja hävittämismenettelystä.

### 4.3 Kotikoneella

Mikäli sinulla on oma tietokone ja Internet-liittymä, on tärkeää huolehtia myös niiden tietoturvallisuudesta.

- Pyydä ajoittain luotettavaa tietotekniikka-asiantuntijaa tarkistamaan, että työasemaympäristösi on turvallinen.
- Tee jokaiselle käyttäjälle omat henkilökohtaiset tunnukset, joilla on vain ns. normaalikäyttäjän oikeudet.
- Käytä ylläpitäjän tunnusta (esim. Järjestelmänvalvoja, Administrator) vain ylläpito-tehtäviin.
- Asenna vain virallisia, ajan tasalla olevia ohjelmistoja.
- Huolehdi käyttöjärjestelmän ja muun varusohjelmiston jatkuvasta automaattisesta päivittämisestä.
- Käytä tunnettua ja hyvämaineista tietoturvaohjelmopakettia (sis. mm. virustorjunta, palomuuuri, vakoiluohjelmatorjunta, roskapostisuodatus) ja huolehdi sen jatkuvasta automaattisesta päivittämisestä.
- Älä avaa epäilyttäviä sähköpostiviestejä ja -liitteitä.
- Tee säännöllisesti varmuuskopiot ja harjoittele niiden käyttöönottoa.
- Kun kirjautut Internetin palveluihin ja teet esim. ostoksia, käytä vain luotettavia palveluita ja toimittajia. Älä anna enempää henkilökohtaista tietoa kuin on tarpeen – älä anna työnantajaan liittyvää tietoa lainkaan.
- Sammuta tietokone ja katkaise Internet-yhteys, kun et käytä niitä.

## 4.4 Matkatyö

- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.
- Mikäli työskentelet julkisessa kulkuvälineessä, varmistu, etteivät kansamatkustajat pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Varo myös aiheettomien langattomien yhteyksien aktivoitumista koneeseesi.
- Säilytä tieto ja laitteet turvassa. Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitetta lukitussa paikassa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita ja matkapuhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulle ei myöskään tarjoudu mahdollisuutta poistaa näitä tietoja laitteelta.

## 5 ONGELMATILANTEET

### 5.1 Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

- Mikäli hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi ao. vastuuhenkilölle oman vastuusi rajaamiseksi.
- Ilmoita aina haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuden liittyvistä ongelmista välittömästi tietoturvavastaavalle, tietohallinto-organisaatioon tai omalle esimiehellesi.
- Ilmoita aina myös muista turvallisuuden liittyvistä epäilyistä, suojauspuutteista tai ongelmista turvallisuusvastaaville tai omalle esimiehellesi.

### 5.2 Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa...

- Älä hätiköi.
- Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki. Kirjoita muihin tekemisesi ja kirjaa menetetty työaika mahdollista korvausvaatimusta varten.
- Ota yhteyttä tietohallinto-organisaatioon ja/tai tietoturvavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

### 5.3 Seuraamukset

- Lakien, määräysten ja ohjeiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle.
- Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimukseen ja rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös irtisanominen tai palvelussuhteen purkaminen.

## 6 MISTÄ SAA LISÄTIETOJA?

Lisää tietoa tietoturvallisuudesta on saatavissa mm. seuraavista lähteistä:

- Tietoturvavastaava, tietohallinto-organisaatio, turvallisuusvastaava, esimies
- Organisaation omat ohjeet
- Lainsäädäntö – Valtion säädöstietopankki ([www.finlex.fi](http://www.finlex.fi))
- Tietoturvallisuutta ohjeistavat ja säätelevät organisaatiot, esimerkiksi
  - Valtiovarainministeriön VAHTI-ohjeet ([www.vm.fi/vahti](http://www.vm.fi/vahti))
  - Arkistolaitoksen ohjeet ([www.narc.fi](http://www.narc.fi))
  - Tietosuojavaltuutetun toimiston ohjeet ([www.tietosuoja.fi](http://www.tietosuoja.fi))
  - Tietoyhteiskunnan kehittämiskeskuksen ohjeet ([www.tieke.fi](http://www.tieke.fi))
  - Viestintäviraston ohjeet ([www.ficora.fi](http://www.ficora.fi))
  - Julkishallinnon ja elinkeinoelämän yhteiset ohjeet ([www.tietoturvaopas.fi](http://www.tietoturvaopas.fi))



# LIITE 1: TIETOTURVALLISUUTEEN KESKEISESTI LIITTYVÄT SÄÄDÖKSET

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731/1999) 2.luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
- Suomen perustuslaki (731/1999) 2.luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Valtion virkamieslaki (750/1994) 17§: Säädös valtion virkasuhteesta
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM0024:00/02/99/1998)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): Arkaluonteiset kansainväliset asiakirjat
- Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
- Laki turvallisuusselfityksistä (177/2002): Henkilöiden taustat
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki sähköisistä allekirjoituksista (14/2003)

- Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
- Rikoslaki (39/1889) 34.luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
- Rikoslaki (39/1889) 38.luku 8 §: Tietomurto
- Rikoslaki (39/1889) 38.luku 9 § 1. kohta: Henkilötietorikos
- Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
- Vahingonkorvauslaki (41/1974)

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki –sivustolta ([www.finlex.fi](http://www.finlex.fi)).

## LIITE 2: VOIMASSA OLEVAT VAHTI-JULKAISUT

- VAHTI 10/2006 Henkilöstön tietoturvaohje
- VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
- VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
- VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen - hallittu prosessi
- VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
- VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
- VAHTI 4/2006 Selvitys valtionhallinnon ympäri vuorokautisen tietoturvatavoiminnan järjestämisestä
- VAHTI 3/2006 Selvitys valtionhallinnon tietoturvaressurssien jakamisesta
- VAHTI 2/2006 Electronic-mail Handling Instruction for State Government
- VAHTI 1/2006 VAHTIn toimintakertomus vuodelta 2005
- VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta
- VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
- VAHTI 1/2005 Information Security and Management by Results
- VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
- VAHTI 4/2004 Datasäkerhet och resultatstyrning
- VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje
- VAHTI 2/2004 Tietoturvallisuus ja tulosohejaus
- VAHTI 1/2004 Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
- VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
- VAHTI 5/2003 Datasäkerhetsanvisning för användaren
- VAHTI 5/2003 User's Information Security Instruction
- VAHTI 4/2003 Valtionhallinnon tietoturvakäsitteistö
- VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus
- VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista

- VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvaluusohje
- VAHTI 4/2002 Arkaluonteisten kansainvälisten aineistojen käsittelyohje
- VAHTI 3/2002 Etätöön tietoturvaohje
- VAHTI 1/2002 Tietoteknisten laittilojen turvallisuussuositus
- VAHTI 6/2001 Tietotekniikkahankintojen tietoturvaluusustarkistuslista
- VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvaluusuden yleisohje
- VAHTI 3/2001 Salauskäytäntöjä koskeva valtiorhallinnon tietoturvaluusussuositus
- VAHTI 2/2001 Valtiorhallinnon lähiverkkojen tietoturvaluusussuositus
- VAHTI 1/2001 Valtion viranomaisen tietoturvaluusustyön yleisohje
- VAHTI 3/2000 Tietojärjestelmäkehityksen tietoturvaluusussuositus
- VAHTI 2/2000 Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)

Uudistuva ja täydentyvä ohjeisto löytyy VAHTIn Internet-sivuilta ([www.vm.fi/vahti](http://www.vm.fi/vahti)) ja ohjeita saa myös tilattua painotalo Editasta.

# VAHTI



VALTIOVARAINMINISTERIÖ  
Snellmaninkatu 1 A  
PL 28, 00023 VALTIONEUVOSTO  
Puhelin: (09) 160 01  
Telefaksi: (09) 160 33123  
[www.vm.fi](http://www.vm.fi)

10/2006  
HENKILÖSTÖN  
TIETOTURVAOHJE

ISSN 1455-2566  
ISBN 951-804-664-6 (nid.)  
ISBN 951-804-665-4 (pdf)