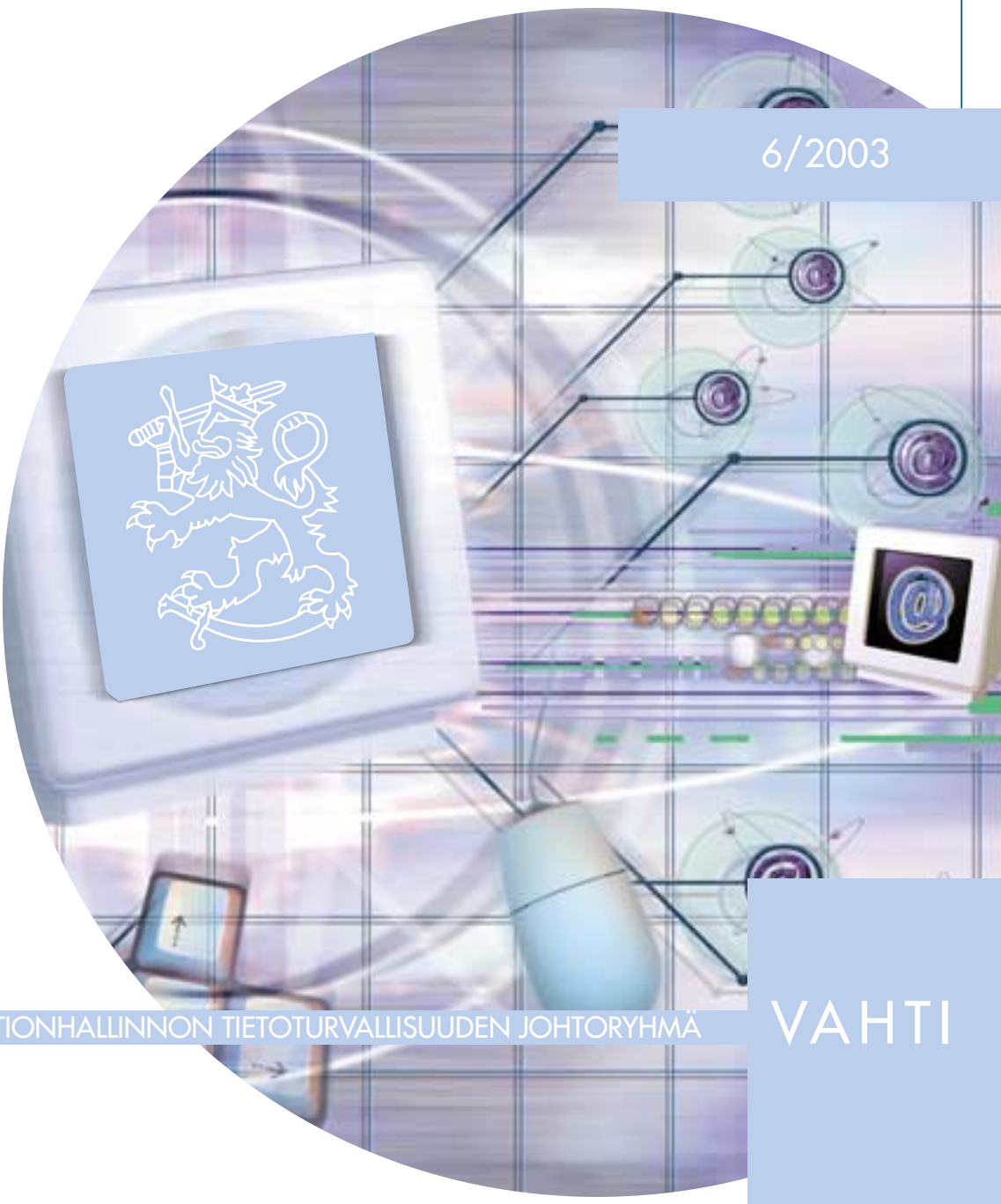
VALTIOVARAINMINISTERIÖ

OPAS JULKISHALLINNON TIETOTURVAKOULUTUKSEN JÄRJESTÄMISESTÄ



6/2003

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

OPAS JULKISHALLINNON TIETOTURVAKOULUTUKSEN JÄRJESTÄMISESTÄ

6/2003

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33 222

Sähköposti: vahtijulkaisut@vm.fi

ISSN 1455-2566
ISBN 951-804-407-4

Edita Prima Oy
HELSINKI 2003

VALTIOVARAINMINISTERIÖ VM 40/01/2003

1.12.2003

Ministeriöille, virastoille ja laitoksille

OPAS JULKISHALLINNON TIETOTURVAKOULUTUKSEN JÄRJESTÄMISESTÄ

Valtiovarainministeriö antaa oheisen tietoturvaoppaan (jäljempänä opas), joka on laadittu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Opas, jonka valmisteluun on osallistunut myös kunnallishallinto, täydentää laajaa valtiovarainministeriön antamaa tietoturvaohjeistoa.

Oppaan kohderyhminä ovat organisaatioiden tietoturvaohjeista ja koulutuksesta vastaavat henkilöt, koulutussuunnittelijat sekä johto. Oppaan tarkoituksena on toimia apuvälineenä tietoturvakoulutuksen ja –ohjeiden suunnittelussa, valmistelussa, toteutuksessa, päivityksessä ja arvioinnissa. Opas osaltaan tukee tietoturvatietoisuuden nostamista ja koko henkilökunnan tietoturvallisuuteen liittyvien toimintatapojen kehittämistä.

Opas sisältää kuvauksen käyttäjän tietoturvaohjeistuksen ja –koulutuksen tietosisällön perustasta, joka muodostuu muun muassa lainsäädännöstä, valtioneuvoston periaatepäätöksistä kansallisesta tietoturvallisuusstrategiasta (4.9.2003) ja valtionhallinnon tietoturvallisuudesta (11.11.1999), valtiovarainministeriön antamista tietoturvaohjeista sekä ministeriöiden ja niiden alaisten organisaatioiden omista ohjeista. Oppaassa kuvataan myös julkishallinnon organisaation ohjekokonaisuus ja kultakin tietoturvallisuuden osa-alueelta yksityiskohtaisia ohjeistukseen ja koulutukseen sisällytettäviä asioita.

Koko henkilöstön sitoutuminen tietoturvallisuuteen on tärkeää, jonka varmistamiseksi hallinnon yksiköissä tulee panostaa henkilökunnan tietoturvakoulutukseen. Tietoturvatoiminnan organisointi ja suunnittelu sekä organisaation tietoturvapolitiikka ja periaatteet antavat perustan jatkuvalle tietoturvallisuuden kehittämiselle. Käyttäjien riittävä ohjeistus sekä koulutus ovat osa kaikkein keskeisimpiä tietoturvallisuuden kehittämistoimenpiteitä. Näiden avulla nostetaan tietoturvatietämyksen tasoa sekä edistetään käyttäjien valmiuksia hyvään tietoturvatyöhön osana omia tehtäviään ja sitoutumista organisaation turvalliseen toimintaan.

Opas tulee VAHTIn Internet-sivuille, jotka ovat osoitteissa www.vm.fi/tietoturvallisuus ja www.vm.fi/vahti. Opasta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi). Lisätietoja antavat neuvottelevat virkamiehet Arja Terho ja Mikael Kiviniemi sekä ylitarkastaja Terttu Mellin (etunimi.sukunimi@vm.fi).

Alivaltiosihteeri Juhani Purunen

Neuvotteleva virkamies Mikael Kiviniemi

Liite Opas julkishallinnon tietoturvakoulutuksen järjestämisestä (VAHTI 6/2003)

TIIVISTELMÄ

Julkishallinnon toiminta on nykyisin erittäin riippuvaista tietojenkäsittelystä ja tiedonsiirrosta. Tietoyhteiskuntakehitys, kansainvälistyminen, verkottuminen sekä toimintojen ja palveluiden siirtyminen tietoverkkoihin lisäävät niiden merkitystä edelleen. Tämä on otettu huomioon myös lainsäädännössä, jossa esimerkiksi laissa viranomaisen toiminnan julkisuudesta määritellään hyvä tiedonhallintatapa. Henkilötietojen käsittelyä sääntelevän lain keskeinen tavoite on niin ikään hyvän tietojenkäsittelytavan ja hyvän tiedonhallinnan aikaan saaminen. Hyvään tiedonhallintatapaan kuuluu erottamattomasti tietoturvallisuus. Molempiin lakeihin sisältyy tietoturvallisuuden suunnittelua ja suojaamista koskevia vaatimuksia.

Koko henkilöstön sitoutuminen tietoturvallisuuteen on tärkeää. Sitoutumista ei kuitenkaan tapahdu, jos käyttäjät eivät miellä tietoturvallisuutta tärkeäksi omassa työssään tai eivät ymmärrä mitä tietoturvallisuudella tarkoitetaan. Turvallisuussuunnittelu, tietoturvatoiminnan organisointi sekä johdon määrittelemät tietoturvapolitiikka ja periaatteet antavat perustan jatkuvalle tietoturvallisuuden kehittämiselle. Keskeisimpiä kehittämiseen liittyviä toimenpiteitä ovat käyttäjien oikea ja riittävä ohjeistus sekä koulutus. Näiden avulla voidaan nostaa tietoturvatietämyksen tasoa organisaatiossa, herättää käyttäjät miettimään tietoturvaa omassa työssään ja sitä kautta luoda sitoutumista organisaation turvalliseen toimintaan. Tällä hetkellä julkishallinnon olemassa oleva tietoturvallisuuteen liittyvä ohjeistus on laaja ja vain osa ohjeistosta peruskäyttäjälle suunnattua. Käyttäjien tietoturvatietoisuuden ja -osaamisen lisäämiseksi valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) perusti tammikuussa 2003 valmisteluryhmän, jonka tehtävänä oli valmistella ministeriöille, valtion virastoille ja laitoksille sekä muille julkishallinnon organisaatioille tarkoitettu peruskäyttäjän tietoturvallisuuden koulutusaineisto.

Tämä oppaan on tarkoitus toimia apuvälineenä tietoturvakoulutusten ja -ohjeiden suunnittelussa, valmistelussa, toteutuksessa, päivityksessä ja arvioinnissa. Tavoitteena on, että tämä opas ja siihen liittyvät käyttäjän ohje, kouluttajan aineisto sekä multimedia-aineisto tukevat tietoturvatietoisuuden nostamista ja tietoturvallisuuteen liittyvien toimintatapojen kehittämistä julkishallinnon organisaatioissa.

Oppaan kohderyhminä ovat julkishallinnon organisaatioiden tietoturvaohjeista ja koulutuksista vastaavat henkilöt, koulutussuunnittelijat sekä johto.

Opas sisältää kuvauksen käyttäjän tietoturvaohjeistuksen ja –koulutuksen tietosisällön perustasta, joka muodostuu lainsäädännöstä, valtioneuvoston periaatepäätöksestä kansallisesta tietoturvallisuusstrategiasta, valtioneuvoston periaatepäätöksestä valtionhallinnon tietoturvallisuudesta, VAHTI-ohjeista sekä ministeriöiden ja niiden alaisten organisaatioiden omista ohjeista. Lisäksi oppaassa kuvataan julkishallinnon organisaation ohjekokonaisuus ja siihen liittyen on kultakin tietoturvallisuuden osa-alueelta nostettu esiin yksityiskohtaisia ohjeistukseen ja koulutukseen sisällytettäviä asioita. Lopussa on annettu ohjeistuksen ja koulutuksen kehitysehdotuksia.

SISÄLLYS

I TIETOTURVAOHJEISTON TAVOITTEET JA RAKENNE

1 JOHDANTO

1.1 Taustaa ja oppaan valmistelu

Tietoturvallisuus on kiinteä ja keskeinen osa organisaation toimintaa ja koskee koko henkilöstöä. Teknisillä ja fyysisillä tietoturvaratkaisuilla ei koskaan voidaan kokonaan taata tietoturvan toteutumista. Keskeisessä asemassa ovat ihmiset ja heidän toimintatapansa. Käyttäjien toimintatavat perustuvat organisaation johdon määrittelemiin tietoturvaperiaatteisiin. Tietoturvallisuuden varmistaminen ja kehittäminen edellyttää jatkuvaa kehitystyötä ohjeistuksessa, toteutuksessa ja henkilöstön osaamisen kehittämisessä.

Julkishallinnon tietoturvallisuuteen liittyvä ohjeistus on laaja ja vain osa ohjeistosta on peruskäyttäjälle suunnattua. Valtionhallinnon tietoturvallisuuden johtoryhmässä ja sen alaryhmissä sekä valtion tietoturvaseminaarin keskusteluissa on vuonna 2002 tullut esille peruskäyttäjiin kohdistuvan tietoturvallisuustyön tehostamistarpeita. Osassa virastoista ja laitoksista tietoturvallisuudesta vastuussa olevilla ei ole aikaa eikä välttämättä valmiuksia hoitaa tietoturvallisuuskoulutusta.

Valtioneuvoston periaatepäätöksessä valtion tietoturvallisuudesta 1999 ja VAHTIn ohjeissa korostetaan sitä, että tietoturvallisuustyö koskee julkishallinnossa koko henkilöstöä. OECD:n (Organisation for Economic Co-operation and Development) suosituksen “tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet” ja kansallisen tietoturvastrategian mukaisesti tietoturvallisuustietoisuuden tasoa on yleisesti nostettava. Samoin julkishallinnon peruskäyttäjän tietoturvallisuustietoisuuden ja osaamisen tasoa on nostettava.

Käyttäjien tietoturvatietoisuuden ja -osaamisen lisäämiseksi VAHTI perusti tammikuussa 2003 valmisteluryhmän, jonka tehtävänä oli valmistella ministeriöille, valtion virastoille ja laitoksille sekä muille julkishallinnon organisaatioille tarkoitettu peruskäyttäjän tietoturvallisuuden koulutusaineisto. Koulutusaineistoon sisällöksi määri-

teltiin vähintään tiivistetty kirjallinen käyttäjän tietoturvaohje, verkkokäyttöinen käyttäjäohje sekä tietoturvavastaaville tarkoitettu kouluttaja-aineisto, joka sisältää myös esityksen väärinkäytöksistä.

Lisäksi valmisteluryhmän tehtävänä oli tehdä esitys käyttäjien tietoturvaosaamisen ja tietoturvakouluttamisen kehittämisestä.

Oppaan laatineen valmisteluryhmän kokoonpano oli seuraava:

Eeva Björklund, Ilmailulaitos, valmisteluryhmän puheenjohtaja
Riitta Hallberg, Viitasaaren kaupunki
Kalervo Jakonen, Tulli
Maija Kleemola, Tietosuojavaltuutetun toimisto
Eero Koljonen, Tilastokeskus
Antti Laari, Helsingin kauppakorkeakoulu
Minna Manninen, Tampereen yliopisto
Terttu Mellin, Valtiovarainministeriö
Asta Partti, Verohallinto
Seppo Sundberg, Valtiokonttori

Konsulttityöstä vastasivat:

Jari Kivelä, Secgo Group Oy
Elina Salmi, Secgo Group Oy

VAHTI linjasi ohjeen sisältöä ja jatkovalmistelua kokouksessaan elokuussa 2003. VAHTI linjasi viimeistelyä kokouksessaan lokakuussa 2003 ja tämän pohjalta viimeisteltiin lopullinen versio.

1.2 Oppaan tarkoitus ja rajaukset

Oppaan on tarkoitus toimia apuvälineenä tietoturvakoulutusten ja -ohjeiden suunnittelussa, valmistelussa, toteutuksessa, päivityksessä ja arvioinnissa. Tavoitteena on, että tämä opas ja siihen liittyvät käyttäjän ohje, kouluttajan aineisto sekä multimediaaineisto tukevat tietoturvatietoisuuden nostamista ja tietoturvallisuuteen liittyvien toimintatapojen kehittämistä julkishallinnon organisaatioissa.

Oppaan sisällössä on keskitytty tavallisen käyttäjän tietoturvaohjeistuksen ja -koulutuksen keskeisiin asioihin. Opas ei ota kantaa organisaatioiden johdon, tietoturva-asiantuntijoiden, tietojärjestelmien ylläpitäjien tai muiden tietoturvallisuuteen enemmän perehtyneiden henkilöiden ohjeistukseen ja koulutukseen. Luonnollisesti he toimivat organisaatiossa myös käyttäjän roolissa ja tällöin heitä koskevat samat perus-

periaatteet kuin kaikkia käyttäjiä, mutta tässä oppaassa ei ole perehdytty heille erityisesti tarkoitettuihin tietoturvaohjeisiin.

Tietoturvallisuutta koskevasta lainsäädännöstä on huomioitu erityisesti niitä säännöksiä, jotka säätelevät julkishallinnon työntekijän jokapäiväisiä tietoturvallisuuteen liittyviä asioita. VAHTI:n ohjeistosta on tähän oppaaseen koottu yhteenvetona ne asiat, jotka koskevat tavallista käyttäjää.

1.3 Oppaan rakenne

Opas julkishallinnon tietoturvallisuuskoulutuksen järjestämisestä on jaettu kolmeen osaan.

I osa

Oppaan ensimmäinen osa käsittelee tietoturvaohjeiston tavoitteita ja rakennetta. Siihen sisältyvät luvut 1-3.

Luvussa 1 kuvataan tämän oppaan valmistelu sekä oppaalle asetetut tavoitteet, rajaukset, rakenne ja kohderyhmät.

Luku 2 käsittelee tavoitteet ja vaatimukset, jotka käyttäjän ohjeistus- ja koulutustyölle on asetettu.

Luvussa 3 on esitelty käyttäjän tietoturvaohjeistus- ja –koulutuskokonaisuus. Se sisältää tämän oppaan lisäksi käyttäjän ohjeen, kouluttajan aineiston ja multimediaaineiston.

II osa

Oppaan toinen osa sisältää käyttäjän tietoturvallisuuskoulutuksen ja ohjeistuksen lähtökohdat. Toiseen osaan kuuluvat luvut 4-7.

Luku 4 luo lähtökohdat käyttäjien koulutukselle ja ohjeistukselle. Luku korostaa tiedon ominaisuuksien, luottamuksellisuuden, eheyden ja käytettävyyden merkitystä käyttäjien koulutuksessa ja ohjeistuksessa.

Luvussa 5 käsitellään käyttäjän tietoturvaohjeistuksen ja –koulutuksen tietosisällön perusta. Luku sisältää yhteenvedon julkishallinnon käyttäjää velvoittavista laeista ja VAHTI-ohjeista sekä muiden julkishallinnon tietoturvaa ohjaavien organisaatioiden ohjeista.

Luvussa 6 kuvattu julkishallinnon organisaation ohjekokonaisuus täydentää käyttäjän tietoturvaohjeistus- ja –koulutusaineistoa.

Luvussa 7 on tietoturvan eri osa-alueilta nostettu yksityiskohtaisesti esiin asioita, jotka kultakin osa-alueelta tulee sisällyttää julkishallinnon käyttäjän ohjekokonaisuuteen.

III osa

Oppaan kolmas osio sisältää käyttäjän ohjeiden ja koulutuksen jatkokehittämisen.

Luku 8 sisältää esitykset käyttäjien tietoturvallisuusosaamisen ja tietoturvallisuuskouluttamisen kehittämiseksi julkishallinnossa.

1.4 Kohderyhmät

Oppaalla on kolme pääasiallista kohderyhmää:

1. Julkishallinnon organisaatioiden tietoturvaohjeiden laatimisesta ja päivittämisestä vastaavat henkilöt

   Julkishallinnon organisaatioiden tietoturvaohjeiden laatimisesta ja päivittämisestä vastaaville henkilöille tärkein on luku 5, jossa kuvataan ohjeiden tietosisällön perusta. Lisäksi ohjeista vastaaville opas sisältää kuvauksen organisaation ohjekokonaisuudesta luvussa 6 sekä tietoturvan eri osa-alueilta käyttäjän ohjeisiin liittyvät asiat luvussa 7. Tämän lisäksi ohjeista vastaaville henkilöille on annettu kehitysesityksiä luvussa 8.5.

2. Julkishallinnon organisaatioiden tietoturvakouluttajat sekä koulutussuunnittelijat

   Julkishallinnon organisaatioiden tietoturvakouluttajille sekä koulutussuunnittelijoille opas sisältää tietoturvan eri osa-alueilta käyttäjän koulutukseen liittyvät asiat luvussa 7. Kouluttajille ja koulutussuunnittelijoille on annettu kehitysesityksiä luvussa 8.4.

3. Organisaation johto

   Organisaation johdolle tämä opas kuvaa käyttäjän tietoturvaohjeistuksen ja ohjeistuskokonaisuuden luvussa 6. Lisäksi organisaation johdolle on suunnattu erityisesti luku 7.1., jossa kuvataan hallinnollisen turvallisuudesta käyttäjän ohjeisiin liittyvät asiat. On myös tärkeä huomata, että luvussa 8.3. esitetyt organisaatioiden tietoturvan kehitysehdotusten toteuttaminen vaatii organisaation johdon tuen ja hyväksynnän.

Tämän lisäksi oppaassa on osia, joista voi olla hyötyä myös muissa tehtävissä oleville, kuten esimerkiksi tietojärjestelmien ja tietoturvallisuuden suunnittelijoille ja kehittäjille.

2 YLEISTÄ KÄYTTÄJÄN TIETOTURVAKOULUTUS- JA OHJEISTUSAINEISTOSTA

Tämä luku sisältää käyttäjän koulutus- ja ohjeistusaineistolle asetetut tavoitteet ja vaatimukset.

2.1 Käyttäjän koulutus- ja ohjeistusaineiston tavoitteet

Koulutus- ja ohjeistusaineistolle ja sen laatimiselle asetettiin seuraavat tavoitteet:

1. Tavoitteena on yhtenäistää julkishallinnon käyttäjien perustietoturvaohjeita. Lähtökohtaisesti kaikilla julkishallinnon käyttäjillä tulee olla samat perustiedot tietoturvallisuudesta. Jokaisella organisaatiolla on kuitenkin omia ohjeita ja toimintatapoja, jotka saattavat olla keskenään hyvinkin erilaisia. Käyttäjän ohjeen tavoitteena on antaa kaikille julkishallinnon organisaatioille yhteinen pohja käyttäjän tietoturvaohjeistukseen.
2. Tavoitteena on käyttäjien tietoturvatietämyksen lisääminen ja asenteiden muokkaaminen. Käyttäjän ohje antaa perustiedot tietoturvallisista toimintatavoista ja tämän lisäksi multimedia-aineiston avulla käyttäjät voivat itse hankkia lisätietoja tietoturvallisuudesta. Multimedia-aineistoon on lisäksi koottu kuvauksia toteutuneista arkipäivän tietoturvauhkista ja väärinkäytöksistä. Näiden tarkoituksena on parantaa käyttäjän valmiuksia tunnistaa tietoturvauhat ja toisaalta lisätä organisaatioiden kiinnostusta aiheeseen liittyvään osaamisen kehittämiseen ja koulutukseen.
3. Tavoitteena on helpottaa julkishallinnon organisaatioiden tietoturvakouluttajien ja koulutussuunnittelijoiden työtä. Kouluttajan aineisto sisältää

valmiit koulutuskalvot. Lisäksi multimedia-aineistoon on koottu paljon kouluttajan työtä tukevaa aineistoa ja kouluttajille löytyy lisätietoja tästä oppaasta. Tähän oppaaseen on myös sisällytetty ehdotukset koulutusten toteuttamisesta organisaatioissa.

2.2 Koulutus- ja ohjeistusaineistolle asetettavat vaatimukset

Koulutus- ja ohjeistusaineistolle ja sen laatimiselle asetettiin seuraavat vaatimukset:

1. Ohjeiden ja koulutusten tietosisällön on oltava linjassa sekä lainsäädännön että VAHTI-ohjeiden kanssa.
2. Ohje- ja koulutusaineiston on oltava helppolukuista. Ne eivät saa sisältää käyttäjille tuntemattomia tai vaikeita termejä.
3. Käyttäjän ohjeen ensisijainen kohderyhmä on organisaation työntekijät. Ohje on laadittava niin, että se on ymmärrettävä kaikille työntekijöille organisaatiosta tai työtehtävästä riippumatta. Muita kohderyhmiä ovat esimerkiksi kunnalliset luottamushenkilöt, oppilaitosten oppilaat ja opiskelijat, yhteistyökumppanit, konsultit ja atk-ammattilaiset.
4. Käyttäjän ohjeen kirjoitustyylin on oltava käyttäjälle läheinen. Tätä tavoitellaan mm. sinuttelulla ja opastamisella.
5. Käyttäjän ohjeen on herätettävä käyttäjät ajattelemaan tietoturva-asioita omassa työssään.
6. Multimedia-aineiston on oltava verkkokäyttöinen ja muokattavissa.
7. Multimedia-aineiston tulee sisältää työkalu käyttäjän tietoturvatason mittaamiseen.
8. Multimedia-aineiston tulee sisältää esimerkkejä käytännön elämästä. Nämä voivat olla esimerkiksi uhkakuvaesimerkkejä.
9. Multimedia-aineiston tulee sisällyttää taulukko luokitellun aineiston käsittelyyn.

3 KOULUTUS- JA OHJEISTUSAINEISTON RAKENNE

Käyttäjien tietoturvakoulutus ja –ohjeistusaineisto sisältää neljä kokonaisuutta:

1. Oppaan julkishallinnon tietoturvallisuuskoulutuksen järjestämisestä
2. Käyttäjän ohjeen
3. Kouluttajan aineiston
4. Multimedia-aineiston

3.1 Opas julkishallinnon tietoturvallisuuskoulutuksen järjestämisestä (loppuraportti)

Opas kokoaa työn tulokset yhteen. Se toimii samalla loppuraporttina. Oppaan liitteitä ovat käyttäjän ohje (liite 2), kouluttajan aineisto (liite 3) ja multimedia-aineisto (liite 4). Oppaan tarkoitus ja sisältö on kuvattu tarkemmin luvussa 1.

3.2 Käyttäjän ohje

Käyttäjän tietoturvaohje on yleisluonteinen malli. Ohjeen kohderyhmänä on julkishallinnon organisaatioiden henkilöstö. Ohje on laadittu niin, että sitä voidaan soveltaa kaikissa julkishallinnon organisaatioissa. Siinä on huomioitu lainsäädäntö ja VAHTI-ohjeet.

Ohjeesta on laadittu sekä kirjallinen että sähköisessä muodossa oleva versio. Ohje ei välttämättä sellaisenaan sovi organisaation käyttöön, koska eri organisaatioissa ja tilanteissa on erityisiä tietoturva-asioita, joita on painotettava. Käyttäjälle on keskeis-

tä myös oman organisaation muiden ohjeiden tunteminen ja noudattaminen. Tarkoitus on, että käyttäjän ohje laaditaan organisaatio- tai toimintayksikkökohtaiseksi ja se muokataan organisaation tarpeita vastaavaksi. Ohje on kuitenkin valmistelutyöryhmässä laadittu niin, että jos organisaation aika tai muut resurssit eivät riitä ohjeen muokkaamiseen, voidaan ohjetta jakaa käyttäjille myös tällaisenaan.

Käyttäjän ohje on tämän loppuraportin liitteenä (liite 2). Ohjeen verkkokäyttöinen versio löytyy multimedia-aineistosta.

3.3 Kouluttajan aineisto

Kouluttajan aineisto on tarkoitettu julkishallinnon organisaatioiden tietoturvakouluttajille. Aineisto muodostuu kahdesta osasta:

1. Kouluttajan kalvoaineisto käyttäjän ohjeen kouluttamiseen

   Aineistossa on valmiit kalvot, joita kouluttaja voi käyttää joko sellaisenaan käyttäjiä kouluttaessaan tai muokata ne omia tarpeitaan vastaaviksi. Kalvot on tehty niin, että ne muodostavat luentokokonaisuuden, mutta tarvittaessa kalvoista voidaan valita vain osa, jos koko kalvosarjaa ei haluta tai ehditä käydä läpi. Kalvot ovat Microsoft PowerPoint 2000 -muodossa ja niiden muistiinpano-osiosta (engl. *Notes View*) löytyvät kuhunkin kalvoon liittyvät kouluttajan ohjeet.

2. Saate kouluttajalle tietoturvakoulutukseen

   Saatteessa opastetaan kouluttajan aineiston käyttöön.

3.4 Multimedia-aineisto

Multimedia-aineisto on tarkoitettu organisaation käyttäjille, tietoturvakouluttajille ja muille tietoturvallisuudesta kiinnostuneille. Multimedia-aineisto sisältää:

- Käyttäjän tietoturvaohjeen, johon on liitetty linkkejä valtakunnallisiin ohjeisiin
- Testin tietoturvatietämyksen tason kartoittamiseksi
- Tietoturvallisuuteen liittyvän lainsäädännön
- Tietoturvakouluttajan aineiston
- Linkit mm. VAHTI-sanastoon ja VAHTI-ohjeisiin

Lisäksi multimedia-aineistoon on luotu paikat organisaation omalle ohjeistukselle.

Multimedia-aineiston käyttö ja muokkausohjeet ovat tämän loppuraportin liitteenä (liite 5).

II. KÄYTTÄJÄN TIETOTURVALLISUUSKOULUTUKSEN JA OHJEISTUKSEN LÄHTÖKOHDAT

4 TIETOJEN JA TIETOPÄÄOMAN SUOJAAMINEN

Käyttäjän koulutusta ja ohjeita suunniteltaessa ja toteutettaessa on hyvä muistaa, että liian usein tietoturvallisuus mielletään tietoteknisiksi toimenpiteiksi ja puhtaasti osaksi organisaation tietojenkäsittelyä. Tämä vaikuttaa myös käyttäjän asenteisiin ja kiinnostukseen tietoturvallisuutta kohtaan. Useasti myös koetaan, että omien tietoteknisten taitojen ollessa heikot, ei käyttäjä voi vaikuttaa tietoturva-asioihinkaan.

Käyttäjän tietoturvakoulutuksen ja -ohjeiden lähtökohtana tulee olla organisaation tiedot, tietopääoma ja muut suojattavat kohteet. Käyttäjille tulee alusta asti luoda tietoisuus siitä, mitä tietoja organisaatioissa on tarpeen suojata. Tätä varten organisaatiossa tulee olla määriteltynä ja luokiteltuna suojattavat kohteet. Käyttäjille on myös hyvä antaa selkeät ohjeet kunkin tiedon tai tietoryhmän turva- ja suojaustarpeista sekä tietojen salassapitovaatimuksista. Käyttäjillä tulee myös olla saatavilla tietojärjestelmäselosteet (Laki viranomaisten toiminnan julkisuudesta 18§) ja henkilörekisteriselosteet (Henkilötietolaki 10§).

Tietojen käytön mahdollistaminen ja turvaaminen ovat tietoturvallisuuden tärkeimpiä vaatimuksia. Näiden vaatimusten toteuttamisessa tietotekniikka ja –järjestelmät ovat vain välineitä. Tiedot turvataan, jotta voidaan taata niiden luottamuksellisuus, eheys ja käytettävyys. Nämä ovat tiedon ominaisuuksia, jotka toimivat tietoturvallisuuden perustana ja lähtökohtana käyttäjien koulutukselle ja ohjeistukselle.

Luottamuksellisuudella tarkoitetaan, että tietoja saavat käyttöönsä vain niihin oikeutetut henkilöt eikä tietoa paljasteta muille. Luottamuksellisuuden varmistamiseksi tietoliikennettä salataan, tietojen ja tietojärjestelmien käyttöoikeuksia rajataan ja tietojen käyttöä valvotaan.

Eheys viittaa siihen, että tiedot ovat oikeita, luotettavia ja ajantasaisia eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa inhimillisen toiminnan, laitteisto- tai ohjelmistovikojen tai luonnon tapahtumien seurauksena.

Käytettävyydellä varmistetaan, että tiedot ja palvelut ovat käytettävissä oikea-aikaisesti ja häiriöittä silloin, kun niitä tarvitaan. Käytettävyyttä turvataan esimerkiksi varajärjestelmillä.

Tietoturvakoulutuksen tulee perustua organisaation omien suojattavien kohteiden turvaamiseen ja siihen liittyviin periaatteisiin, toteutustapoihin ja ohjeisiin.

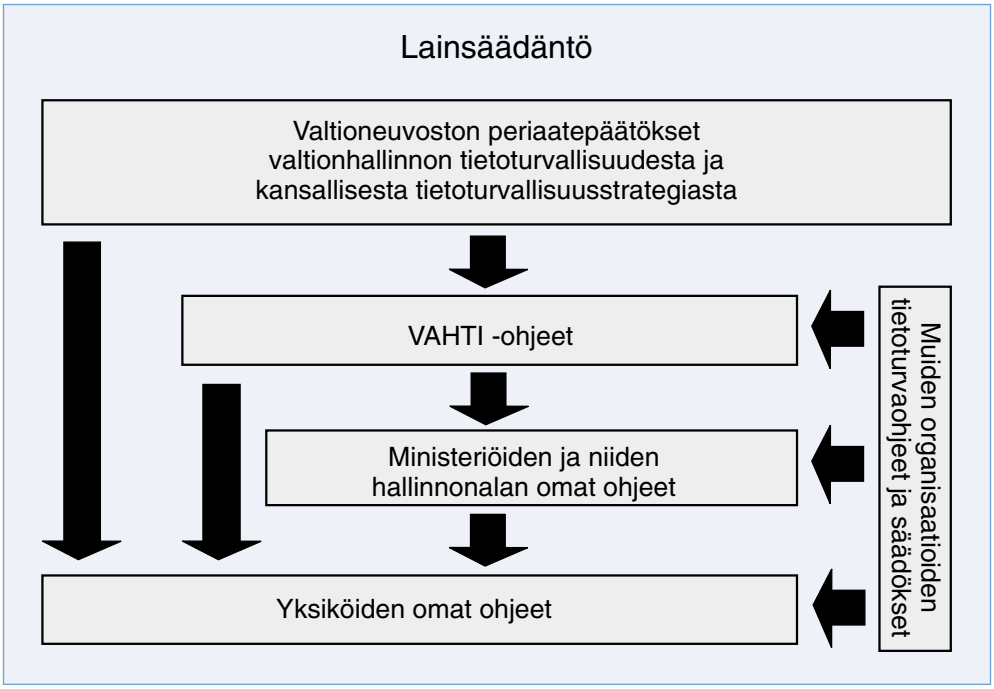
5 LAINSÄÄDÄNTÖ, NORMIT JA OHJEET

Julkishallinnossa tietoturvallisuuden yhteisinä lähtökohtina ovat mm. jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta sekä säädöksissä määritellyt tietoturvavelvoitteet ja valtiovarainministeriön antamat tietoturvaohjeet.

Kaiken tietoturvatoiminnan perustana on Suomen lainsäädäntö. Useat lait, asetukset sekä määräykset ja ohjeet sisältävät viranomaisia koskevia tietoturvavelvoitteita. Lainsäädäntö on myös huomioitu valtioneuvoston periaatepäätöksissä valtionhallinnon tietoturvallisuudesta ja kansallisesta tietoturvastrategiasta. Periaatepäätös valtionhallinnon tietoturvallisuudesta luo pohjan valtionhallinnon tietoturvallisuuden kehittämiselle. Se edistää osaltaan kansallisella tasolla valtion ja erilaisten yhteisöjen tietoturvallisuuden ja tietosuojan toteutumista viranomaisten tietojärjestelmissä ja julkisissa palveluissa. Kansallinen tietoturvastrategia antaa puolestaan valtioneuvoston, elinkeinoelämän, järjestöjen ja yksittäisten kansalaisten tietoturvallisuusponnisteluille yhteisen suunnan.

Valtionhallinnon tietoturvallisuuden johtoryhmä kehittää valtionhallinnon tietoturvallisuuden ohjeistusta. Tämän lisäksi ministeriöt ja muut tietoturvatoimintaa säätelevät organisaatiot antavat omia ohjeitaan.

Yksiköiden omien ohjeiden tulee perustua kaikkiin edellä mainittuihin ohjeisiin, periaatteisiin ja lainsäädäntöön. Valmistelutyöryhmän laatima käyttäjän ohje sijoittuu juuri yksiköiden omiin ohjeisiin.



5.1 Lainsäädäntö

5.1.1 Tietoturvatoimintaa ohjaavat lait ja asetukset

Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä. Tietoturvallisuuden järjestämistä koskevia säännöksiä sisältyy useisiin lakeihin ja asetuksiin. Lainsäädännöstä on tiedostettava organisaation toiminnan perusteita koskevat säännökset, kuten tietojen salassa pidettävyyttä sekä tietojen ja aineistojen käsittelyä koskevat säännökset. Tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen sekä tietoturvarikkomusten käsittelyyn otetaan kantaa seuraavissa laeissa:

- Perustuslaki (731/1999, 2 luku 10§ ja 12§)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Henkilötietolaki (523/1999)
- Arkistolaki (831/1994)

- Rikoslaki (39A/1889, RL 38:3, 38:5-7, 38:8, 34:1a ja 35:1 sekä 28:7)
- Valmiuslaki (1080/1991, muutos 198/2000)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Valtion virkamieslaki (750/1994) (17§)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Henkilökorttilaki (829/1999)
- Vahingonkorvauslaki (41/1974)
- Laki yksityisyyden suojasta työelämässä (477/2001)
- Laki puolustustaloudellisesta suunnittelukunnasta (238/1960, muutokset 1241/1987 ja 623/1999)
- Väestötietolaki (507/1993, muutokset 202/1994 ja 527/1999)
- Asetus puolustustaloudellisesta suunnittelukunnasta (239/1960, muutokset 42/1981, 1391/1992 ja 444/1997)
- Viestintämarkkinalaki (393/2003)
- Laki sähköisestä viestinnän ja automaattisen tietojenkäsittelyn käyttämisestä yleisissä tuomioistuimissa (594/1993)
- Asetus valtion talousarviosta (1243/1992)
- Valtioneuvoston ohjesääntö (262/2003)

Näiden lisäksi oppaan laatimishetkellä ovat luonnosvaiheessa tai käsittelyn alla seuraavat tietoturvallisuutta ohjaavat hallituksen esitykset:

- Hallituksen esitys Eduskunnalle laiksi viestintämarkkinalain muuttamisesta (13/2003)
- Hallituksen esitys sähköisen viestinnän tietosuojalaiksi (HE 125/2003)

Kaikki lait ja hallituksen esitykset löytyvät valtion säädöstietopankista osoitteesta http://www.finlex.fi.

5.1.2 Keskeiset tietoturvatoimintaan vaikuttavat lain kohdat

Perustan tietoturvatoiminnalle julkishallinnossa antavat seuraavat lain kohdat:

Suomen perustuslaki (731/1999) 10§

”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.”

”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.”

Suomen perustuslaki (731/1999) 12§

”Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.”

Laki viranomaisten toiminnan julkisuudesta (621/1999) 18§

Hyvä tiedonhallintatapa

Viranomaisen 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 sekä tässä tarkoituksessa erityisesti:

1) pitää luetteloa käsiteltäviksi annetuista ja otetuista sekä ratkaistuista ja käsitellyistä asioista tai muutoin huolehtia siitä, että sen julkiset asiakirjat ovat vaivattomasti löydettävissä;

2) laatia ja pitää saatavilla kuvaukset pitämistään tietojärjestelmistä sekä niistä saatavissa olevista julkisista tiedoista, jollei tiedon antaminen ole vastoin 24£:n tai muun lain säännöksiä;

3) selvittää tietojärjestelmien käyttöönottoa sekä hallinnollisia ja lainsäädännöllisiä uudistuksia valmisteltaessa suunniteltujen toimenpiteiden vaikutus asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun samoin kuin ryhtyä tarpeellisiin toimenpiteisiin tietoon liittyvien oikeuksien ja tiedon laadun turvaamiseksi sekä asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan järjestämiseksi;

4) suunnitella ja toteuttaa asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen julkisuus voidaan vaivattomasti toteuttaa ja että asiakirjat ja tietojärjestelmät sekä niihin sisältyvät tiedot arkistoidaan tai hävitetään asianmukaisesti ja että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvajärjestelyin ottaen

huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvatoimenpiteistä aiheutuvat kustannukset;

5) huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa ja käsittelyssä sekä niiden ja asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvajärjestelyistä ja tehtävänjaosta, samoin kuin siitä, että hyvän tiedonhallintavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan.

Tarkempia säännöksiä 1 momentissa säädettyjen velvoitteiden toteuttamiseksi tarpeellisista toimenpiteistä annetaan asetuksella. Tuomioistuimen ja syyttäjän diaarista antaa kuitenkin tarkempia määräyksiä oikeusministeriö. Asetuksella voidaan säätää valtioneuvoston oikeudesta antaa tarkempia säännöksiä ja ohjeita asiakirjojen sekä tietojärjestelmien ja niihin sisältyvien tietojen suojaamisessa, tietojen eheyden ja laadun varmistamisessa sekä tietojen siirrossa tietoverkkojen välityksellä noudatettavista teknisistä tietoturvatoimenpiteistä ja menettelyä koskevista vaatimuksista sekä niiden tason määrittelyssä noudatettavasta asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen luokituksesta valtionhallinnossa.

Arkistotoimen tehtävistä on voimassa, mitä arkistolaissa tai sen nojalla säädetään tai määrätään.

Laki viranomaisten toiminnan julkisuudesta (621/1999) 24§

Salassa pidettävät viranomaisen asiakirjat

Laissa nimetään ne viranomaisten asiakirjat, jotka ovat salassa pidettäviä ellei toisin säädetä. Asiakirja voi olla perinteisessä muodossa oleva paperidokumentti tai se voi olla tietojärjestelmässä oleva elektroninen tieto. Laki ryhmittelee asiakirjat 32 eri ryhmään asiakirjojen tietosisällön ja käyttötarkoituksen mukaisesti. Esimerkkeinä voidaan mainita salassa pidettävät henkilötiedot sekä liike- ja ammattisalaisuudet, yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi arkaluonteiset tiedot.

Asetus viranomaisten toiminnan julkisuudesta ja hyväst tiedonhallintatavasta (1030/1999)

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta määrittelee hyvän tiedonhallintatavan toteuttamisen, tiedonsaantioikeuksien toteuttamisen ja edistämisen sekä valtionhallinnan viestinnän.

Henkilötietolaki (523/1999)

Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Oleellista henkilötietojen käsittelyssä ovat

henkilötietojen käsittelyn suunnitteluvaatimus sekä tarpeellisuus- ja virheettömyysvaatimukset. Käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia (tarpeellisuusvaatimus). Rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä (virheettömyysvaatimus).

Käyttäjälle laista erityisesti huomioitavia kohtia ovat:

- 2 luku 5§: Huolellisuusvelvoite
- 2 luku 6§: Henkilötietojen käsittelyn suunnittelu
- 2 luku 8§: Käsittelyn yleiset edellytykset
- 2 luku 9§: Tietojen laatua koskevat periaatteet
- 3 luku: Arkaluonteiset tiedot ja henkilötunnus
- 7 luku: Tietoturvallisuus ja tietojen säilytys
- 7 luku 32§: Tietojen suojaaminen

Arkistolaki (831/1994)

Arkistolaki koskee arkistonmuodostajia. Arkistolaista käyttäjän on erityisesti huomioitava:

- 4 luku: Asiakirjojen laatiminen, säilyttäminen ja käyttö

Arkistolain mukaan pysyvään säilytykseen määrätyt asiakirjat on laadittava ja tiedot tallennettava pitkäaikaista säilytystä kestäville materiaaleille. Asiakirjoja on säilytettävä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä. Pysyvästi säilytettäviä asiakirjoja on säilytettävä sellaisissa arkistotiloissa kuin arkistolaitos erikseen määrää. Asiakirjat, joita ei ole määrätty pysyvästi säilytettäviksi tulee hävittää niille määrätyn säilytysajan jälkeen siten, että tietosuoja on varmistettu.

Rikoslaki (39/1889) 34 luku 9a§

Vaaran aiheuttaminen tietojenkäsittelylle

Joka, aiheuttaakseen haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle,

1) valmistaa tai asettaa saataville sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai levittää sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka

2) asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseen tai levittää sellaista ohjetta,

on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Rikoslaki (39/1889) 38 luku 8§

Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

Rikoslaki (39/1889) 38 luku 9§ 1.kohta

Henkilörekisteririkos

Joka tahallaan tai törkeästä huolimattomuudesta

1) käsittelee henkilötietoja vastoin henkilötietolain (523/1999) käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä, henkilötietojen tarpeellisuutta tai virheettömyyttä, arkaluonteisia tietoja, henkilötunnusta tai henkilötietojen käsittelyä erityisiä tarkoituksia varten koskevia säännöksiä taikka rikkoo henkilötietojen käsittelyä koskevia erityissäännöksiä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava henkilörekisteririkoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. (8.6.2001/480)

5.2 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta

Valtionhallinnon tietoturvallisuuden kehittämistä, hoitamista ja ohjausta koskeva periaatepäätös koskee ministeriöitä, virastoja ja laitoksia sekä näiden ulkopuolisilta tahoilta hankkimia tai perustamiinsa osakeyhtiöihin ulkoistamia tiedonkäsittely-, tieto-

hallinto- ja tiedonsiirtopalveluja. Tätä päätöstä sovelletaan myös valtion liikelaitoksiin silloin, kun niillä on viranomaistoimintaa.

Periaatepäätöksen tarkoituksena on parantaa organisaatioiden toimintojen ja tiedonkäsittelyn tietoturvallisuuden sekä henkilötietojen tietosuojan tasoa. Tämä tapahtuu kehittämällä valtionhallinnon tietoturvaperiaatteita ja antamalla tietoturvallisuuden hallintaa ja kehittämistoimenpiteitä koskevia suosituksia. Lisäksi päätös täsmentää tietoturvallisuuden työnjakoja ja vastuita sekä yksilöi keskeisiä viranomaisten tehtäviä.

Periaatepäätöksen mukaan kunkin viranomaisen tulee huolehtia siitä, että tietoturvallisuus ja tietojen sekä asiakirjojen suojaaminen toteutuvat omassa organisaatiossa ja myös hankittaessa palveluita organisaation ulkopuolelta. Toimeksianto ei vapauta käyttäjää velvoitteestaan huolehtia tietoturvallisuudesta, eikä vastuuta voi siirtää yksinomaan toimeksisaajalle. Kokonaisvastuu tietoturvallisuudesta on aina asianomaisen viraston tai laitoksen johdolla.

Periaatteita noudatetaan myös valtionhallinnon ja muiden organisaatioiden, kuten kuntien, yritysten ja yhteisöjen, välisessä tiedonkäsittelyn yhteistyössä ja tiedonsiirrossa.

Periaatepäätös löytyy osoitteesta: http://www.vm.fi/tiedostot/pdf/fi/6294.pdf

5.3 Valtioneuvoston periaatepäätös kansallisesta tietoturvallisuusstrategiasta

Valtioneuvosto teki 4.9.2003 periaatepäätöksen kansallisesta tietoturvallisuusstrategiasta. Strategiaan on koottu linjauksia ja toimia, joilla tietoturvallisuutta ja yksityisyyden suojaa voidaan parantaa. Kansallisella tietoturvallisuusstrategialla halutaan lisätä kansalaisten ja yritysten luottamusta tietoyhteiskuntaan.

Strategia antaa yhteiset tavoitteet valtioneuvoston, elinkeinoelämän, järjestöjen ja yksityisten kansalaisten tietoturvallisuusponnisteluille. Kansallisen tietoturvallisuusstrategian tavoitteena on rakentamaa Suomesta tietoturvallinen tietoyhteiskunta. Strategian tavoitteena on:

1. Edistää kansallista ja kansainvälistä tietoturvallisuusyhteistyötä.
2. Edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia.
3. Parantaa tietoturvallisuusriskien hallintaa.
4. Turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma.
5. Lisätä tietoturvallisuustietoisuutta ja –osaamista.

Periaatepäätös perustuu keväällä 2003 toimikautensa päättäneen tietoturvallisuusasioiden neuvottelukunnan joulukuussa 2002 tekemään ehdotukseen kansalliseksi tietoturvallisuusstrategiaksi. Tietoturvallisuusstrategiassa ehdotetaan uuden tietoturva-asioiden neuvottelukunnan perustamista. Liikenne- ja viestintäministeriö aikoo asettaa neuvottelukunnan syksyllä.

Kansallinen tietoturvastrategia löytyy osoitteesta:

http://www.mintc.fi/www/sivut/suomi/tele/periaatepaatos.pdf

5.4 Valtionhallinnon tietoturvallisuusohjeet (VAHTI-ohjeet)

Valtiovarainministeriö (VM) ohjaa ja yhteensovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Ohjeita kehittää valtionhallinnon tietoturvallisuuden johtoryhmä, joka on VM:n asettama, tietoturvallisuuden asiantuntemusta laajapohjaisesti edustava ryhmä. Sen toiminnassa pyritään ottamaan huomioon myös muu julkishallinto, kuten esimerkiksi kunnallishallinto. Ohjeistus kattaa kaikki tietoturvallisuuden osa-alueet.

Tässä luvussa on otettu huomioon ne VAHTI-ohjeet, joissa käsitellään käyttäjän tietoturvakoulutusta tai ohjeistusta.

Ohjeet löytyvät osoitteesta: http://www.vm.fi/vahti

Valtion tietohallinnon Internet-tietoturvallisuusohje (VAHTI 1/2003)

Valtion tietohallinnon Internet-tietoturvallisuusohjeen on tarkoitus olla apuvälineenä Internet-käytön ja Internetissä tarjottavien palveluiden tietoturvallisen toteutuksen ohjauksessa, suunnittelussa, valvonnassa, itse toteutuksessa ja myös näihin liittyvissä hankinnoissa. Ohjeen pääasiallisena kohderyhmänä ovat organisaation tietohallinto- ja tietoturvallisuustehtävissä toimivat. Ohjeessa keskitytään Internet-verkon ja sen tietoturvallisuuden keskeisiin asioihin. Ohjeen keskeisen sisällön muodostavat varsinainen Internetin käytön tietoturvallisuuden ohjeistus (luku 3), Internet-verkon ja sen infrastruktuurin kuvaus (luku 2) sekä näitä lukuja täydentävät liitteet.

Käyttäjän tietoturvakoulutusta ja -ohjeistusta suunniteltaessa voidaan Internet-tietoturvallisuusohjeesta käyttää mm. seuraavia lukuja:

- Luku 2.3, joka käsittelee mm. selaimia ja niihin liittyen evästeitä ja välimuistia.
- Luku 3.3, joka käsittelee mm. tiedonhakua, ostamista ja asiointia Internetissä mukaan lukien viranomaisasiointi.

- Luku 3.6, joka käsittelee sähköpostia ja sähköpostin luottamuksellisuutta ja salausta.
- LIITE 1, joka on henkilökunnan Internet-käytön tietoturvaohjeen malli.

Arkaluonteiset kansainväliset tietoaineistot (VAHTI 4/2002)

Arkaluonteiset kansainväliset tietoaineistot -ohjeistus on laadittu siten, että viranomaisessa työskentelevä, kansainvälisiä tietoaineistoja käsittelevä henkilö pystyy sen avulla tarkistamaan helposti vaaditut käsittelymenettelyt eri tilanteissa. Ohjeen alussa on käsitelty Suomen lainsäädäntöä, Suomea sitovia kansainvälisiä sopimuksia ja säädöksiä ja lisäksi sivulla 15 on lyhyt turvaluokkien vertailutaulukko. Kappale 3 käsittelee arkaluonteisen kansainvälisen tietoaineiston turvallisuusvaatimuksia ja liitteissä 1 ja 2 on yksityiskohtaiset käsittelyohjeet eri turvaluokille ja merkinnöille.

Valtionhallinnon etätyön tietoturvallisuusohje (VAHTI 3/2002)

Valtionhallinnon etätyön tietoturvallisuusohje antaa suosituksia etätyön ja tietojärjestelmien etäkäytön tietoturvalliseen toteuttamiseen, mutta ei ota kantaa etätyön työoikeudellisiin, henkilöstöhallinnollisiin tai muihin vastaaviin kysymyksiin. Pääpaino on tietojärjestelmien turvallisessa etäkäytössä, mutta myös työpisteen fyysistä turvallisuudesta sekä paperimuodossa olevan tiedon käsittelystä annetaan ohjeita. Ohjeistuksessa ei käsitellä puhelimen ja telekopiolaitteen käytön turvallisuuskysymyksiä.

Kappale 4 on tarkoitettu erityisesti etätyöntekijälle ja Liite 1 esittelee etätyöhön kohdistuvia uhkia.

Toimet tietoturvaloukkaustilanteissa (VAHTI 7/2001)

Toimet tietoturvaloukkaustilanteissa -ohjeen tavoitteena on auttaa tietoturvaloukkauksen, esimerkiksi viraston palvelimiin kohdistunut tietomurto tai palvelunestohyökkäys, uhriksi joutunutta valtionhallinnon organisaatiota selviytymään tilanteesta. Ohje ei koske varsinaisesti yhteen henkilöön kohdistuneita tietoturvaloukkauksia, mutta sivun 2 pikaohje on lyhyytensä vuoksi käytännöllinen myös käyttäjiä ohjeistettaessa.

Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje (VAHTI 5/2001)

Valtionhallinnon sähköpostien ja lokitietojen käsittelyohjeessa esitetään valtionhallinnon suositeltavat käytännöt sähköpostien käsittelyyn koskien ministeriöitä sekä valtion virastoja ja laitoksia. Ohjeen keskeinen tarkastelunäkökulma on työnantajan ja työntekijän välinen suhde sähköpostien ja lokitietojen käsittelyssä. Ohjeessa tarkastellaan kokonaisuutena asiaan liittyvää lainsäädäntöä ja ongelmia sekä esitetään suositeltavat menettelytavat. Ohjeen keskeisiä kohderyhmiä ovat eritoten valtion organisaatioiden johto sekä tietohallinto- ja tietoturvavastaavat. Ohjeessa kuvataan periaatteet eri tyyppisten sähköpostiviestien käsittelyyn ja viestien lukemiseen. Liitteissä on mallit salassapitositoumuksesta, sähköpostiviestin luottamuksellisuusilmoituksesta ja suostumuksesta sähköpostiviestien lukemiseen.

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus (VAHTI 2/2001)

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus on tarkoitettu julkishallinnon johdon käyttöön hallinnollisten ja organisatoristen velvollisuuksien selvittämiseen sekä vastuualueiden ja tehtävien jakamiseen. Tietohallinnon ja tietoturvallisuuden ja erityisesti lähiverkkojen vastuuhenkilöt voivat käyttää suositusta lähiverkkojensa turvallisuustason arviointiin, toimenpideohjelman laatimiseen sekä tarvittavaan jatkuvaan kehitys- ja muutostyöhön. Lisäksi kouluttaja voi käyttää suositusta taustatiedon keräämiseen eri tietoturvallisuuden osa-alueilta ja mm. lähiverkon suojattavien kohteiden tunnistamiseen käytettäväksi opetusesimerkeissä.

Valtion viranomaisen tietoturvallisuustyön yleisohje (VAHTI 1/2001)

Valtion viranomaisen tietoturvallisuustyön yleisohjeen keskeisenä tavoitteena on tietoturvallisuuden kokonaistilanteen parantaminen valtionhallinnossa. Se tukee organisaatiota tietoturvallisuuden hoitamisessa tarvittavien asiakirjojen laatimisessa tietoturvallisuuden ylläpitämiseksi ja kehittämiseksi. Kouluttajan on erityisesti syytä huomioida sivun 46 Koulutus -kappale, jossa on malli koulutuksen sisällöstä eri aiheineen ja kohderyhmineen.

Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje (VAHTI 4/2000)

Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohjeessa esitetään suositukset haittaohjelmilta suojautumiseksi valtionhallinnossa. Ohje sisältää suositukset tietojärjestelmiin sijoitettavista haittaohjelmien havaitsemis- ja torjuntamenetelmistä, työasemien käyttäjien ohjeista sekä menettelytavat haittaohjelmien käsittelyyn ja raportointiin. Pääpaino on asetettu ennalta ehkäisevään toimintaan. Yleisohjetta voivat käyttää sekä kouluttaja että peruskäyttäjä lisätiedon keräämiseksi aiheesta. Erityisesti on syytä huomioida Liite 5, joka on tiivis peruskäyttäjän pikaohje.

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VAHTI 2/2000)

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeen tarkoituksena on parantaa ministeriöiden, virastojen ja laitosten tietoaineistojen käsittelyn elinkaaren eri vaiheiden tietoturvallisuutta sekä määritellä asiakirjojen luokittelun pohjalta yhteneviä käsittelyperiaatteita. Ohjeeseen sisältyvät linjaukset asiakirjojen ja tietojen luokituksesta ja suojaamisesta. Se sisältää myös linjaukset tietojen käsittelyn elinkaaren eri vaiheiden turvallisuusvaatimuksista ja suositeltavista käytännöistä. Ohje määrittelee hyvän tiedonhallintatavan ja tietoturvallisuuden varmistamistarpeiden mukaiset tietojen luokituskäytännöt erityisesti luottamuksellisuuden osalta sekä tähän luokitteluun perustuvat tietojen käsittelyohjeet. Lisäksi on määritelty yleisesti eheyteen ja käytettävyyteen liittyviä vaatimuksia.

Kouluttaja voi käyttää mm. sivun 7 kuvaa ja liitteen 2 kuvauksia turvaluokista esitellessään tietojen luokittelua. Liite 2 on julkaistu aiemmin erillisenä ohjeena nimellä

’Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje (VM 19.1.2000)’

Valtionhallinnon tietoturvallisuuskäsitteistö (VAHTI 1/2000)

Valtionhallinnon tietoturvallisuuskäsitteistö on julkaistu linkissä:

http://www.vm.fi/tietoturvasanasto/sisallys.htm

Sanasto on sekä suomeksi että englanniksi. Sanasto uusitaan vuoden 2003 aikana.

5.5 Muiden tietoturvallisuutta ohjeistavien julkishallinnon organisaatioiden ohjeet

5.5.1 Viestintävirasto

Viestintävirasto valvoo yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain (TTsL 565/1999) noudattamista. Lain tarkoituksena on edistää yleisen teletoiminnan tietoturvallisuutta ja tilaajien ja käyttäjien yksityisyyden ja oikeutettujen etujen suojaa televiestinnässä. Myös Viestintäviraston valvoma viestintämarkkinalaki (396/1997) sisältää teleyrityksiä koskevan yleisen tason tietoturvallisuusvelvoitteen.

Lisäksi Viestintäviraston tehtäviin kuuluu valvoa TTsL:n nojalla annettujen säännösten ja määräysten noudattamista. Yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta on annettu asetus (723/1999) ja päätös (760/1999). Viestintävirasto on antanut myös teletoiminnan tietoturvallisuutta koskevia määräyksiä ja suosituksia, mutta ne eivät käsittele yksittäisen käyttäjän tietoturvallisuutta, vaan keskittyvät ohjaamaan organisaatioiden tietoturvallisuuteen.

Näiden lisäksi Viestintävirasto ylläpitää CERT-toimintaa. CERT-toiminnalla tarkoitetaan tietoturvaloukkauksien ennaltaehkäisyä ja niiden havainnointia sekä niistä tiedottamista. CERT on lyhenne englanninkielisistä sanoista Computer Emergency Response Team. CERT-organisaatioita on useita ympäri maailmaa. CERT-organisaatiot toimivat yhteistyössä keskenään jakaen tietoa tietoturvaloukkauksista ja niihin liittyvistä seikoista sekä tiedottavat niistä järjestelmien käyttäjille esimerkiksi Internetin välityksellä. CERT-toiminnan päämääränä voidaan pitää tietojärjestelmien tietoihin kohdistuvien tietoturvaloukkauksien ja uhkien toteutumisen ennaltaehkäisyä ja torjuntaa mahdollisimman objektiivisesti ja tehokkaasti.

Viestintäviraston toiminnasta löytyy tietoa osoitteesta:

http://www.ficora.fi

5.5.2 Tietosuojavaltuutetun toimisto

Tietosuojavaltuutettu antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa sekä valvoo henkilötietojen käsittelyä henkilötietolain tavoitteiden toteuttamiseksi. Tietosuojalautakunta käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa tietosuoja-asioissa. Tietosuojaviranomaiset toimivat yhteistyössä muiden Euroopan unionin jäsenvaltioiden tietosuojaviranomaisten kanssa ja antavat tarvittaessa virka-apua.

Tietosuojavaltuutettu voi antaa tarkempia ohjeita siitä, miten henkilötiedot on suojattava henkilötietojen laittomalta käsittelyltä.

Tietosuojavaltuutettu julkaisee erillisesitteitä, julkaisusarjoja ja mallilomakkeita. Julkaisut painottuvat erityisesti rekistereihin sekä rekisterin pitäjän että rekisteröidyn näkökulmasta. Käyttäjille hyödyllisiä julkaisusarjoja ovat erityisesti:

- ASIAA TIETOSUOJASTA -sarjassa julkaistaan henkilötietolakia koskevaa, tietosuojavaltuutetun toimistossa laadittua ja erityisesti rekisterinpitäjille suunnattua ohjeistusta.
- HYVÄ TIETÄÄ -sarjassa julkaistaan sekä rekisterinpitäjille ja että rekisteröidyille suunnattua yhteistä tiedotus- ja ohjausaineistoa.
- AJANKOHTAISTA TIETOSUOJASTA -sarjassa julkaistaan tiedotteen luonteista ohjeistusta, jossa lyhyesti käsitellään jotain ajankohtaista tietosuoja-asiaa tai ilmiötä

Julkaisusarjojen lisäksi Tietosuojavaltuutetun toimisto on julkaissut muun muassa

- erillisjulkaisun “Ota oppaaksi henkilötietolaki”, sekä
- Asiaa tietosuojasta -sarjassa mm. esitteet
- 4/2000 Tietosuojan ja tietoturvan “tee se itse“ -tarkastus
- 4/2000 Henkilötietolaki henkilötietojen käsittelyn ohjaajana
- 10/1999 Henkilötietojen luovuttaminen viranomaisten henkilörekisteristä
- 1/2003 Käyttäjälokin tietojen käsittely henkilötietolain mukaan sekä
- 4/2001 Yksityisyyden suoja kameravalvonnassa
- Hyvä tietää sarjassa mm. esitteen
- 1/2001 Henkilötietolain seuraamusjärjestelmä

Julkaisut löytyvät osoitteesta: http://www.tietosuoja.fi

5.5.3 Kansallisarkisto

Arkistolaitos on asiantuntija- ja palveluorganisaatio, jonka toiminnan tuloksena yksilölle ja yhteiskunnalle merkittävä arkistoaines säilyy suppeassa ja käyttökelpoisessa muodossa ja on tehokkaasti käytettävissä.

Arkistolaitoksen tehtäviä, organisaatiota sekä sisäisiä toimivaltasuhteita säätelee arkistolaitoksesta annettu asetus (832/1994). Asetuksen mukaan arkistolaitoksen tehtävänä on arkistotoimen ohjaaminen, arkistotoimen yleinen kehittäminen, viranomaisten asiakirjojen säilyttäminen, yhteiskunnan ja tutkimuksen kannalta merkityksellisten asiakirjojen hankkiminen ja säilyttäminen sekä aineistoon liittyvästä tietopalvelusta huolehtiminen. Kansallisarkisto johtaa arkistolaitoksen toimintaa, hallintoa ja kehittämistä, ohjaa valtion keskushallinnon ja muiden sellaisten arkistolaissa tarkoitettujen arkistonmuodostajien arkistotointa, joiden toimipiiri kattaa koko maan sekä toimii valtakunnallisena keskusarkistona ja toimialansa tutkimus- ja kehittämiskeskuksena. käyttävät itsenäistä päätösvaltaa niiden ratkaistaviksi säädetyissä tai määrätyissä asioissa, ohjaavat piirinsä arkistonmuodostajien arkistotointa, toimivat alueellisina keskusarkistoina sekä tutkimus ja kehittämiskeskuksina.

Kansallisarkisto on ohjeistanut valtion virastojen ja laitosten arkistointitoimea. Ohjeissa otetaan kantaa tietoturvallisuuden näkökulmasta käytettävyyteen eli arkistojen tulee tarvittaessa olla saatavilla. Lisäksi niiden hävittämistä säädellään valtionarkiston ohjeilla.

Käyttäjien tietoturvatoimintaan vaikuttavia Kansallisarkiston ohjeita ovat:

- Valtionarkiston yleisohje valtion virastojen ja laitosten arkistotoimesta. Annettu Helsingissä 27. päivänä kesäkuuta 1985. Valtionarkiston yleinen ohje n:o 13.
- Valtionhallinnon asiakirjojen seulonta ja hävittäminen. Määräys ja ohje 216/40/03, 2.6.2003.
- Sähköisten tietojärjestelmien ja aineistojen käsittely. Määräys ja ohje 126/40/01, 22.5.2001.Helsinki 2001, 19 s.

Ohjeet löytyvät osoitteesta: http://www.narc.fi/ohjeet.html

5.5.4 Tietoyhteiskunnan kehittämiskeskus (TIEKE)

Tietoyhteiskunnan kehittämiskeskus ry (TIEKE) palvelee suomalaisen tietoyhteiskunnan kehittämisessä. Se on riippumaton verkostojen rakentaja, jonka jäsenet ja yhteistyökumppanit edustavat laajaa kirjoa eri Yhteinen nimittäjä kaikilla on kehittää tietoyhteiskuntaa Suomen kansalaisten ja elinkeinoelämän parhaaksi. TIEKE toimii myös kansainvälisesti.

TIEKE yhdistää toiminnassaan jäsenistönsä ja yhteistyökumppaniensa näkemykset kansalaisnäkökulmaan. Toimintatapana on useimmiten erilaisten hankkeiden käynnistäminen ja toteuttaminen. Niiden valintaan vaikuttavat ajankohtaiset tarpeet sekä sidosryhmien kanssa käytävät keskustelut.

TIEKEn www-sivuilla on julkaistu ”Tietoturvaa peruskäyttäjille” –opas, joka on kaikille tietokoneen käyttäjille tarkoitettu tietoturvaohjeisto. Opas sisältää mm. muistilistan tärkeimmistä tietoturva-asioista, perustelut sille, miksi tietoturvallisuuden takia kannattaa nähdä vaivaa sekä runsaasti linkkejä lisätietoihin.

Opas löytyy osoitteesta: http://www.tieke.fi

6 ORGANISAATION TIETOTURVAOHJEISTUS-KOKONAISUUDEN MALLI

Käyttäjän tietoturvaohje on vain yksi osa käyttäjiä koskevasta organisaation tietoturvaohjeistuksesta. Käyttäjän ohjeen rinnalle tulee laatia selkeä ohjekokonaisuus, jonka avulla käyttäjä pystyy toimimaan asianmukaisesti ja hankkimaan tarvittavia lisätietoja tietoturvallisista toimintatavoista. Tämä on otettu huomioon myös käyttäjän ohjeen muistilistassa, jossa käyttäjä velvoitetaan tutustumaan organisaation muuhun tietoturvaohjeistukseen.

Tässä luvussa on esitetty malli tietoturvallisuuteen liittyvien ohjeiden kokonaisuudesta julkishallinnon organisaatiossa. Tarvittavat ohjeet, niiden lukumäärä ja kattavuus vaihtelevat organisaatioittain. Tietoturvaohjeiden ei pidä olla joukko satunnaisesti kirjoitettuja, toisistaan riippumattomia ohjeita, vaan selkeä ohjekokonaisuus, joka palvelee organisaation toiminnasta lähteviä tarpeita. Tavallisesti ohjeet koostuvat eri tasoilla olevista ohjetyypeistä, joista kullakin on oma käyttötarkoituksensa. Tässä mallissa on kolmentasoisia ohjeita:

1. Politiikkatason ohjeet
2. Periaatetason ohjeet
3. Toimintaohjeet

6.1 Politiikkatason ohjeet

Politiikkatason ohjeet sisältävät kuvauksen tietoturvatoimintaan liittyvistä johdon linjauksista, velvoitteista, tavoitteista ja vastuiden määrittelystä. Politiikkatason ohjeet luovat perustan organisaation tietoturvaohjeille. Niissä myös kuvataan tietoturvallisuuden vastuut ja tehtäväjako. Politiikkatason ohjeita ovat esimerkiksi:

- Tietoturvapolitiikka
- Internet-politiikka
- Sähköpostipolitiikka
- Etätyöpolitiikka

6.2 Periaatetason ohjeet

Periaatetason ohjeet sisältävät organisaatiotasoisesti kuvaukset, miten tietoturvallisuuden eri osa-alueilla toimitaan ja miten tietoturva-asioissa toimitaan. Periaatetason ohjeet voivat olla esimerkiksi seuraavilta aihealueilta:

- Suojattavat kohteet
- Tilaluokitus
- Tietojen luokittelu
- Tietoturvallisuudesta tiedottaminen
- Henkilörekisteriselosteet
- Tietojärjestelmäselosteet
- Henkilöstöturvallisuus
- Tietoturvallisuus tehtävänkuvauksissa
- Tietovälineiden käsittely
- Palvelujen tietoturvallisuuden valvonta ja raportointi
- Sopimusten tietoturvallisuus
- Tietoliikenne ja käyttötoiminnot
- Järjestelmäkehityksen tietoturvallisuus
- Tietoturvallisuuden mittarit
- Menettely tietoturvarikkomuksessa
- Avainten hallinta ja lukitukset

6.3 Toimintaohjeet

Käytännön toimintaohjeet ovat velvoittavia ohjeita. Toimintaohjeissa kuvataan yksityiskohtaisesti tietoturvatoimintaan liittyvät asiat. Toimintaohjeita voivat olla mm.:

- Käyttäjän tietoturvaohje
- Etätyöohje ja siihen liittyvä sopimus
- Etätyön tietoturvaohje
- Salassa pidettävien ja luottamuksellisten tietojen käsittelyohje
- Ohje atk-laitteiden suojauksesta
- Sähköpostiohje
- Ohje vieraiden ilmoittamisesta kulunvalvontaan
- Ohje tietoturvallisuuden auditoinnista
- Ohje tietoteknisen häiriön ilmoittamisesta
- Ohje asiakirjojen arkistoinnista ja säilytyksestä
- Ohje salaustuotteiden käytöstä
- Ohje toimikortin käytöstä
- Ohje lisenssien ja käyttäjämäärien seurannasta
- Ohje kirjattavan tiedon tarkastamisesta
- Ohje lokien seurannasta

6.4 Ohjeita täydentävät lomakkeet

- Tietoturva-aloite
- Virusilmoitus
- Häiriöilmoitus
- Käyttäjätunnushakemus (järjestelmä x)
- Kulkuoikeuslomake
- Käyttäjän vaitiolositoumus
- Harjoittelijan tietoturvalupaus
- Salassapitositoumus
- Tietoturvarikkomusilmoitus
- Tietoturvallisuuden poikkeamailmoitus

7 TIETOTURVALLISUUDEN OSA-ALUEET KÄYTTÄJÄN NÄKÖKULMASTA

Organisaation ohjekokonaisuus kattaa kaikki tietoturvallisuuden kahdeksan osa-aluetta. Tässä luvussa on tarkasteltu kutakin osa-aluetta käyttäjän näkökulmasta ja nostettu esiin niitä asioita, jotka kullakin osa-alueella erityisesti vaikuttavat käyttäjien koulutukseen ja ohjeistukseen.

Tärkeää on ymmärtää, että tietoturvallisuuden, ja erityisesti tietoturvaohjeiden saattaminen toiminnan edellyttämälle tasolle vaatii organisaation ylimmän johdon päätöstä, sitoutumista ja tukea. Organisaation johdon on tunnettava organisaation tietoturvaympäristö sekä eri sidosryhmien palveluille ja toiminnalle asettamat odotukset ja tietojenkäsittelyn riippuvuudet. Korkeimmalla tasolla se tarkoittaa tietoturvapolitiikan, tiettyjen minimivaatimusten asettamista sekä toimintojen tärkeysluokituksen määrittelyä. Näiden pohjalta laaditaan käyttäjien ohjeet kullekin tietoturvallisuuden osa-alueelle.

7.1 Hallinnollinen turvallisuus

Hallinnollinen tietoturvallisuus on tietoturvallisuuden johtamistoiminto ja organisaation koko tietoturvatoiminnan lähtökohta. Se muodostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista. Varsinaiset toimenpiteet perustuvat hallinnollisiin ohjeisiin, joiden pohjana toimivat johdon määrittelemät periaatteet. Ilman kunnollista tietoturvaperiaatteiden luomista, hallinnointia ja suunnittelua turvallisuusjärjestelyt saattavat sisältää suuria puutteita tai ne voivat olla suunnattu vääriin asioihin.

Hallinnollisen turvallisuuden tarkoituksena on luoda organisaatioon tietoturvalliset toimintatavat. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi.

Hallinnollisessa turvallisuudessa on oleellista, että käyttäjät tietävät ja ymmärtävät ne periaatteet, joille organisaation tietoturvallisuus rakentuu. Tätä varten organisaation johdon tulee julkaista organisaation tietoturvapolitiikka. Politiikka jaetaan koko henkilökunnalle. Tietoturvapolitiikan tueksi tulee suunnitella organisaation ohjekokonaisuus (vrt. luku 6) ja määritellä vaadittu tietoturvakuvausten taso. Lisäksi laaditaan tietoturvasuunnitelmat, jotka osoittavat organisaatiolle elintärkeät tietojärjestelmät, niiden toipumistoimet sekä vaatimukset poikkeusolojen valmiudelle.

Käyttäjille oleellisia asioita hallinnollisessa turvallisuudessa ovat:

- Organisaation tietoturvapolitiikka ja –periaatteet
- Tietoturvavastuiden jako työjärjestyksissä ja tehtäväkuvauksissa
- Tietoturvaohjeiden laatu, kattavuus ja niiden koulutus
- Allekirjoitetut vakuutukset turvaohjeiden lukemisesta ja noudattamisesta

Käyttäjän tulee olla tietoinen ohjekokonaisuudesta ja erityisesti niistä ohjeista, jotka säätelevät hänen omaa työtänsä. Lisäksi organisaation tietoturvavastuut tulee olla selkeästi määriteltynä ja kirjoitettuna muistiin. Käyttäjiä koskevat vastuut tulee kouluttaa ja ohjeistaa, jotta jokainen käyttäjä on tietoinen omista tietoturvavastuista ja pystyy toimimaan vastuun edellyttämällä tavalla. Koulutus tulee aloittaa jo uuden työntekijän perehdytyskoulutuksessa. Käyttäjän tulee myös tietää, kuka on organisaation tietoturvallisuudesta vastaava henkilö.

7.2 Henkilöstöturvallisuus

Valtionhallinnon tietoturvakäsitteistön mukaan henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien riskien hallintaa koskien henkilöstön soveltuvuutta, toimenkuvia, sijaisuuksia, tiedonsaanti- ja käyttöoikeuksia, suojaamista, turvallisuuskoulutusta ja valvontaa.

Henkilöstöturvallisuuteen voidaan vaikuttaa käyttäjien motivoinnilla ja koulutuksella. Henkilöstöturvallisuuteen vaikuttavat myös käyttäjän palkkaus, työsopimus ja työkyky. On hyvä tiedostaa, että luotettavankin käyttäjän motivaatio ja elämäntilanne saattavat muuttua ja johtaa luvattomuuksiin, häirintään ja tietojen luvattomaan luovutukseen. Lisäksi lyhyiden työsuhteiden ja alihankinnan vuoksi julkishallinnon organisaatioiden henkilökunta saattaa vaihtua useasti ja toimintaan osallistuu lähes tuntematonta henkilöstöä. Kuitenkin tietojenkäsittelyyn osallistuvien henkilöiden määrä kasvaa koko ajan.

Henkilöstön oikea valinta ja koulutus sekä irtisanomisten yhteydessä noudatettavat selkeät menettelytavat pienentävät henkilöstöturvallisuuden riskiä. Henkilöstöturval-

lisuuteen liittyviä riskejä yritetään välttää myös käyttäjien taustatarkistuksilla, soveltuvuustesteillä ja joissain tapauksissa huumetesteillä. Käyttäjille tulee avoimesti sekä koulutuksissa että ohjeistuksessa kertoa näistä toimenpiteistä ja niiden perusteista. Käyttäjille tulee myös selvittää, mitä esimerkiksi taustatarkistuksesta saatavat tulokset merkitsevät käyttäjän työtehtävien kannalta.

Henkilöstöturvallisuuteen liittyvät myös avainhenkilöriskit. Niihin voidaan vaikuttaa suunnittelemalla ajoissa sijaisuusjärjestelyt, harjoittamalla tehtäväkiertoa, nimeämällä ja kouluttamalla varahenkilöt sekä kuvaamalla kirjallisesti toimintamallit ja tietojärjestelmät. Näiden lisäksi jokainen yksittäinen käyttäjä pystyy vaikuttamaan avainhenkilöriskiin toimimalla niin, että tiedot ja osaaminen eivät ole ainoastaan hänen hallussaan. Organisaatio ei saa toimia niin, että yksittäisen käyttäjän työpaikka tai urakehitys perustuu itsensä tekemiseen korvaamattomaksi.

Avainhenkilöriskien lisäksi yksittäisen käyttäjän kohdalla ei saa muodostua vaarallista työyhdistelmää. Sama käyttäjä ei saa esimerkiksi hyväksyä ostolaskua ja laittaa sitä maksuun. Vastaavia työyhdistelmiä tulee välttää myös kahden tai useamman toisilleen läheisen henkilön, kuten perheenjäsenten, kesken. Käyttäjien koulutuksessa on hyvä ottaa esiin vaaralliset työyhdistelmät, jotta käyttäjät osaavat itsekin kiinnittää asiaan huomiota esimerkiksi työtehtävien muuttuessa.

Käyttäjän ohjeistuksessa henkilöstöturvallisuudesta on hyvä huomioida ainakin seuraavat asiat:

- Lainsäädännön velvoitteet (esim. virkamieslaki, julkisuuslaki)
- Tietoturvavelvoitteet käyttäjän työ- tai virkasopimuksessa
- Salassapitositoumukset
- Käyttöoikeuksien vastaavuus tehtäviin
- Varahenkilöjärjestelyt
- Puuttuminen turvallisuusriskejä aiheuttavaan toimintaan
- Ostopalveluiden ja muun organisaation ulkopuolisen henkilökunnan henkilöstöturvallisuuden hallinta
- Muiden organisaatioiden henkilökuntaan kuuluvien oikeudet ja rajoitukset (esimerkiksi toimittaessa samoissa toimitiloissa)

7.3 Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa niitä toimenpiteitä, joilla tietojenkäsittelyyn liittyviä kohteita suojellaan fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä. Laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä ja erilaisilta palo-, vesi- ja kiinteistövahingoilta.

Toimitilojen turvallisuudesta käyttäjälle on ohjeistettava:

- Toimitilaluokitus
- Kulunvalvontasäännöt
- Kulunvalvonta- ja murtohälytyslaitteiden käyttäminen
- Toimitilojen turvavyöhykkeet ja siirtyminen turvavyöhykkeeltä toiselle
- Henkilö- ja vierailijakorttien käyttö
- Tilat, joihin saa tuoda vierailijoita
- Vierailijoiden kanssa toimiminen (esim. vieraiden vastaanotto ja saattaminen tai vieraiden jättäminen yksin asiakastiloihin)
- Laitteiden sijainti ja sijoittelu omassa työpisteessä (esim. asiakaspalvelussa tietokoneen näyttö ei saa näkyä asiakkaalle tai työasemaa ei kannata pitää ikkunalaudalla suorassa auringonpaisteessa)
- Yleisestä toimitiloihin liittyvät turvallisuudesta huolehtiminen (esim. kahvinkeittimen sammuttaminen ja ikkunoiden sulkeminen töiden päätyttyä)

Käyttäjän tulee myös tiedostaa, että tilojen järjestys ja siisteys on olennainen osa tietoturvallisuutta. Käyttäjille tulee ohjeistaa ns. ”Puhtaan pöydän” –periaate, mikä tarkoittaa, että työpöydällä tai muulla näkyvällä paikalla ei saa säilyttää salassa pidettävää aineistoa. Samalla tavoin levykkeet, CD-Rom –levyt ja muut tietovälineet tulee säilyttää niin, että ne eivät vahingoitu tai kärsi fyysisiä vaurioita.

Omien laitteiden käsittelyyn sisältyy erityisesti kannettavan tietokoneen ja matkapuhelimen kuljetus ja säilytys organisaation toimitilojen ulkopuolella. Käyttäjällä on oltava ohjeet kannettavan tietokoneen asianmukainen säilytyksestä autossa, julkisessa liikennevälineessä, kotona, hotellihuoneessa sekä julkisella paikalla.

Käyttäjän on myös hyvä olla tietoinen niistä periaatteista, jotka ohjaavat organisaation fyysisen turvallisuuden suunnittelua ja toteutusta. Esimerkiksi käyttäjille on hyvä kertoa, että kulkuoikeuksien saaminen perustuu työtehtävistä syntyviin tarpeisiin. Käyttäjän tulee myös olla tietoinen häneen kohdistuvasta valvonnasta organisaation toimitiloissa. Jos organisaatiolla on käytössään kamera- tai kulunvalvonta, on niistä tiedotettava henkilökuntaa.

Jos organisaation toimitilaturvallisuudesta ja fyysisestä turvallisuudesta vastaavat eri henkilöt kuin tietoturvallisuudesta, on vastuunjako oltava selkeästi käyttäjien tiedossa.

7.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan toimenpiteitä, joilla varmistetaan tietojen turvallisuus niiden liikkuessa järjestelmästä toiseen joko organisaation sisällä tai organisaatioiden välillä. Käyttäjälle oleellisia tietoliikenneturvallisuuteen liittyviä asioita ovat sähköpostin ja Internetin käyttö, tietoliikenteen salaus sekä etäyhteydet.

7.4.1 Sähköposti

Sähköposti on julkishallinnon organisaatioiden viestinnän tärkein palvelu. Sitä käytetään paitsi organisaation sisäiseen viestintään, myös virka-asioiden hoitamiseen kansalaisten sekä muiden sidosryhmien kanssa. Julkisen hallinnon tietohallinnon neuvottelukunta on julkaissut suosituksen JHS 132 Sähköpostin käyttö asioinnissa, joka käsittelee sähköpostin tuomia mahdollisuuksia ja ongelmia sekä julkishallinnon yksiköiden sisäisessä että niiden välisessä toiminnassa. Julkaisussa on ohjeistettu myös sähköpostilla tapahtuvan asioinnin kirjaamis-, arkistointi- ja säilytysmenetelmiä. Arkistolaitos on täydentänyt kyseistä ohjetta ja antanut myös viranomaisia sitovia määräyksiä sähköpostiin liittyvien asiakirjojen arkistoinnista, kirjaamisesta ja säilyttämisestä.

Käyttäjille on oleellista, että jokainen käyttäjä ymmärtää sähköpostin käyttöön liittyvät velvoitteet, rajoitteet ja säädökset. Sähköpostin turvallisen ja asianmukaisen käytön varmistamiseksi käyttäjille täytyy luoda organisaatiossa selkeät periaatteet sähköpostin käyttöön. Ylätasolla sähköpostin käyttö- ja valvontaperiaatteet määritellään tietoturvapolitiikassa, mutta yksityiskohtaisemmista periaatteista laaditaan oma ohjeensa. Lähtökohta on, että periaatteiden on oltava koko henkilöstön tiedossa ja niiden tulee olla organisaation johdon vahvistamat.

Periaatteissa tulee ottaa kantaa sähköpostin käytön rajoituksiin, työntekijän henkilökohtaisen sähköpostiosoitteen käyttöön, virkapostien ohjaamiseen organisaation ulkopuolelle sekä sähköpostin käytön valvontaan. Kunkin käyttäjän tulee ymmärtää, että viranhoitoon liittyvän sähköpostiliikenteen tulee kulkea organisaatioiden, ei yksittäisten virkamiesten, välillä.

Liitteenä 2 oleva käyttäjän ohje sisältää seuraavat sähköpostin käyttöä koskevat asiat:

- Viranomaisen velvollisuudet virkasähköpostin käsittelyssä
- Virkasähköpostin käsittelyä koskevat rajoitukset (laitteet, sähköpostiohjelmat)
- Liitetiedostojen käsittely
- Sähköpostin virustorjunta
- Roskaposti
- Sähköpostin luotettavuus
- Sähköpostitietojen oikeellisuuden tarkistaminen

Käyttäjän tulee myös olla tietoinen sähköpostiviesteihin ja sähköpostin käyttöön liittyvistä säädöksistä. Sähköpostin tietoturvallisuuteen kohdistuvat rikoslain säädökset oikeudettomasta puuttumisesta toisten viesteihin ja henkilötietolain säädökset henkilötietojen käsittelystä. Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta koskee televiestinnän luottamuksellisuutta, salassapitovelvollisuutta ja hyväksikäyttökieltoa. Laissa viranomaisen toiminnan julkisuudesta annetut säädökset koskevat viranomaisen tietojen ja asiakirjojen salassapitoa ja käsittelyä myös sähköpostissa. Laissa yksityisyyden suojasta työelämässä sähköpostin ja tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa sekä yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin.

Käyttäjän tulee myös tiedostaa, että salassa pidettävää tietoa ei saa lähettää sähköpostissa salaamattomana. Vaikka sähköpostia käytetään nykyään paljon virkatehtävien hoitamiseen, ei salaamattoman sähköpostin lähettäminen ole turvallisempaa kuin postikorttien lähettäminen. Suojaamattomia sähköpostiviestejä voidaan lukea, muuttaa tai poistaa lähettäjän ja vastaanottajan tietämättä. Käyttäjille tulee ohjeistaa, miten salassa pidettävät tiedot voidaan suojata tehokkaasti salauksen ja digitaalisen allekirjoituksen avulla. Salauksen ja digitaalisen allekirjoituksen käytön helpottamiseksi ohjeissa tulee selkeästi kertoa, mitkä tiedot täytyy salata sähköpostia käytettäessä ja kuinka salaus tapahtuu. Useasti salausta ei käytetä, koska käyttäjät eivät tiedä organisaatiossa käytössä olevista salausohjelmistoista tai eivät osaa niitä käyttää.

7.4.2 Internet

Julkishallinnon organisaatioissa on viime vuosina yhä enenevissä määrin annettu käyttäjille mahdollisuus Internetin käyttöön työssään. Myös valtioneuvoston periaatepäätös tietoturvallisuudesta velvoittaa ministeriöt ja virastot huolehtimaan siitä, että merkittävä osa julkishallintoon osoitetuista viesteistä ja hakemuksista voidaan vastaanottaa ja saattaa vireille verkkojen kautta.

Internetin käytössä pätee sama lähtökohta kuin sähköpostin käytössä eli organisaation on luotava käyttäjille yksiselitteiset periaatteet Internetin käyttöön. Internetin käyttöperiaatteet, ehdot ja vaatimukset tulee määritellä organisaatiokohtaisesti tietoturvapolitiikassa.

Liitteenä 2 oleva käyttäjän ohje ottaa kantaa seuraaviin Internetiin käyttöä koskevat asioihin:

- Internet on tarkoitettu työkäyttöön.
- Salassa pidettävän aiheiston välittäminen Internetin kautta
- Internetistä saatavien ohjelmien asennus ja käyttö
- Internetin käyttö julkisilta päätteiltä tai toisen käyttäjän koneelta
- Internetissä leviävien virusten ja muiden haittaohjelmien torjunta

Internetin tietoturvasuosituksia on Valtion tietohallinnon Internet-turvallisuusohjeessa sekä PTS:n selvityksessä: Internet, toiminnan verkottuminen ja sen haavoittuvuus. Valtion periaatteet velvoittavat myös julkishallinnon tietoja käsitteleviä ulkopuolisia tahoja.

Tietoliikenteen salaus on tärkeä keino Internetissä siirrettävän tiedon suojaamiseen. Salauksella nostetaan ratkaisevasti eheyden, luottamuksellisuuden, käytettävyyden, todentamisen sekä kiistämättömyyden tasoa.

Käyttäjälle on ohjeistettava, missä tilanteissa salausta käytetään, mitä salausohjelmistoja organisaatiolla on käytössään ja miten niitä käytetään.

7.4.3 Etäyhteydet

Etäyhteyksien käyttö voi liittyä etäkäyttöön tai etätyöskentelyyn. Etäkäytöstä on kysymys silloin, kun käytetään organisaation tietoverkkoa tai sen osaa tietoliikenneyhteyden avulla organisaation ulkopuolelta. Etätyöllä tarkoitetaan muualla kuin viraston vakituisessa toimipisteessä tehtävää työtä.

Lähtökohtana on, että etäyhteysoikeus on poikkeuksetta henkilökohtainen ja yhteyden avaaminen edellyttää käyttäjältä aina erikseen allekirjoitettua sopimusta. Organisaation johto päättää, keille etäkäyttöoikeus annetaan ja minkä tasoinen yhteys on.

Käyttäjille oleellista on ymmärtää, että etäkäyttöympäristöstä ja -työasemasta vastaa yksinomaan yhteyden käyttäjä itse. Käyttäjä vastaa siitä, ettei yhteyden välityksellä saatava tai työasemassa oleva muu kuin julkinen tieto joudu missään olosuhteissa ulkopuolisten saataville eikä nähtäville.

Etäyhteyksiä ohjeistettaessa käyttäjien täytyy saada vastaus ainakin seuraaviin kysymyksiin:

- Miten hoidetaan pääsynvalvonta tietokoneelle? Käytetäänkö toimikorttia?
- Mitä jos pääsynvalvontaan käytettävä todennusväline varastetaan?
- Miten etäyhteyden tietoliikenne suojataan?
- Mitä tietoa saa käsitellä etäkäyttöisesti?
- Miten suojataan yrityksen ulkopuolella olevassa työasemassa säilytettävät tiedot?
- Mitä jos tietokone varastetaan?

7.5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan tietoturvallisuuden osa-aluetta, joka käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen. Laitteistoturvallisuuden tavoitteena on ensisijaisesti vähentää laitteista aiheutuvia häiriöitä ja keskeytyksiä.

Laitteistoturvallisuudesta on käyttäjille hyvä ohjeistaa ja kouluttaa ainakin seuraavat asiat:

- Laitteiden asianmukainen käsittely (esim. monitorin virran sammuttaminen yöksi)
- Laitteiden toiminnan seuraaminen (esim. tietokoneen tuulettimen toimimattomuus tai sen muuttuminen äänekkääksi tai jonkin laitteen ylikuumeneminen)
- Laitteiden turvallinen säilytys (esim. lukittu huone ja laitteen sijoittelu työhuoneessa)
- Omien tietotekniikkalaitteiden tuominen töihin ja liittäminen organisaation tietojärjestelmiin, laitteisiin tai tietoverkkoon.

Jos käyttäjällä on valtuus hankkia laitteistoja ilman, että organisaation tietohallinto on hankintaprosessissa mukana, tulee käyttäjää ohjeistaa hankkimaan laitteisto toimittajalta, joka pystyy vastaamaan laitteen huollosta ja takuista. Lisäksi käyttäjän on osattava laitehankinnan yhteydessä arvioida mm. laitteen kapasiteetti- ja ylläpitotarvetta

7.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus on tietoturvallisuuden osa-alue, joka käsittää käyttöjärjestelmät, väliohjelmistot *(middle ware)*, sovellusohjelmat ja tietoliikenneohjelmistot. Alueeseen kuuluvat ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt, ohjelmistojen laadunvarmistus sekä niiden ylläpitoon ja päivitykseen liittyvät turvallisuustoimet. Ohjelmistoturvallisuuden tarkoituksena on suunnata hankinnat sellaisiin ohjelmistoihin, jotka omilla piirteillään tukevat turvallisuutta. Ohjelmistoturvallisuuteen kuuluvat myös varsinaisten turvallisuusohjelmien luotettavuus ja laadun varmistus.

Käyttäjille tärkeimpiä asioita ohjelmistoturvallisuudessa ovat väliaikaistiedostot (temptiedostot), ohjelmien versiohallinta, ohjelmistolisenssit sekä viruksiin ja muihin haittaohjelmiin varautuminen.

Versioerot voivat synnyttää toimimattomia yhdistelmiä ja esimerkiksi uudella versiolla tehdyt aineistot eivät välttämättä aukea, jos niitä yritetään avata vanhemmalla ohjelmistoversiolla.

Käyttäjiltä tulee kieltää ohjelmistojen lataaminen Internetistä. Tähän on olemassa useita perusteluja:

- Internetistä ladattavat ohjelmat saattavat sekoittaa muiden ohjelmistojen asetukset ja tällä tavoin estää muiden ohjelmien tai koko tietokoneen käytön.
- Internetistä ladattavat ohjelmat saattavat sisältää haittaohjelmia.
- Internetistä ladattavat ilmaisohjelmat voivat olla täysin luotettavia, mutta vain yksityiskäytössä ilmaisia. Työkäyttöön ladattuna ne useimmiten vaativat maksullisen lisenssin.
- Ohjelmien lataaminen saattaa kuormittaa organisaation verkkoa huomattavasti.

Virukset voivat aiheuttaa vakavia keskeytyksiä yksittäisen käyttäjän tai koko organisaation toimintaan ja äärimmillään aiheuttaa koko toiminnan lamautumisen. Käyttäjiä tulee ohjeistaa toimimaan oikein sekä virustorjunnassa että tilanteessa, jossa virus on päässyt käyttäjän koneelle. Käyttäjiä tulee lisäksi ohjeistaa, että viruksilta suojautumiseen kuuluu myös hyvin hoidettu puhtaiden varmuus- ja suojakopioiden ylläpito sekä tarpeettoman sähköpostiaineiston poistaminen. On kuitenkin muistettava, että virusten torjunta ei voi jäädä yksittäisten käyttäjien ja kieltojen varaan.

Käyttäjille on hyvä tiedottaa organisaation käyttöoikeus- ja pääsynvalvontamenettelyistä. Käyttäjän tulee noudattaa tiukasti työtehtävissä sallittavia valtuuksia. Hänen tulee olla tietoinen organisaatiossa käytettävistä tietoturvarikkomuksien havainnointimenetelmistä.

Jos käyttäjällä on valtuus hankkia ohjelmistoja ilman, että organisaation tietohallinto on hankintaprosessissa mukana, tulee käyttäjää ohjeistaa hankkimaan ohjelmisto toimittajalta, joka pystyy takaamaan ohjelmiston ylläpidolle riittävän jatkuvuuden ja tuen. Lisäksi ohjelmistotoimittajan tulee pystyä osoittamaan, että ohjelmisto on testattu ja dokumentoitu.

7.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tietojen ja niitä sisältävien järjestelmien tunnistusta, luokittelua ja valvontaa käsittelyn eri vaiheissa. Se sisältää asiakirjojen, tiedostojen, ääninauhojen, kuvanauhojen, näytteiden ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden takaamisen kaikissa tiedon elinkaaren vaiheissa. Tiedon elinkaaren vaiheet ovat tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi sekä tuhoaminen.

Keinoja tietoaineistoturvallisuuden takaamiseksi ovat mm. tietoaineistojen luetteloinnti ja luokitus sekä tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen.

Käyttäjien koulutuksessa on hyvä painottaa niitä seurauksia, jotka syntyvät tietoaineiston tietosisällön heikkoudesta, tietojen eheyden menetyksestä tai luottamuksellisuuden rikkoutumisesta tiedon elinkaaren eri vaiheissa. Näitä ovat mm.

- Väärinymmärrykset
- Virheellisen tiedon leviäminen jatkokäsittelyyn
- Päätösten tekeminen virheellisin tiedoin
- Työmäärän lisääntyminen
- Huono kuva viranomaisen toiminnasta

Käyttäjiä on myös hyvä muistuttaa, että tietoaineistojen käsittely muutoin kuin työtehtävien edellyttämällä tavalla, on kiellettyä. Esimerkiksi julkishallinnon rekistereitä ei saa käyttää muuhun kuin työtehtäviin liittyvään tiedonhakuun.

Tietoaineistoturvallisuus koskee kaikkea organisaation tietoa, mutta tämän lisäksi julkishallinnon tietojärjestelmissä on paljon tietoja, jotka ovat erityisten säädösten perusteella suojattava. Tiedon suojaamisen perustana on tietojen, tietojärjestelmien ja sovellusten luokitus luottamuksellisuuden mukaan sekä luokituksen perusteella käyttöön otetut suojausmenetelmät. Tallennetun tiedon ja ohjelmistojen suojaaminen vahingoilta, vahingoittamiselta ja menetyksiltä koskee kaikkia käyttäjiä. Tietoaineiston turvallisuus ei kuitenkaan kohdistu ainoastaan tietojärjestelmiin, vaan luokituksen perusteella määritellään käsittelysäännöt myös muulle tiedonkäsittelylle. Asiakir-

jan virallisuus ei riipu viestintä- ja käsittelyvälineestä tai asiakirjan fyysisestä muodosta. Sähköpostitse lähetettävä ja vastaanotettava asiakirja voi olla yhtä virallinen kuin paperimuotoinen asiakirja, jos se liittyy virka-asian hoitamiseen.

7.7.1 Tiedon luokitus

Luokituksen tarkoituksena on jakaa tiedot ryhmiin, joille asetetaan käsittelysäännöt. Niiden tulee sisältää ohjeet tiedon käsittelystä, säilytyksestä, tuhoamisesta ja viestittämisestä erilaisia tiedonsiirtoyhteyksiä käyttäen. Ohjeet koskevat eri olomuodoissa olevaa tietoaineistoa.

Käyttäjien koulutuksen ja ohjeistuksen tulee sisältää ainakin seuraavat tietojen luokitteluun liittyvät asiat:

- Tietojen luokitus ja luokitusperiaatteet
- Aineiston salassapitotarpeen ja siitä seuraavan luokittelun määrittely aineistoa luotaessa
- Käyttövaltuuksien myöntäminen eri luokitusryhmille ja siitä seuraavat tiedon käyttö- ja käsittelysäännöt
- Luokitellun tiedon välittäminen tietojärjestelmissä ja Internetissä
- Erityisesti erittäin salaisen ja salaisen aineiston suojaaminen
- Henkilörekisterien käsittely ja suojaaminen

7.7.2 Tietosuoja

Tietosuoja on tietoaineiston turvaamisen erikoisalue. Sillä tarkoitetaan henkilötietojen suojaamista valtuudettomalta tai henkilöä vahingoittavalta käytöltä. Käytännössä tietosuoja liittyy pitkälti henkilörekisterien tietoturvallisuuteen.

Arkaluonteisten henkilötietojen käsittely on kielletty henkilötietolaissa määriteltyjä poikkeuksia lukuun ottamatta. Henkilörekisterin pitäjänä organisaation on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomilta ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Käyttäjien ohjeistuksessa ja koulutuksessa tulee erityisesti painottaa seuraavia asioita:

- Henkilötietojen käsittelyyn, luovutukseen ja käyttöön liittyvät säännökset
- Henkilötietojen käsittelyyn, luovutukseen ja käyttöön liittyvät turvatoimet (esim. tietojen salaus)

7.7.3 Varmuuskopionti

Tietoaineistoturvallisuuteen liittyy olennaisena osana varmuuskopiointi. Varmuuskopioinnilla varmistetaan erityisesti tietojen käytettävyys. Varmuuskopioita tarvitaan esimerkiksi, kun työasema tai palvelin hajoaa, tallennettu aineisto tuhoutuu tai virus saastuttaa työstettävät aineistoversiot.

Käyttäjien ohjeistuksessa ja koulutuksessa tulee erityisesti painottaa seuraavia varmuuskopiointiin liittyviä asioita:

- Organisaation mahdolliset varmuuskopiointia helpottamaan tehdyt järjestelyt (esim. ”Varmuuskopioi”-painike työaseman näytöllä)
- Varmuuskopioinnin vastuunjako (esim. käyttäjä varmistaa oman kovalevynsä, tietohallinto varmistaa verkkolevyt)
- Varmuuskopiointivaihtoehdot (verkkolevy, levyke, CD-Rom, zip-asema)
- Varmuuskopioinnin suositeltu aikaväli (esim. varmuuskopiot otetaan kerran viikossa)

7.7.4 Suoja-/turvakopiointi

Suoja-/turvakopioinnilla tarkoitetaan tietojen ja aineistojen tallettamista pysyvään säilytykseen. Sitä tarvitaan esimerkiksi silloin, kun halutaan tietoaineiston säilyvän, mutta sitä ei arkistoida. Näin voidaan toimia esimerkiksi silloin, kun halutaan jonkin tutkimus- tai luonnosaineistojen säilyvän, mutta joita ei ole järkevä arkistoida.

7.7.5 Arkistointi

Arkistointi ei ole sama asia kuin varmuus tai suojakopiointi. Arkistoinnilla tarkoitetaan asiakirjojen tai tallenteiden pitkäaikaista tai pysyvää säilyttämistä. Arkistoinnin avulla varmistetaan tietojen käytettävyys. Julkishallinnon arkistointia säädellään arkistolailla.

Käyttäjille tulee laatia omat ohjeet arkistoinnista. Ohjeessa on hyvä muistuttaa, että sähköpostijärjestelmä ei ole arkistointijärjestelmä ja ohjetta laadittaessa tulee ottaa huomioon arkistolaitoksen määräys “Arkistotoimen vaatimukset sähköpostin käsittelyssä”.

Sähköisessä muodossa olevien asiakirjojen arkistoinnissa tulee myös hyvin selkeästi ohjeistaa, missä tallennusmuodossa arkistointi tapahtuu. Tämä on tärkeää, jotta asiakirjat saadaan avattua pitkänkin ajan päästä tietotekniikan, -järjestelmien ja ohjelmistojen muutoksista huolimatta.

7.7.6 Tietoaineiston käytöstä poisto ja hävittäminen

Tarpeettomaksi tulleiden tietoaineistojen hävittäminen koskee papereita, mikrofilmejä sekä sähköisiä, magneettisia ja optisia tietovälineitä. Näitä tietoaineistoja voi organisaatiossa olla arkistoissa, tallenteilla ja tietovarastoissa sekä sähköpostissa. Käytöstä poistosta ja hävittämisestä on VAHTI-ohje: Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje 2/2000.

Käyttäjälle tulee ohjeistaa tarpeettomaksi tulleen asiakirjan poistaminen käytöstä. Erityisesti on ohjeistettava salassa pidettävien asiakirjojen käytöstä poisto ja hävittäminen. Käyttäjän koulutuksessa on hyvä muistuttaa, että omalle organisaatiolle tarpeeton tietoaineisto saattaa kuitenkin ulkopuolisissa käsissä aiheuttaa merkittäviäkin tietoriskejä.

7.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvää turvallisuutta. Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet. Käyttöturvallisuuden tarkoituksena on huolehtia tietojärjestelmien luotettavasta toiminnasta. Käyttöturvallisuus koskee yksittäisiä työasemia, palvelimia, keskuslaitteita, tietoliikenneyhteyksiä, verkkoja ja näiden valvontaa.

Käyttöturvallisuuden perustana ovat toiminnan ja tietojärjestelmien käyttöohjeet. Kun käyttäjät tietävät, miten tietojärjestelmiä käytetään tai miten tulee toimia erilaisissa tietoturvallisuuteen vaikuttavissa tilanteissa, vähenevät virheellisestä toiminnasta ja huolimattomuudesta syntyvät ongelmat ja riskit huomattavasti.

Käyttöturvallisuuteen liittyy olennaisena osana myös käyttäjätunnuksien ja salasanojen sekä toimikorttien ja PIN-koodien käyttö ja hallinnointi. Tämän loppuraportin liitteenä 2 olevassa käyttäjän ohjeessa lähdetään siitä, että käyttäjätunnukset ja todentamisvälineet ovat henkilökohtaisia. Käyttäjiä tulee opettaa suhtautumaan niihin kuin omaan pankkikorttiin ja siihen liittyvään salasanaan. Henkilökohtaisten tunnusten lisäksi joissain organisaatiossa on käytössä yhteistunnuksia. Myös näiden käyttö tulee selkeästi ohjeistaa kaikille käyttäjille. Käyttäjille on hyvä tiedottaa, että käyttöoikeuksien saaminen perustuu työtehtäviin ja ne poistetaan heti, kun työtehtävä vaihtuu tai työsuhde päättyy.

Käyttöturvallisuus sisältää myös käytön seurannan ja valvonnan. Käyttäjille tulee selkeästi kertoa, mitä toimintaa organisaatiossa seurataan ja valvotaan ja mitä menetelmiä siihen käytetään. Käyttäjille täytyy myös kuvata heidän oma roolinsa valvonnassa. Tähän liittyy esimerkiksi tietoturvallisuuden loukkausten havainnointi ja niistä raportointi tai tietoturvasuojausten toimivuuden valvonta ja häiriöraportointi.

III KÄYTTÄJÄN OHJEIDEN JA KOULUTUKSEN JATKOKEHITTÄMINEN

8 KEHITYSESITYKSET

Seuraavassa esitetään valmisteluryhmän ehdotuksia käyttäjäohjeden ja -koulutuksen jatkokehittämisestä.

8.1 Yleiset kehitysesitykset

1. Tietoturvallisuus ja tietosuoja osaksi oppilaitosten opetussuunnitelmia

Tietoturvallisuus ja tietosuoja ovat erottamaton osa kaikkea tietojenkäsittelyä. Tietoturvatoimien toteutumiseen jokapäiväisessä työnteossa vaikuttaa paljon henkilön ymmärtämys aiheesta ja asennoituminen tietoturvallisuuteen. Tietoturvallisuus ja tietosuoja tulisi ottaa huomioon jo päiväkotien ja koulujen opetussuunnitelmissa osana tietojenkäsittelyn opetusta. Samalla tavoin tietoturvallisuuden opetus ja koulutus tulisi jatkua myös ylemmissä koulutusasteissa, jotta oppilaat ja opiskelijat mieltäisivät alusta lähtien tietojenkäsittelyn ja tietoturvallissuden liittyvän yhteen. Tähän on otettu kantaa myös kansallisessa tietoturvastrategiassa, jossa esitetään tietoturvallisuuteen liittyvän opetuksen sisällyttämistä kaikille kouluasteille.

8.2 Esitykset VAHTIlle

1. Ohjeiden katselmointi ja päivittäminen

Valtiovarainministeriö ja VAHTI julkaisevat ohjeita, joissa on helposti vanhenevaa asiaa, kuten esimerkiksi viittauksia lainkohtiin tai muihin VAHTI-ohjeisiin. Ehdotetaan, että ohjeita katselmoidaan ja päivitetään tasaisin väliajoin, jotta ohjeissa olevat tiedot pysyisivät ajantasaisina ja ohjeista olisi näiltä muuttuviltakin osin hyötyä organisaatioille myös pidemmän ajan kuluttua. Päivitykset ehdotetaan tehtäväksi VAHTIn www-sivuilla olevaan materiaaliin. Kirjalliseen materiaalin muutoksia ei ole tarpeen tehdä.

2. Ohjeiden ja menetelmien jakaminen julkishallinnon organisaatioiden välillä

Julkishallinnon organisaatioissa laaditaan paljon erilaisia tietoturvaohjeita, -menetelmiä ja -dokumentteja. Monista ohjeista voisi olla hyötyä muillekin organisaatioille joko sellaisenaan tai muokattuna. Ehdotetaankin, että VAHTI miettii tapaa, jolla ohjeita ja menetelmiä voidaan jakaa ja hyödyntää organisaatioiden välillä.

8.3 Esitykset ministeriöille

1. Ministeriöiden ja niiden hallinnonalan tietoturvaohjeet

Eri ministeriöt ovat eri tavoin ottaneet kantaa hallinnonalan tietoturvallisuuteen. Ehdotetaan, että ministeriöt laativat jatkossa omalle hallinnonalalleen yhteisiä tietoturvaohjeita ja suosituksia, mikäli ministeriöissä on tarvetta käyttää VAHTI-ohjeita tiukempia tietoturvaohjeita tai mikäli ministeriön alaisissa virastoissa on tarvetta soveltaa myös VAHTI-ohjeista poikkeavia ohjeita.

2. Ministeriöiden ja niiden hallinnonalan tietoturva- ja tietosuojayhteyshenkilö

Ehdotetaan, että ministeriöt nimeävät tietoturva- ja tietosuojayhteyshenkilön, joka pystyy ottamaan kantaa ministeriön ja sen hallinnonalan kuuluvien laitosten ja organisaatioiden tietoturvallisuuteen ja tietosuojaan. Yhteyshenkilön sijaan voidaan myös nimetä ministeriön tietoturva- ja tietosuojaryhmä, joka koostuu ministeriön ja sen hallinnonalan tietoturva-asiantuntijoista. Tarvittaessa tietoturvallisuudelle ja tietosuojalle voidaan nimetä omat yhteyshenkilönsä.

8.4 Esitykset julkishallinnon organisaatioille

1. Tietoturvallisuuden koulutussuunnitelman laatiminen ja toteuttaminen

Ehdotetaan, että organisaatiot laativat tietoturvallisuuden koulutussuunnitelman, joka sisältää sekä koulutettavat asiakokonaisuudet että koulutuksen kohderyhmät. Koulutussuunnitelman avulla pystytään ottamaan ajoissa huomioon tietoturvallisuuden kehitystarpeet ja erilaisista muutoksista syntyneet uudet koulutustarpeet. Koulutussuunnitelman avulla voidaan myös varmistua tietoturvallisuuden jatkuvuuden hallinnasta organisaatiossa sekä ajoissa kohdentaa koulutukselle tarvittavat resurssit.

Koulutussuunnitelman laatiminen sisältää ainakin seuraavat vaiheet:

- Organisaation tietoturvakehitystarpeiden kartoittaminen
- Henkilöstön osaamis- ja lähtötason kartoittaminen
- Koulutusten kohderyhmien valinta
- Koulutusaiheiden valinta
- Koulutusten organisointi (aika, paikka, kouluttajat, osallistujat)

- Koulutus- ja harjoitusaineiston laatimisen organisointi
- Koulutussuunnitelman ja sen tavoitteiden toteutumisen seuranta- ja arviointimenetelmistä päättäminen

2. Tietoturvallisuus osaksi henkilöstösuunnitelmaa

Ehdotetaan, että tietoturvallisuus otetaan organisaatioissa osaksi henkilöstösuunnitelmaa. Esimerkiksi henkilöstösuunnitelman ”Työympäristö ja työolot” –lukuun voidaan kirjata tietoturvallisuuteen liittyviä asioita. Lisäksi jos henkilöstösuunnitelmassa on otettu kantaa henkilöstön koulutukseen, voidaan siinä kohtaa tietoturvallisuus nostaa omana asianaan erikseen esiin.

3. Tietoturvallisuus osaksi toiminta- ja taloussuunnittelua

Ehdotetaan, että tietoturvallisuus otetaan osaksi organisaatioiden toiminta- ja taloussuunnittelua. Tällä tavoin pystytään varmistamaan tietoturvallisuuden kehittämiseen ja ylläpitoon tarvittavat taloudelliset resurssit kullekin vuodelle.

4. Kansallisen tietoturvastrategian huomioiminen organisaation toiminnassa

Kansallisesta tietoturvastrategia on hyväksytty 4.9.2003. Kansallinen tietoturvastrategia ei syrjäytä hallinnon tai muiden toimijoiden omia tietoturvalinjauksia, mutta toisaalta strategiassa ei myöskään käsitellä yhteiskunnan poikkeusoloihin ja julkishallinnon sisäiseen tietoturvallisuuteen liittyviä kysymyksiä. Julkishallinnon organisaatioiden tulee kuitenkin toteuttaa kansallista tietoturvastrategiaa, vaikka julkishallinnon sisäinen tietoturvallisuus on jätetty strategian ulkopuolelle.

5. Vastuuhenkilöiden yhteistyön varmistaminen organisaatiossa

Julkishallinnon organisaatioissa on tyypillisesti useita henkilöitä, joiden vastuulla on jokin tietoturvallisuuden osa-alue. Esimerkiksi valmiusvastuu, tietoturvavastuu, tietosuojavastuu ja turvallisuusvastuu ovat usein eri henkilöillä. Organisaation tulee mahdollistaa ja varmistaa näiden vastuuhenkilöiden välinen yhteistyö tietoturva- ja tietosuoja-asioissa.

8.5 Esitykset tietoturvakouluttajille

1. Koulutusmenetelmät

Ehdotetaan, että tietoturvallisuuden kouluttamisessa käytetään useampia menetelmiä. Näitä ovat esimerkiksi:

- Tietoturvaluento koko henkilökunnalle
- Kohdistetut tietoturvaluennot eri henkilöstöryhmille / yksiköille
- Sisäisten tietoturvakouluttajien koulutus (motivointi, asiasisältö, viestintä)

- Tärkeiden tukihenkilöiden koulutus (esim. helpdeskin tai atk-tuen koulutus)
- Tietoturvateemapäivät/-viikot
- Ulkopuolisten asiantuntijoiden käyttö luennoilla
- Itseopiskeluaineisto organisaation intranetiin
- Tiedottaminen sisäisissä palavereissa (esim. osastopalaverit)
- Tietoiskut (esim. tilaisuuksissa, neuvottelupäivillä, intranetin etusivulla, näytönsäästäjässä)
- ”Slogan” tietoturvatietoisuuden lanseerauksen helpottamiseksi
- Tietoturva-FAQ (*Frequently Asked Questions* – Usein esitetyt kysymykset)
- Tietoturvatietoa uuden työntekijän perehdytysaineistoon
- Leikkimielinen tietoturvatesti
- Tietoturvajulisteet
- Tietoturvatavara tai ”tietoturvalelu” (esim. hiirimatto)

2. Kohderyhmän mukaan kohdennettu koulutus

Ehdotetaan, että koulutukset suunnitellaan kohderyhmän mukaan. Kaikille tulee kouluttaa vähintään käyttäjän ohjeessa esitetyt perusasiat, mutta kohderyhmän mukaan koulutuksia voidaan muokata ja täydentää. Erityiskohderyhmiä ovat mm. organisaation tietoturvavastaavat, atk-henkilöstö ja johto.

3. Ohjeiden käyttöönottoon liittyvien koulutusten suunnittelu

Ehdotetaan, että koulutusvastaavat suunnittelevat yhdessä organisaation tietoturvaohjeista vastaavien henkilöiden kanssa toimintatavan, jonka avulla kaikki uudet ohjeet voidaan kouluttaa käyttäjille. Tällä tavoin käyttäjät perehdytetään ohjeisiin ja varmistutaan, että käyttäjät ovat tietoisia uudesta tietoturvaohjeesta.

8.6 Esitykset tietoturvaohjeista vastaaville

1. Ohjeiden jatkokehitys

Ohjeiden jatkokehityksestä on laadittu pohja, josta jokainen organisaatio voi muokata omat ohjeensa. Ehdotetaan, että organisaatiot jatkokehittävät sekä käyttäjän ohjetta että multimedia-aineistoa parhaiten omia tarpeitaan vastaaviksi.

2. Ohjeiden ylläpito ja päivitys

Ehdotetaan, että organisaatiot laativat toimintamallin ohjeiden ylläpitoon ja päivitykseen. Tällä varmistutaan, että ohjeet ovat ajantasalla ja vastaavat organisaation kulloistakin tilannetta.

LIITE 1 Lähdeluettelo

VAHTI:n suositukset ja VM:n ohjeet (www.vm.fi/vahti)

- Valtion tietohallinnon Internet-tietoturvallisuusohje
- Arkaluonteiset kansainväliset tietoaineistot
- Valtionhallinnon etätyön tietoturvallisuusohje (erityisesti Etätyöntekijälle-kappale)
- Toimet tietoturvaloukkaustilanteissa (Pikaohje)
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
- Valtion viranomaisen tietoturvallisuustyön yleisohje (erityisesti 4.3.13 Koulutus)
- Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje
- Valtionhallinnon tietoturvallisuuskäsitteistö
- Tarpeettomiksi tulleiden tietoaineistojen hävittämisohje
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje

Kirjallisuus

- Maija Kleemola, Raija Tervo-Pallikka: Tietosuoja, Suomen Atk-kustannus 1998
- Juha E. Miettinen: Tietoturvallisuuden johtaminen

  – näin suojaat yrityksesi toiminnan, Kauppakaari 1999
- Juha E. Miettinen: Yritysturvallisuuden käsikirja, Kauppakaari 2002
- Juhani Paavilainen: Tietoturva, Suomen Atk-kustannus 1998
- Arto Suominen: Riskienhallinta, WSOY 2003

Muita lähteitä

- Puolustustaloudellinen suunnittelukunta: Tietotekniikan turvallisuus ja toiminnan varmistaminen, Tietojärjestelmäjaoston ohje 1/2002, Helsinki 2002
- BS 7799-2:fi, 2002

LIITE 2 Valtiovarainministeriön ja VAHTIn tietoturvallisuusohjeistoa

- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003
- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän auditointi, VAHTI 3/2003
- Turvallisen etäkäytön arkkitehtuuri, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuuusohje, VAHTI 1/2003
- Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2003
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tunnistaminen valtionhallinnon verkkopalveluissa VM 6/01/2003
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, VM ja PTS, 2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvallisuustarkistuslista, VAHTI 6/2001 . Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmistoilta suojautumisen yleisohje, VAHTI 4/2000
- Tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtion tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000
- Tarpeettomien tietoaineistojen hävittämisohje, VM 19.4.2000
- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000

- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 5/01/2000
- Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 2/1997

.

VAHTI

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

6/2003

OPAS JULKISHALLINNON TIETOTURVAKOULUTUKSEN JÄRJESTÄMISESTÄ

ISSN 1455-2566
ISBN 951-804-407-4