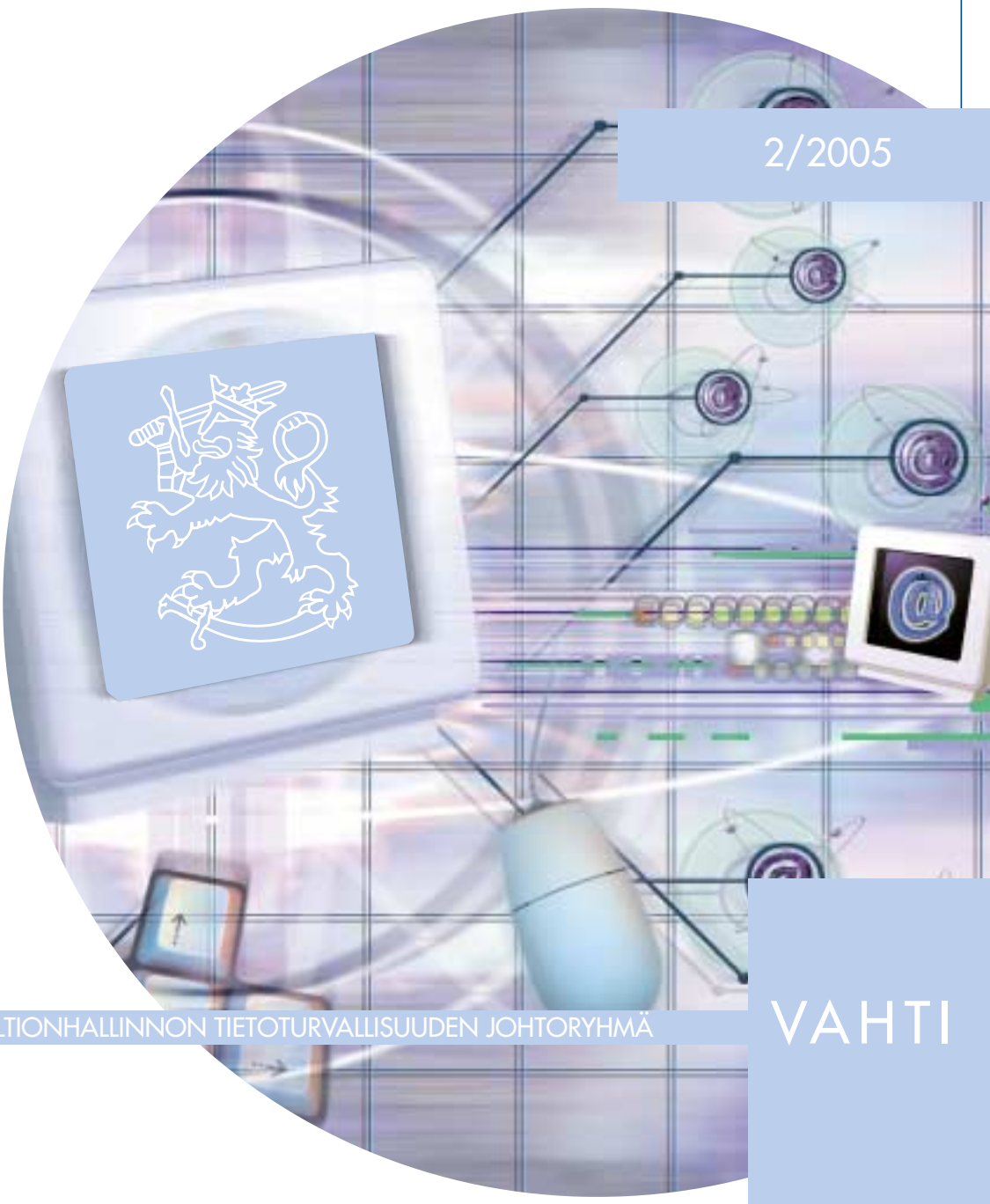
VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON SÄHKÖPOSTIEN KÄSITTELYOHJE



2/2005

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIONHALLINNON SÄHKÖPOSTIEN KÄSITTELYOHJE

2/2005

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A, Helsinki
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Vahtijulkaisut@vm.fi

ISSN1455-2566
ISBN 951-804-515-1
ISBN 951-804-516-X (pdf)

Edita Prima Oy
HELSINKI 2005

VALTIOVARAINMINISTERIÖ VM 10/01/2005

24.5.2005

Ministeriöille, virastoille ja laitoksille

VALTIONHALLINNON SÄHKÖPOSTIEN KÄSITTELYOHJE

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta.

Ohjeessa käsitellään sähköpostin erityiskysymyksiä tietoturvallisuuden kannalta. Ohje korvaa ohjeen Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001.

Ohjeen suositukset on tarkoitettu organisaation sähköpostipolitiikan perusteiksi sekä käytännön toiminnan ja sen ohjeistuksen pohjaksi.

Ohjeessa käsiteltyjen kysymysten kannalta keskeistä lainsäädäntöä ovat laki yksityisyyden suojasta työelämässä (759/2004) sekä sähköisen viestinnän tietosuojalaki (516/2004).

Asiakirja tulee valtion tietoturvallisuuden johtoryhmän Internet-sivuille, jotka ovat osoitteissa www.vm.fi/vahti. Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat erityisasiantuntija Olli-Pekka Rissanen (etunimi.sukunimi@vm.fi) sekä neuvotteleva virkamies Mikael Kiviniemi (etunimi.sukunimi@vm.fi)

Toinen valtiovarainministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Valtionhallinnon sähköpostien käsittelyohje (VAHTI 2/2005)

JOHDON TIIVISTELMÄ

Ohje on ensisijaisesti suunnattu ministeriöille, valtion virastoille ja laitoksille, mutta se on sovellettavissa muissakin organisaatioissa. Suositukset on tarkoitettu sähköpostipolitiikan perusteiksi ja käytännön toimintaohjeistuksen pohjaksi. Ohjeessa on keskitytty käsittelemään valtion työnantajan ja työntekijän välistä suhdetta. Työntekijällä tarkoitetaan viranomaisen palveluksessa olevaa palvelussuhteen laadusta riippumatta.

Tarkasteltu lähtökohtana on ollut asiaan välittömästi liittyvä, voimassa oleva lainsäädäntö.

Suomen perustuslaissa on säännelty yksityiselämän suojaa, sananvapautta ja julkisuutta. Rikoslaissa on säädelty rangaistavaksi viestintäsalaisuuden loukkauksena toisten viesteihin puuttuminen. Henkilötietolaki (523/1999) säätelee henkilötietojen käsittelyä. Henkilötiedolla tarkoitetaan kaikenlaista luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään koskevaksi. Laki viranomaisten toiminnan julkisuudesta määrittelee muun muassa viranomaisen asiakirjan.

Laissa yksityisyyden suojasta työelämässä (759/2004) on annettu hyvin selkeät säännökset esimerkiksi sähköpostin lukemisesta työntekijän ollessa estynyt. Lakiin on syytä tutustua kokonaisuudessaan. Samoin sähköisen viestinnän tietosuojalaki (516/2004) sisältää niin keskeisiä säännöksiä, että siihen olisi syytä tutustua kokonaisuudessaan; sähköpostin kannalta keskeisimpiä ovat luvut 1-3 ja 5.

Lain tasoisten säännösten lisäksi sähköpostia käsittelyä koskevia ohjeita on annettu ministeriöiden toimesta. Esimerkiksi Valtionhallinnon tietoturvallisuuden johtoryhmän www-sivuilta (www.vm.fi/vahti) on löydettävissä voimassa olevat VM:n antamat julkiset ohjeet ja suositukset.

Lainsäädännöstä ja suosituksista huolimatta vallitseva tilanne ei ole ongelmaton. Kunkin organisaation ratkaistavaksi jää esimerkiksi:

– millaiseen organisaation ulkoiseen tai sisäiseen viestintään ja mihin palveluihin virkasähköpostia sallitaan käytettävän

– rajoitetaanko tai salataanko viestintää jollain tavalla
– sallitaanko sähköpostin käyttö työntekijän omiin yksityisiin viesteihin
– miten menetellään viestien sisällön suhteen henkilön ollessa poissa tilapäisesti tai pysyvästi

Suosituksena esitetään muun muassa sähköpostikäyttöpolitiikan luomista ja käytön ohjeistamista. Vaitiolovelvollisuutta ja hyväksikäyttökieltoa on syytä korostaa. Sähköpostin käyttöä tulee valmistella yhteistyössä henkilöstön kanssa ja sovellettavista menettelyistä tulee tiedottaa. Suositellaan käytettäviksi mahdollisimman paljon organisaatio-osoitteita (kirjaamo@organisaatio.fi) ja henkilökohtaisten sähköpostiosoitteiden käytön rajaamista tiettyihin toimintoihin.

Erityiskysymyksenä kannattaa huomioida niin sanottu roskaposti. Organisaation velvollisuutena on suodattaa sähköpostit, koska roskapostin osuus liikenteestä on kohonnut jopa 90 prosenttiin. Sähköpostia käytetään myös haittaohjelmien levittämiseen ja rikollisiin tarkoituksiin kuten huijauksiin. Se muodostaa näin ollen merkittävän tietoturvauhan.

Liitteinä ovat mallit sähköpostin suodatusohjeesta, salassapitositoumuksesta, luottamuksellisuusilmoituksesta ja suostumuksesta sähköpostiviestien lukemiseen.

Sisällysluettelo

1 JOHDANTO

1.1 Ohjeen tarkoitus

Tämä on ministeriöille, valtion virastoille ja laitoksille sähköpostin käsittelyä varten tehty ohje. Ohje on sovellettavissa myös kunnissa, koska niitä koskee sama lainsäädäntö. Suositukset on tarkoitettu sähköpostipolitiikan luonnin perusteiksi ja järjestelmävastuu-henkilöille sekä heidän esimiehilleen käytännön toimintaohjeistuksen pohjaksi.

Ohje on rajattu käsittelemään työnantajan ja työntekijän välistä suhdetta sähköpostin käsittelyssä. Ohjeessa tarkoitetaan työntekijällä viranomaisen palveluksessa olevaa palvelussuhteen laadusta riippumatta. Ohjeistus koskee siten myös sekä vuokratyövoimaa että muita tilapäisiä työntekijöitä kuten harjoittelijoita. Ohjeessa kerrotut laissa säädetyt vaitiolovelvollisuutta ja hyväksikäyttöä koskevat säännökset koskevat myös viranomaisen toimeksiannon saajan palveluksessa olevia.

Ohjeistus koskee sekä organisaation sisäistä että ulkoista viestintää. Viestinnän luottamuksellisuus ei ole riippuvainen käytettävästä tekniikasta, viestinnän osapuolten fyysisestä sijainnista tai siitä, että virasto on ulkoistanut sähköpostijärjestelmänsä.

Arkistolaitos antaa ohjeita sähköpostiviestien kirjaamisesta tai muusta rekisteröinnistä sekä niiden arkistoinnista (http//www.narc.fi).

1.2 Sähköpostiviestien luokittelu

Sähköpostiviestit on tässä ohjeessa jaettu neljään eri luokkaan sen mukaisesti millaiseen osoitteeseen ne liittyvät. Ohjeessa sekä lähetetyt että vastaanotetut viestit määritellään seuraavasti:

– **organisaation sähköpostiviesti** on organisaation organisaatio-osoitteeseen (esim. kirjaamo@organisaatio.fi) liittyvä viesti. Julkisuus määräytyy julkisuuslain tai erityislain mukaan.

– **virkasähköpostiviesti** liittyy sekä organisaation työntekijälle työkäyttöön antamaan henkilökohtaiseen virkasähköpostiosoitteeseen (esim. vili.virta@organisaatio.fi) että työntekijän työtehtäviin. Julkisuus määräytyy julkisuuslain tai erityislain mukaan.
– **henkilökohtainen sähköpostiviesti** on organisaation antamaan sähköpostiosoitteeseen (yleensä sama kuin virkasähköpostiosoite) liittyvä henkilökohtainen viesti. Julkisuuslain ulkopuolelle jäävä. Sähköisen viestinnän tietosuojalaki.
– **muu sähköpostiviesti** on käyttäjän organisaation ulkopuoliseen sähköpostiosoitteeseen esim. vili.virta@omakaytto.fi tai vili.virta@muuorganisaatio.fi) liittyvä viesti. Sähköisen viestinnän tietosuojalaki

Sähköpostiviestiin sisältyvät myös sen liitteet.

Virkasähköpostiosoite ja henkilökohtainen sähköpostiosoite on yleensä sama sähköpostiosoite. Tästä ohjeessa käytetään näistä osoitteista nimeä virkasähköpostiosoite. Tähän osoitteeseen tulevat viestit jakautuvat työtehtäviin liittyviin virkasähköpostiviesteihin ja työntekijän henkilökohtaisiin sähköpostiviesteihin. Laki yksityisyyden suojasta työelämässä koskee näitä sähköpostiosoitteita. Se ei koske organisaatio-osoitteita.

Ohjeessa käsitellään yksityistä sähköpostiosoitetta ja yksityisiä sähköpostiviestejä, koska työntekijällä on työnantajan niin salliessa mahdollisuus käyttää esimerkiksi www-selaimella yksityiskäyttöön hankkimaansa sähköpostiosoitetta. Viestit eivät tällöin kulje organisaation sähköpostireitityksen kautta, vaan www-liikenteenä, josta jää merkintöjä organisaation lokitietoihin.

2 KÄYTÄNNÖN TILANTEISTA JA RATKAISUOHJEISTA

2.1 Nykytilanteen kuvaus

Sähköpostin käytössä on kyse työnantajan omistaman tai vuokraaman laitteiston ja tietoliikenneyhteyksien käytöstä. Järjestelmän käytöstä aiheutuu työnantajalle kustannuksia, mutta erityisesti on kyse työajan käytöstä. Sähköpostijärjestelmien keskeisiä elementtejä ovat itse viestien ja tietoliikenneyhteyksien lisäksi tietokoneissa olevat hakemistot ja lokit sekä niitä eri vaiheissa käsittelevät henkilöt.

Sähköisen viestinnän tietosuojalaissa (516/2004) on määritelty yhteisötilaajan velvollisuudet. Julkisen sektorin organisaatiot ovat lain tarkoittamia yhteisötilaajia. On huomattava, että 3.3 §:n mukaan lain 4 (Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuus) ja 5 §:iä (Vaitiolovelvollisuus ja hyväksikäyttökielto) sovelletaan myös sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, vaikka näitä verkkoja ei ole liitetty 1 momentissa tarkoitettuun yleiseen viestintäverkkoon.

Kyseistä lakia ei sovelleta (3.7 §:) viranomaistoimintaan viestintämarkkinalaissa tarkoitetussa viranomaisverkossa tai muussa yleiseen järjestykseen ja turvallisuuteen, maanpuolustukseen, pelastustehtäviin, väestönsuojeluun tai maaliikenteen, meriliikenteen, raideliikenteen taikka ilmaliikenteen turvallisuuteen liittyvien tarpeiden vuoksi rakennetussa viestintäverkossa.

Työnantajat antavat henkilöstönsä käytettäväksi sähköpostin ja tietoliikenneyhteyden, joita käytettäessä tallentuu tietoja työnantajan omille tai ulkoistetuille palvelimille. Sähköpostin ja yhteyksien käyttöön liittyvien tietojen keräämiseen liittyy monenlaisia tarpeita. Lokitietoa syntyy muun muassa sähköpostijärjestelmissä, palomuureissa, palvelimiin kirjautumisista sekä tietokantojen ja tietojärjestelmien käytöstä. Proxyt eli www-sivuja välittävät ja varastoivat palvelimet keräävät tietoja siitä, miten käyttäjät selaavat verkkoa. Myös www-palvelimet keräävät lokia haetuista sivuista. Lokeja kerätään muun muassa:

– järjestelmän ja sen käyttäjän ongelmien selvittämiseksi
– järjestelmän toiminnan valvomiseksi ja ongelmia ennalta ehkäisevän toiminnan tukemiseksi
– organisaation tietoturvallisuuden valvomiseksi
– organisaation sisäisten ja ulkoisten väärinkäytösten ja häiriköinnin selvittämiseksi
– laskutustietojen keräämiseksi
– järjestelmän kehittämiseksi
- kapasiteettimittauksia varten
– tilastointia

Lokit ovat lain yksityisyyden suojasta työelämässä 21 §:ssä säädeltyä teknisin menetelmin toteutettua valvontaa. Niiden käsittelyn periaatteista tulee sopia yhteistoimintamenettelyssä.

Työntekijät ja viestien lähettäjät käyttävät yleisesti sähköpostia muuhunkin kuin työasioihin liittyvään viestintään. Käytännössä esiintyy ongelmia, koska sähköpostin käytöstä yksityisiin tarkoituksiin ei ole sovittu tai sitä ei ole ohjeistettu.

Sähköpostiviestit voivat olla osoitettuja väärälle henkilölle, lähetetty väärän henkilön nimissä ja viesti voi harhautua virheellisen osoitteen tai sähköpostijärjestelmissä olevan virheen johdosta. Tällöin myös joku muu kuin se, jolle viesti oli tarkoitettu, saattaa nähdä viestin sisällön.

Ongelmia aiheutuu myös työntekijän poistumisesta työnantajan palveluksesta, epätietoisuudesta vaitiolovelvollisuuden ja hyväksikäyttökiellon merkityksestä sekä haittaohjelmien leviämisestä sähköpostiviestien mukana. Roskapostien suodattaminen on välttämättömyys ja velvollisuus sähköpostijärjestelmän toiminnan turvaamiseksi. Niiden suodattamisesta on syytä informoida henkilökuntaa YT-menettelyn kautta.

Sähköpostin salaaminen yleistyy. Salattujen viestien avaaminen onnistuu yleensä vain vastaanottajan salaisella avaimella. Työntekijän poistuttua palveluksesta tällaisia viestejä ei voida avata. Salauksen käyttö tulee selkeästi ohjeistaa esimerkiksi määräämällä, että salatut sähköpostit tulee avata, kun ne on vastaanotettu.

2.2 Organisaatio- ja virkasähköpostin käyttö

Työnantajan tulee antaa työntekijälle selkeät ohjeet sähköpostin käytöstä. Ohjeistusta tulee valmistella yhteistyössä henkilöstön tai heidän edustajiensa kanssa. Organisaatiosähköpostia saa käyttää vain viranomaistehtävissä ja virkasähköpostia viranomaistehtävien ohella vain työnantajan antamien ohjeiden mukaisesti. Työnantajan on huolehdittava, että työntekijälle saapuneen sähköpostiviestin käsittely on etukäteen ohjeistettu ja että käsittelyssä otetaan huomioon lainsäädännön vaatimukset.

Ohjeistusta laadittaessa tulee huomioida ainakin seuraavia asioita:

- millaiseen viestintään ja mitä palveluita sähköpostiosoitteella sallitaan käytettävän
- turvaluokittelusta ja sen mukaisesta käsittelystä annetut ohjeet
- millaisia rajoituksia viestintään mahdollisesti liittyy
- etäkäyttö
- käyttöön liittyvät riskit
- haittaohjelmatarkistuksen järjestäminen
- rajoitetaanko liitetiedostojen kokoa ja käyttöä
- saako työntekijä ilmoittaa työkäyttöön tarkoitetun sähköpostiosoitteen jakelulistoille
- salauksen tarve ja menetelmät
- varmistetaan, että järjestelmän ylläpitohenkilökunta ja sen käyttäjät tuntevat sähköpostiviesteistä säädetyn vaitiolovelvollisuuden ja hyväksikäyttökiellon
- viestinnän valvonnan lainmukaisuus
- sähköpostiviestien kirjaaminen tai rekisteröinti sekä niiden arkistointi
- osoitteiden jakelu eri tahoille
- osoitteiden käyttö poliittiseen tai yritystoimintaan
- saako virkasähköpostiosoitetta käyttää kuluttajapalveluihin

Organisaation ohjeessa on syytä ottaa kantaa myös luottamusmiesten, työsuojeluvaltuutetun ja muiden mahdollisten henkilöstön edustajien oikeuteen käyttää virkasähköpostiosoitetta tätä tehtäväänsä hoitaessaan. Valtion virka- ja työehtosopimuksen mukaan luottamusmies ja työsuojeluvaltuutettu voivat käyttää tehtäviensä suorittamisessa viraston tavanomaisessa käytössä olevia viestintä- ja toimistovälineitä. On tärkeää huomata, etteivät luottamushenkilöiden viestit ole julkisuuslain (vrt. 5.3 § 1 kohta) tarkoittamia asiakirjoja.

Sähköpostitse saapuneet, *julkisuuslain 5 §:n mukaiset viranomaisen* asiakirjat on kirjattava tai niiden saapuminen on muulla luotettavalla tavalla rekisteröitävä. Lisäksi virkasähköpostiviestien osalta on muistutettava henkilöstöä julkisuuslain 23 §:n mukaisesta viranomaisten asiakirjoihin liittyvästä vaitiolovelvollisuudesta ja hyväksikäyttökiellosta.

2.3 Henkilökohtaisen ja yksityisen sähköpostin käyttö

Työnantajan tulee antaa työntekijälle selkeät ohjeet sähköpostin käytöstä. Ohjeet on valmisteltava yhteistyössä henkilöstön tai heidän edustajiensa kanssa. Työntekijöille on oltava selvää, sallitaanko työnantajan järjestelmillä henkilökohtainen viestintä. Ohjeistukseen vaikuttaa työnantajan toimiala, työntekijän tehtävät, viestinnän ja välitettävien viestien laatu, virustorjunta, henkilöstön valvonnan sekä väärinkäytösten estämisen tarpeet.

Työnantajan tulee ratkaista, sallitaanko työnantajasta riippumattomien yksityisten sähköpostiosoitteiden käyttö työpaikalta. Virkasähköposteja ei saa edelleen ohjata tällaiseen osoitteeseen eikä virka-asioita saa hoitaa näillä osoitteilla.

Jos työnantaja sallii virkasähköpostiosoitteen käyttämisen henkilökohtaiseen viestintään tai omien sähköpostiosoitteiden käytön, ohjeistusta laadittaessa tulee huomioida ainakin seuraavia asioita:

- millaiseen viestintään ja mitä palveluita sallitaan käytettävän
- millaisia rajoituksia viestintään mahdollisesti liittyy
- käyttöön liittyvät riskit
- haittaohjelmatarkistuksen järjestäminen
- rajoitetaanko liitetiedostojen kokoa ja käyttöä
- sallitaanko jakelu- ja postituslistojen luominen työnantajan laitteisiin
- sallitaanko osoitetietojen ilmaiseminen ulkopuolisille jakelu- ja postituslistoille
- sallitaanko työntekijälle salauksen käyttö
- saako työntekijä ilmoittaa työkäyttöön tarkoitetun sähköpostiosoitteen jakelulistoille
- saako työntekijä antaa sähköpostiosoitteensa työtehtäviin liittymättömille www-sivuille
- varmistetaan, että järjestelmän ylläpitohenkilökunta ja sen käyttäjät tuntevat henkilökohtaisista sähköpostiviesteistä säädetyn vaitiolovelvollisuuden ja hyväksikäyttökiellon.

Työnantajalla ei ole oikeutta hankkia tietoa yksityisten viestien sisällöstä, on työnantaja sallinut työntekijälle virkasähköpostin ja –osoitteen henkilökohtaisen käytön tai ei.

2.4. Sähköpostin käsittely erityistilanteissa

Automaattisten vastausten käyttöä tulee tarkoin harkita. Siihen liittyy riskejä, mutta se palvelee organisaation asiakkaita sekä muita työntekijöitä. Automaattivastausten jakelu voidaan harkinnan mukaan rajoittaa vain omaan organisaatioon. Jos automaattivastaus katsotaan välttämättömäksi (esimerkiksi työntekijöiden pitkät lomat tai virkavapaudet tai palvelussuhteen päättyminen), tulee siinä kehottaa lähettäjää ottamaan yhteyttä ensisijaisesti sopivaan organisaatio-osoitteeseen.

Henkilön käyttöoikeus työnantajan antamaan sähköpostiosoitteeseen päättyy palvelussuhteen päättyessä. Käyttöoikeuden päättymisen jälkeen työantaja ei ota vastaan eikä lähetä eteenpäin henkilölle lähetettyjä viestejä vaan ilmoittaa automaattisesti lähettäjälle osoitteen toimimattomuudesta. Ennen palvelussuhteen päättymistä työntekijän tulee ilmoittaa viestintäkumppaneilleen sähköpostiosoitteensa poistumisesta ja poistaa henkilökohtaiset viestinsä. Jos työntekijä lakkaa hoitamasta tehtäviään jo ennen työsuhteen päättymistä, tulee sähköpostin vastaanotto estää jo siinä vaiheessa.

Sähköposti viestien käsittelystä kuoleman tapauksissa ei ole vielä ennakkotapauksia ja lain tulkinta on monilta osin ristiriitainen esimerkiksi perikunnan oikeudesta yksityisiin sähköposteihin työnantajan postijärjestelmissä. Oikeudet viesteihin eivät siirry perikunnalle ja yksityisyyden suoja on edelleen voimassa. Kukin tapaus on syytä käsitellä huolella ja yksityisviestien osalta yhteistyöhön perikunnan kanssa pyrkien. Työnantajalla on oikeus työntekijän työhön liittyviin viesteihin. Tässäkin tilanteessa etukäteisohjeistuksella ja organisaatio-osoitteiden käytöllä voidaan helpottaa selvitystyötä.

2.5 Sähköpostiosoitteet henkilörekistereinä

Luonnollisen henkilön sähköpostiosoite on henkilötietolain mukainen henkilötieto. Sähköpostijärjestelmä muodostaa lain tarkoittaman henkilörekisterin, josta tulee laatia rekisteriseloste. Henkilötietolain perustelujen mukaan, jos automaattisen tietojenkäsittelyn avulla laadittu asiakirja (vrt. julkisuuslain 5.1 §; asiakirja voi olla henkilörekisteri) on tarkoitettu säilytettäväksi pysyvämmin sähköisessä muodossa osana tietojenkäsittelyjärjestelmää, se on henkilörekisteri tai osa loogista rekisteriä (rekisterin osien eli henkilötietojen fyysisestä muodosta tai sijainnista huolimatta käsittelyn tarkoituksen kannalta yhteenkuuluvat merkinnät kuuluvat loogiseen kokonaisuuteen).

Yksittäisen sähköpostin käyttäjän ei kuitenkaan tarvitse laatia sähköpostin jakelulistasta rekisteriselostetta, kun kyse on työnantajan sallimasta yksityisestä käytöstä (vrt. henkilötieto-lain 2.3 §) tai kyse on tilapäisenä pidettävästä osoitteistosta. Organisaation sisäisestä jakelulistastakaan ei rekisteriselostetta erikseen tarvitse tehdä. Sen sijaan itse sähköpostijärjestelmästä rekisteriseloste tulee laatia.

Henkilörekisteri muodostuu myös lokitiedostojen osalta, jos ne sisältävät tunnistettavaa henkilöä koskevia merkintöjä. Lokit - kuten myös sähköpostiviestit sinänsä - voivat sisältää henkilötietolain 11 §:n mukaisia arkaluonteisia henkilötietoja - kuten esimerkiksi henkilön yhteiskunnallista, poliittista ja uskonnollista vakaumusta, ammattiyhdistykseen kuulumista sekä sairautta, terveydentilaa ja hoitotoimenpiteitä kuvaavia tai kuvaamaan tarkoitettuja henkilötietoja - ja ovat usein helposti luettavissa. Järjestelmävastaavien vaitiolovelvollisuuden tuntemus on siten korostetun tärkeä. Sähköisen viestinnän tietosuojalaissa on myös säädelty lokitietojen käsittelyä.

Kaikkien henkilötietojen käsittely tulee suunnitella henkilötietolain 6 §:n mukaisesti eli muun muassa määritellä henkilötietojen käsittelyn tarkoitus. Henkilötietojen käsittelylle määritellyn tarkoituksen tulee kuvata totuudenmukaisesti sitä tarkoitusta, miksi henkilötietoja käsitellään.

Henkilötietolain 24 §:ssä on säädetty työnantajaa velvoittavasta tiedottamisvaatimuksesta. Muun muassa henkilötietojen käsittelyn tarkoitus tulee 24 §:n mukaisesti kertoa henkilöstölle, ellei säännöksen 2 momentissa säädettyä poikkeusperustetta ole olemassa. Poikkeus-perusteita ovat muun muassa se, että henkilö on jo saanut työnantajan informaa-

tio-velvollisuuden piiriin kuuluvat tiedot; poikkeaminen on välttämätöntä muun muassa valtion turvallisuuden, puolustuksen tai yleisen turvallisuuden ja turvallisuuden vuoksi sekä rikosten ehkäisemiseksi tai selvittämiseksi.

Säädetty informointivelvoite velvoittaa työnantajaa myös siinä tapauksessa, että verkon hallinnointi on ulkoistettu toimeksiannon saaneen suoritettavaksi. Informointivelvoite merkitsee työntekijän kannalta tiedonsaantioikeutta. Myös lainmukaisesti laaditusta rekisteriselosteesta ilmenee informointivelvoitteen sisältö: tieto rekisterinpitäjästä, henkilötietojen käsittelyn tarkoitus, henkilötietojen säännönmukainen luovutus ja tiedot, jotka ovat tarpeen henkilön oikeuksien käyttämiseksi eli muun muassa tieto siitä kenen puoleen kääntyä, jos haluaa käyttää tarkastusoikeuttaan. Työnantajan tulee aktiivisesti tiedottaa henkilöstölleen sähköpostin käytön yhteydessä kerättävistä tiedoista. Tiedottaminen edistää väärinkäytösten ennaltaehkäisyä.

Julkisuuslain 16 §:n 3 momentin perusteella henkilötietoja saa henkilörekisteristä luovuttaa suoramarkkinointiin ja mielipide- sekä markkinatutkimuksiin vain asianomaisen työntekijän ja viestin lähettäjän suostumuksella.

2.6 Ylläpitäjän velvollisuuksista

Seuraavassa esitettävä koskee sekä työnantajan ylläpitämää että ulkoistettua palvelua. Järjestelmien ylläpitohenkilöstö on keskeisessä asemassa paitsi tietojärjestelmien toimivuuden myös niihin liittyvän luottamuksellisuuden ja turvallisuuden toteuttamisessa.

Sähköpostijärjestelmän ylläpidon ja siinä ilmenevien virhetilanteiden vuoksi ylläpitäjät voivat saada tietoonsa lokitietoina lähettäjä- ja vastaanottajatietoja sekä viestien sisältöjä hakiessaan esim. syytä siihen, miksi käyttäjän lähettämä viesti ei ole mennyt perille. Lokeissa näkyy aikaleimoja, lähettäjän ja vastaanottajan osoite ja mahdollisesti viestin otsikko tai osa siitä.

Työnantaja määrää, mitä ylläpitäjien tehtäviin kuuluu. Sähköpostijärjestelmän seurantaa tarvitaan, jotta esimerkiksi järjestelmä ei ylikuormitu, tietoliikenne toimii ja tapahtumien määrä pysyy ennalta suunnitellussa.

On rajattava tarkasti ja suppeasti valvontaan oikeutetut henkilöt sekä ilmaistava kenelle ja mitä käyttötarkoitusta varten he valvonnan yhteydessä kertyneitä tietoja antavat. Jos valvonta on ulkoistettu toimeksiannon saaneen palveluksessa olevien henkilöiden tehtäväksi, käyttäjien tulee tietää siitä.

Ylläpitäjien on tunnettava tässä ohjeessa kerrotut vaitiolovelvollisuutta ja hyväksikäyttökieltoa koskevat säännökset.

2.7 Työnantajan oikeudet sähköpostiviestien lukemiseen (laki yksityisyyden suojasta työelämässä (759/2004)

Laissa yksityisyyden suojasta työelämässä on säädetty tarkkarajaisesti siitä, millä edellytyksin työnantajalle kuuluvien sähköpostiviestien hakeminen ja avaaminen on mahdollista. Ensimmäinen edellytys on lain 18 §:ssä säädettyjen työnantajan huolehtimisvelvollisuuksien toteuttaminen sähköpostiviestintää suunniteltaessa ja järjestettäessä. Säännöksen 1 momentissa tarkoitettujen sähköpostiviestien esille hakemisen tai avaamisen edellytyksenä on lisäksi, mitä 19 §:ssä ja 20 §:ssä säädetään. Viraston johdon on toteutettava 18 §:ssä säädetyt huolehtimisvelvollisuudet.

2.8 Sähköpostin suodattaminen

Roskapostista on muodostunut yhä paheneva ongelma. Sen määrä on saattanut olla jopa 90 prosenttia kaikesta sähköpostiliikenteestä. Käsite roskaposti ei ole yksikäsitteinen, mutta tässä sillä tarkoitetaan viestejä, jotka sisältävät ei-toivottua markkinointimateriaalia, haittaohjelmia tai muuta haitallista materiaalia. Organisaatiolla on oikeus, mutta myös velvollisuus suodattaa roskapostit (516/2004, 19§). Organisaation tulee huolehtia viestinnän esteettömyydestä. Mikäli roskapostia ei suodateta, on koko viestintäjärjestelmä vaarassa jo roskapostin suuren määrän vuoksi. Se muodostaa suuren tietoturvariskin, koska sähköpostiviestit ovat yhä enenevässä määrin keino levittää erilaisia haittaohjelmia. Niitä käytetään paljon myös rikolliseen toimintaan kuten huijauksiin.

Sähköpostin suodattamisessa on useita vaihtoehtoja. Viestejä, jotka eivät noudata sähköviestistandardeja, ei oteta vastaan. Sähköpostiviestinnän tekniset standardit on määritelty Internetin RFC menettelyin. Viestit, joissa on esimerkiksi väärä osoite tai tuntematon vastaanottaja, luokitellaan roskapostiksi. Yksi vaihtoehto on, että epäilyttävät sähköpostit siirretään karanteeniin, josta käyttäjät voivat lukea niitä mikäli katsovat sen aiheelliseksi.

Liitteenä 1 on ohje sähköpostin suodattamisesta.

3 SUOSITUKSET

Sähköisten asiakirjojen käsittely perustuu kirjesalaisuuden, yksityisyyden suojan ja hyvän hallintomenettelyn periaatteisiin samalla tavalla kuin muussakin virallisten asioiden hoidossa.

3.1 Sähköpostin ja sen lokitietojen käytön ohjeistaminen ja tiedottaminen

- Työnantajan on yhteistyössä henkilöstön kanssa laadittava selkeät säännöt sähköpostin ja lokitietojen käytöstä (sähköisen viestinnän käyttöpolitiikka)
- Käyttöpolitiikan tulee käsitellä muun muassa seuraavia asioita sähköpostien käytöstä ja sähköpostijärjestelmien hallinnasta:
  - viranomaisen virallisen sähköpostiosoitteen määrittely
  - viestinnän luottamuksellisuus, eheys, käytettävyys
  - yksityiskäyttö, henkilökohtainen käyttö, virkakäyttö
  - menettelyt työntekijän poissaolojen aikana ja palvelussuhteen päättyessä
- Käyttöpolitiikka on saatettava koko henkilökunnan tietoon
- Työntekijän on omalta osaltaan sähköpostin käsittelyssä huolehdittava virkavelvoitteistaan
- Tunnistamistiedoista (sähköpostiosoitteisto) on laadittava henkilörekisteriseloste, josta on ilmettävä muun muassa henkilötietojen käsittelyn tarkoitus
- Tunnistamistietojen käsittelyn tarkoituksesta on tiedotettava henkilökunnalle
- Henkilöstön ja toimeksiannon saajan tietoon on saatettava heitä koskevat vaitiolovelvollisuudet ja hyväksikäyttökiellot
- Työnantajan tulee ratkaista, kuinka luotettavasti viestinnän osapuolet on tunnistettava ja harkita esimerkiksi sähköisen allekirjoituksen käyttöönottoa

Liitteenä 2 on malli sähköpostin käyttöpolitiikasta.

3.2 Sähköpostin käytön valvonta

- Valvonnalla ei saa perusteettomasti loukata käyttäjien ja viestien käsittelemien henkilöiden yksityisyyttä esimerkiksi lukemalla henkilökohtaisia sähköposteja
- On huomattava, että mahdollinen sähköpostiin kohdistuva valvonta kohdistuu käytännössä sekä viestin lähettäjään että sen vastaanottajaan; valvonnalla ei saa oikeudettomasti loukata heidän yksityisyyttään
- Käyttäjille on kerrottava valvotaanko heitä, milloin, miten ja millä perusteilla; heille on kerrottava henkilötietolain 24 §:ssä kerrotut tiedot, ellei poikkeusperustetta ole (mm. rikosten selvittäminen)
- Työnantajalla on oikeus määrätä, mihin sähköpostia käytetään
- Käyttöoikeuksia voidaan rajoittaa puhelinsoiton estojen tapaan
- Kustannusten jakamiseen liittyvän tiedon käsittelyyn sovelletaan puhelinlaskutuksen periaatteita; tulosteissa viestinnän osapuolet tulee tehdä tunnistamattomiksi
- Liiallista valvontaa tulee välttää, koska se saattaa heikentää henkilöstön luottamusta työnantajaansa kohtaan ja kääntyy helposti samalla työnantajaa vastaan

3.3 Sähköpostin käytöstä seuraavien lokitietojen kerääminen ja säilyttäminen

- Lokitietoja ei saa käyttää profiiliyhteenvetojen tms. tekemiseen
- Lokitietoja saa käyttää vaitiolovelvollisen ylläpitohenkilöstön teknisluontoisiin tehtäviin sekä muihin sähköisen viestinnän tietosuojalain sallimiin tarkoituksiin (esim. laskutukseen ja tilastointiin verrattavaa yhteenvetoa, joissa ei näy yksityiskohtaista käyttöä)
- Kustannusten jakamiseen liittyvän tiedon käsittelyyn sovelletaan puhelinlaskutuksen periaatteita; tulosteissa viestinnän osapuolet tulee tehdä tunnistamattomiksi
- Työnantajan on määriteltävä lokitietojen säilytysaika ja –paikka
- Ohjelmisto- ja laitetoimittajalta tulee pyytää selvitys siitä, mitä lokitiedostoihin tallentuvat merkinnät kuvaavat ja voidaanko ne yhdistää tiettyyn henkilöön
- Tietosuojavaltuutettu on antanut 10.2.2003 erillisen Asiaa tietosuojasta 1/2003 -ohjeen lokitietojen käsittelystä, joka löytyy www.tietosuoja.fi/18069.htm -sivulta

3.4 Ylläpitohenkilökunta

- Sähköpostijärjestelmällä tulee olla nimetty vastuuhenkilö tai –henkilöt
- Postipalvelimen tulee olla suojattu ja sen ylläpitäminen tapahtua siten, että niin käytettävyys kuin myös luottamuksellisuus säilyvät

- Ylläpitohenkilökuntaan kuuluvat henkilöt, jotka joutuvat työnsä takia tekemisiin lokitietojen ja toisten ihmisten viestien kanssa; heitä sitoo ehdoton vaitiolovelvollisuus ja tiedon hyväksikäyttö kielto
- Ylläpitohenkilöstön vaitiolovelvollisuudesta tulee laatia sitoumuslomake
- Ylläpitohenkilökunnalle tulee määritellä henkilökohtaiset käyttäjätunnukset
- Ylläpidon toimenpiteistä tulee kerätä tarvittavaa tietoa (tiedostojen käsittely, poisto ym.)
- Ylläpitotehtävät tulee mahdollisuuksien mukaan jakaa usealle henkilölle, joilla on eri käyttövaltuudet

3.5 Sähköpostiosoitteet

- Organisaatiolla tulee olla virallisten asioiden hoitoa varten tarkoitettuja organisaatio-osoitteita (esim. kirjaamo@virasto.fi)
- Virastolle tarkoitetut sähköpostiviestit tulee ensisijaisesti ohjata organisaatio-osoitteisiin (esim. tiedotus@virasto.fi ja neuvonta@virasto.fi)
- Esimerkiksi viraston www-sivulla tulee ohjata lähettämään viesti viranomaiselle nimenomaan organisaatio-osoitteeseen, eikä yksittäiselle virkamiehelle tai työntekijälle
- Viranomaisen vastaukset on mahdollisuuksien mukaan lähetettävä organisaatio-osoitteesta
- Sähköpostin käyttäjätunnusten ja sähköpostiosoitteiden luonti ja hallinnointi on ohjeistettava
- Osoitteiden on oltava yksikäsitteisiä, samannimisillä henkilöillä esim. lisäerottimien avulla yksilöitävissä

3.6 Sähköpostiosoitteiden julkaiseminen

- Organisaation on arvioitava, kenen yhteystietoja annetaan julkisuuteen
- Ensisijaisesti tulee julkaista organisaatio-osoite
- Organisaatio-osoitteen julkaisemisesta päättää työnantaja
- Virkasähköpostiosoite voidaan julkaista, jos työnantaja katsoo sen tarkoituksenmukaiseksi otettuaan huomioon ao. työntekijän tehtävän ja oman toimialueensa luonteen.
- Organisaatio ei julkaise työntekijöidensä organisaation ulkopuolisia sähköpostiosoitteita.

3.7 Organisaation sähköpostiviestin käsittelyssä huomioitavaa

- Viran tai toimen hoitoon liittyviä viestejä varten tulee avata oma, organisaation nimellä oleva sähköpostiosoite (organisaatio-osoite voi olla myös postituslista); käyttö tulee ohjeistaa ja osoitteelle tulee nimetä yksi tai useampi vastuuhenkilö
- Yhdellä organisaatiolla voi olle eri tehtäviinsä useita eri organisaatio-osoitteita (esim. kirjaamo@organisaatio.fi, hallintojohtaja@ organisaatio.fi, tietoturvapaallikko@organisatio.fi)
- Organisaatiosähköpostin lähettäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen tulee kieltää
- Vastaukset tulee mahdollisuuksien mukaan lähettää organisaation sähköpostiosoitteesta
- Organisaatio-osoitteeseen saapunut sähköposti jaetaan asian valmistelijalle tai muille asianosaisille tiedoksi
- Organisaatio-osoitteen käyttöön oikeutetun henkilön tulisi lukea yksikköön saapuneet sähköpostiviestit vähintään kerran päivässä ja etenkin hakemuksille määrättyinä tärkeinä määräaikoina
- Vastaanottajan on (viipymättä) lähetettävä sähköisen viestin lähettäjälle vastaanottokuittaus. Asiakkaalle lähetettävä vastaanottokuittaus ei kuitenkaan ole kannanotto asian käsittelyn edellytyksiin tai lopputulokseen eikä sellaisenaan merkitse sitä, että asia on tullut organisaatiossa vireille. Kuittausviestin lähettää asiaa käsittelevä henkilö, automaattikuittauksia ei tule käyttää.
- Viestit on käsiteltävä julkisuuslain edellyttämällä tavalla
- Viestit on arkistoitava arkistointisäännösten mukaisesti

3.8 Virkasähköpostiviestin käsittelyssä huomioitavaa

- Virkasähköpostin lähettäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen tulee kieltää tietoturvallisuuden ja tiedonhallinnan vuoksi
- Käyttöpolitiikan on määriteltävä, millainen viestintä on sallittua (turvaluokiteltu tieto jne.)
- Virkasähköpostiosoitteeseen liittyvää viestiä (lähetetty tai vastaanotettu) tulee pääsääntöisesti kohdella henkilökohtaisena viestinä
- Vastaanottajan on (viipymättä) lähetettävä sähköisen viestin lähettäjälle vastaanottokuittaus. Asiakkaalle lähetettävä vastaanottokuittaus ei kuitenkaan ole kannanotto asian käsittelyn edellytyksiin tai lopputulokseen eikä sellaisenaan merkitse sitä, että

asia on tullut organisaatiossa vireille. Kuittausviestin lähettää asiaa käsittelevä henkilö, automaattikuittauksia ei tule käyttää.
- Työntekijän lähettämästä virkasähköpostiviestistä tulee ilmetä, että sen lähettäjä on viranomainen, ei yksittäinen työntekijä/virkamies
- Mikäli henkilökohtainen posti on kielletty virkasähköpostiosoitteeseen, tulee työntekijän informoida viestintäkumppaneitaan osoitteen käyttämisestä ainoastaan virkapostiin
- Viestit on käsiteltävä julkisuuslain edellyttämällä tavalla
- Sähköpostiviestejä on käsiteltävä ja ne on arkistoitava arkistonmuodostamissuunnitelmassa ilmenevällä tavalla

3.9 Henkilökohtaisen sähköpostiviestin käsittelyssä huomioitavaa

- Henkilökohtainen sähköpostiosoite on tyypillisesti sama kuin virkasähköpostiosoite
- Työntekijän henkilökohtaiset viestit tulee erottaa selvästi organisaatiolle kuuluvista viesteistä. Työntekijän tulee siirtää virkasähköpostiosoitteeseensa tulevat henkilökohtaiset viestit välittömästi omiin kansioihinsa, joiden nimestä yksityisyys on nähtävissä (private, yksityisasiat tms.). Tämä koskee sekä saapuvia että lähteviä viestejä.
- Viraston tulee ohjeistaa työntekijöidensä sähköpostiosoitteiden käyttäminen sähköiseen kauppaan tai muihin yksityisasioihin
- Virasto voi ohjeistaa, ettei työntekijä saa ohjata henkilökohtaisia viestejä viraston sähköpostijärjestelmiin
- Henkilökohtaiseen sähköpostiosoitteeseen liittyvää viestiä (lähetetty tai vastaanotettu) tulee pääsääntöisesti kohdella henkilökohtaisena viestinä
- Palvelussuhteen päättyessä työntekijän tulee poistaa henkilökohtaiset viestit, luovuttaa työhön liittyvät viestit työnantajan nimeämälle henkilölle ja ilmoittaa viestintäkumppaneilleen sähköpostiosoitteen poistumisesta

3.10 Muiden sähköpostiviestin käsittelyssä huomioitavaa

- Työntekijä ei saa käyttää organisaation ulkopuolista sähköpostiosoitetta organisaatioon liittyviin työtehtäviin.
- Virka- ja organisaatiosähköpostiviestien lähettäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen tulee kieltää tietoturvallisuuden ja tiedonhallinnan vuoksi

- Organisaation ulkopuolisessa sähköpostissa ei tule käyttää samoja käyttäjätunnuksia ja salasanoja kuin virkasähköpostissa
- Organisaation ulkopuolisen sähköpostiosoitteen ja –palvelun käyttö työaikana ja organisaation työasemilta käsin tulee ohjeistaa (onko sallittua ja jos, niin miten)

3.11 Perille menemättömän sähköpostiviestin käsittely

- Sähköpostiviestin lähettäjällä on pääasiallinen vastuu viestin luettavuudesta, viestin perillemenosta, määräajoista ja muista näihin verrattavista seikoista
- Perille menemättömän viestin käsittely on pyrittävä hoitamaan automatiikalla ja käyttöoikeuksien avulla
- Mikäli saapuvan viestin osoite ei ole sähköpostijärjestelmän tiedossa, lähetetään viestin lähettäjälle automaattisesti virheilmoitus
- Lähetys- ja palautusvelvollisuudet eivät koske haittaohjelmaviestejä eivätkä roskapostia
- Ylläpitohenkilöstöllä on vaitiolovelvollisuus ja hyväksikäyttökielto viestin sisällöstä ja olemassaolosta
- Vastaanotto- ja välityskelvottomat viestit voidaan hävittää

3.12 Väärään osoitteeseen saapunut sähköpostiviesti

- Viranomaisen toimivaltaan kuulumaton, ilmeisestä erehdyksestä tai tietämättömyydestä viranomaiselle lähetetty sähköpostiviesti on siirrettävä hallintolain mukaisesti toimivaltaiseksi katsotulle viranomaiselle, jos se on tiedossa; siirrosta on ilmoitettava viestin lähettäjälle
- Muu toiselle organisaatiolle tai henkilölle tarkoitettu sähköpostiviesti tulee ohjata edelleen oikeaan osoitteeseen, jos osoite on tiedossa. Mikäli osoitetta ei ole tiedossa, viestin vastaanottaja lähettää alkuperäiselle lähettäjälle tiedon epäonnistuneesta toimituksesta ja hävittää saapuneen viestin
- Roskaposteja ja haittaohjelmia sisältäviä viestejä ei saa lähettää edelleen
- Viestin tietoonsa saaneella henkilöllä on vaitiolovelvollisuus ja hyväksikäyttökielto viestin sisällöstä ja olemassaolosta

3.13 Sähköpostiviestin salaus ja todentaminen

- Pääsääntönä on, ettei erittäin salaiseksi tai salaiseksi luokiteltuja asiakirjoja saa lähettää sähköpostilla
- Muita kuin julkisia tietoja ja julkisia henkilötietoja ei tule siirtää sähköpostina tai muuna Internet-tiedonsiirtona ilman salakirjoitusta
- Salassa pidettäviä tietoja ja salassa pidettäviä henkilötietoja voidaan siirtää, mikäli sen salaukseen käytetään riittävän vahvoja salausalgoritmeja (Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001) tai koko tiedonsiirtoväylää voidaan pitää riittävän turvallisena
- Työnantajalla tulee olla mahdollisuus avata salattu organisaatiosähköpostiviesti
- Käytettävien salausohjelmien tulee organisaatio- ja virkasähköpostiviestien osalta olla työnantajan hyväksymiä ja käyttöönottamia
- Sähköpostilla vastaanotetun asiakirjan oikeellisuus ja aitous on tarvittaessa varmistettava
- Virkasähköpostin ollessa siten salattu, että vain vastaanottaja voi avata sen, se on avattava välittömästi siirron jälkeen, talletettava sekä salattava tarvittaessa organisaation salausavaimella
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeissa on esitetty suosituksia sähköpostin käsittelystä

3.14 Menettelysäännöt työntekijän ollessa väliaikaisesti poissa

- Ennakoiduissa poissaolotilanteissa työntekijän ja esimiehen on huolehdittava työntekijän sähköpostin asianmukaisesta hoidosta. Suositeltavin tapa on postilaatikon lukuoikeuden antaminen tehtäviä poissaolon aikana hoitavalle henkilölle pääsyoikeuslistojen avulla.
- Työnantajalla on oikeus lain yksityisyyden suojasta työelämässä (759/2004, 18-20§) asettamissa rajoissa saada käyttöönsä työnantajalle kuuluvat, sen toiminnan jatkumisen kannalta välttämättömät viestit työntekijän estyneenä ollessa.
- Työntekijälle virkasähköpostiosoitteella lähetettyjen tai tämän lähettämien viestien sekä selville saaminen että niiden avaaminen perustuu ensisijaisesti työntekijän suostumukseen sekä siihen että työntekijän luottamukselliset henkilökohtaiset viestit ovat erotettavissa työnantajalle kuuluvista viesteistä. (viestien erottelusta ks. luku 3.9).

3.15 Palvelussuhteen päättyminen

- Virkasähköpostin ja henkilökohtaisen sähköpostin käyttöoikeudet päättyvät palvelussuhteen päättyessä
- Sähköpostiosoite on poistettava käytöstä palvelussuhteen päättyessä
- Työntekijän tulee poistaa henkilökohtaiset viestit, luovuttaa työhön liittyvät viestit työnantajan nimeämälle henkilölle ja ilmoittaa viestintäkumppaneilleen sähköpostiosoitteen poistumisesta
- Lopetettuun sähköpostiosoitteeseen tulevasta postista lähetetään (virhe)ilmoitus, ettei tunnus ole käytössä
- Sähköpostiosoitteen lopettamisen yhteydessä tulee määritellä vastuut ja toimenpiteet:
  - Kuka antaa määräyksen sähköpostiosoitteen lopettamisesta. Sähköpostiosoitteiden hallinta tulisi kytkeä organisaation henkilöstöhallinnon rekistereihin, joista tieto saadaan automaattisesti
  - Erityisesti tulisi ohjeistaa tilanne, jossa sähköpostiosoitteeseen on voinut tulla organisaatiolle tarkoitettuja viestejä
- Suositellaan harkittavaksi vastausilmoitusta ”... Näitä asioita hoitaa jatkossa ...”
- Työntekijän kuoltua hänen sähköpostitunnuksensa tulee poistaa.
- Sähköpostien käsittelystä kuolemantapauksen jälkeen ei ole oikeuden ennakkotapauksia ja laintulkinta on osin ristiriitainen. Viestien käsittely on syytä tehdä huolellisesti, kirjaten tehdyt toimet ja yksityisten viestien osalta mahdollisuuksien mukaan yhteistyössä perikunnan kanssa.
- Yhteisötilaajan vaitiolovelvollisuus ja tiedon hyväksikäyttö kielto viestinnän osapuolten viesteistä ja tunnistamistiedoista määräytyy SVTSL:n mukaan myös henkilön kuoleman jälkeen. Nämä oikeudet eivät siirry perikunnalle.
- Työnantajan oikeuksista työntekijän sähköpostiviesteihin kuolemantapauksessa on säädetty työelämän tietosuojalaissa.
- Perikunnan oikeudet tekijänoikeuden alaiseen materiaaliin määräytyvät tapauskohtaisesti esimerkiksi tekijänoikeuslain mukaisesti.

3.16 Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen

- Työnantajalla on oikeus asettaa rajoituksia sähköpostiviestien ja niiden liitetiedostojen suhteen; rajoitukset voidaan toteuttaa esimerkiksi suodattamalla liian suuret, vääräntyyppiset, roskapostit tai organisaation tietoturvallisuutta vahingoittavat tai uhkaavat viestit ja tiedostot - kuten haittaohjelmat - pois

- Työntekijöille on tiedotettava sähköpostin ja liitetiedostojen käyttöön liittyvistä rajoituksista
- Työnantajalla on oikeus ohjelmallisesti tarkistaa viestit ja liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta; työnantajalla on oikeus myös poistaa tällaiset viestit ja liitetiedostot
- Ylläpidon oikeudet puuttua sähköpostijärjestelmän toiminnan tai turvallisuuden vaarantaviin viesteihin tulee määritellä
- Työnantajalla on yhteisötilaajana oikeus estää käyttäjän pyynnöstä sähköisen viestinnän tietosuojalain 26-28 §:ssä tarkoitetun suoramarkkinoinnin vastaanottaminen.

4 OHJEESSA HUOMIOON OTETUT SÄÄDÖKSET

4.1 Säädösluettelo

Sähköpostiviestinnän käyttöpolitiikkaa ohjaavat säädöstasolla muun muassa:

- Suomen Perustuslaki 10.2 § ja 12.1 § (731/1999)
- Henkilötietolaki (523/1999) ja laki sen muuttamisesta (986/2000)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 7 §:n muuttamisesta (479/2001, voimaan 1.10.2001)
- Rikoslain 35:1,2 §; 38:2 §, 38:3–4 §; 38:8 §
- Pakkokeinolaki (450/1987) 5a-luku (403/1995; 1026/1995 ja 22/2001)
- Valtion virkamieslaki (621/1999)
- Työsopimuslaki (320/1970) ja (55/2001, voimaan 1.6.2001)
- Hallintolaki (434/2003)
- Arkistolaki (831/1994)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003)

4.2 Suomen perustuslaki

10 § Yksityiselämän suoja

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

Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

12 § Sananvapaus ja julkisuus

Jokaisella on sananvapaus. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja ***vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä.*** *Tarkempia säännöksiä sananvapauden käyttämisestä annetaan lailla.*

Viranomaisten 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.

Luottamuksellisen viestin salaisuus on säädetty kansalaisten perusoikeudeksi. Sähköpostiviesti on katsottava luottamukselliseksi viestiksi ja siihen sovelletaan perustuslaissa säädettyä loukkaamattomuutta.

On huomattava, että perustuslain säädöksessä, samoin kuin edellä mainittujen säädösten esitöissä, korostetaan sitä, ettei perusoikeuksia saa rajoittaa kuin tarkoin määritellyissä tilanteissa ja lain nimenomaisen säädöksen nojalla. Tämä periaate sisältyy myös Suomea velvoittaviin kansainvälisiin sopimuksiin. Erityisesti niihin sisältyy ajatus, ettei perusoikeuksien rajoittamista saa tehdä pelkästään hallinnollisten määräysten, vakiintuneiden tapojen tai tarkoituksenmukaisuuden perusteella.

Luottamuksellisen viestin loukkaamattomuutta koskevan hallituksen esityksen mukaan säännös ei suojaa yksinomaan viestin lähettäjää, vaan kyseessä on molempien viestinnän osapuolten perusoikeus.

4.3 Henkilötietolaki

Henkilötietolakia ovat velvolliset soveltamaan muun muassa kaikki työnantajat, joilla on toimipaikka Suomen alueella tai muutoin Suomen oikeudenkäytön piirissä sekä näiden työnantajien toimeksiannon saajat. Henkilötietolakia on noudatettava käsiteltäessä henkilötietoja, jollei muualla laissa toisin säädetä. Henkilötietolakia sovelletaan muun muassa aina henkilötietojen automaattisen käsittelyyn. Henkilötiedoilla tarkoitetaan kaikenlai-

sia luonnollista henkilöä - kuten työntekijää, viranomaisen asiakasta tai muuta henkilöä kuten henkilökohtaisen viestin lähettäjää - taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa koskevaksi. Lain tarkoittama henkilötieto eli henkilöä koskeva merkintä voi olla tallennettu esimerkiksi sähköiselle, optiselle tai magneettiselle tallenteelle.

Työntekijän lähettämistä ja työntekijälle lähetetyistä sähköpostiviesteistä tallentuu merkintöjä viestien välittämiseen ja säilyttämiseen tarkoitetuille tietokoneille ja niiden käyttöä tukeville palvelintietokoneille. Henkilötiedot, jotka sisältyvät sähköpostin käyttöoikeudet määrittävään käyttäjätiedostoon ja sen käyttöä kirjaavaan käyttökirjanpitoon (mm. kuka lähetti ja milloin viestin tietylle vastaanottajalle) ovat henkilötietolain tarkoittamia henkilötietoja. Luonnollisen henkilön sähköpostiosoite on henkilötieto. Myös itse viestien sisällöstä voi ilmetä henkilötietoja.

Henkilötieto, henkilötietojen käsittely, henkilörekisteri, rekisterinpitäjä, rekisteröity, sivullinen ja suostumus on määritelty henkilötietolain 3 §:ssä. Työnantajan ja sen toimeksiannon saajan on tunnettava käsitteet voidakseen toimia henkilötietolain ja viranomaisten toiminnan julkisuudesta annetun lain edellyttämällä tavalla. On tiedettävä millaista henkilötietojen käsittelyä organisaatiossa tapahtuu ja mitkä määritellyn henkilötietojen käsittelyn tarkoituksen kannalta yhteenkuuluvat merkinnät kulloinkin muodostavat henkilörekisterin. Toimeksianto ei poista rekisterinpitäjälle kuuluvaa juridista vastuuta. Toimeksiantajan ja toimeksiannon saajan keskinäiset vastuut määräytyvät tarvittaessa sopimuksen pohjalta, joka on syytä tehdä kirjallisesti.

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Työnantaja on lain tarkoittama **rekisterinpitäjä** ja työntekijä lain tarkoittama **rekisteröity**. Työnantajan oikeus käsitellä työntekijöitä koskevia, muita kuin 11 §:ssä säädettyjä arkaluonteisia henkilötietoja perustuu henkilötietolain 8.1 §:n 5 kohdassa säädettyyn asialliseen yhteyteen ja lain velvoitteisiin. **Arkaluonteisten henkilötietojen** - kuten poliittista ja uskonnollista vakaumusta taikka ammattiliittoon kuulumista kuvaavien henkilötietojen käsittelyyn työnantajalla tulee olla lain 12 §:ssä säädetty peruste. Henkilötietoja tallentuu myös siitä luonnollisesta henkilöstä, joka lähettää viranomaisen palveluksessa olevalle tai viranomaiselle osoitetun sähköpostiviestin. Myös hänen osaltaan viranomaistyönantajalla tulee olla jokin 8.1 §:ssä mainittu peruste käsitellä henkilötietoja. Sivullisia ovat muu henkilö, yhteisö, laitos tai säätiö kuin ao. rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevä. Annettaessa tai ilmaistessa henkilötietoja sivulliselle tulee varmistaa, että sivullisella on laillinen oikeus käsitellä niitä (ks. jäljempänä kohta 2.4, kappale 8).

Henkilötietolain 5 §:ssä säädetty huolellisuusvelvoite edellyttää, että työnantajan tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelyta-

paa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa tai muita yksityisyyden suojan turvaavia perusoikeuksia - kuten luottamuksellisen viestin salaisuuden loukkaamattomuutta - rajoiteta ilman laissa säädettyä perustetta. Vastaava velvollisuus on toimeksiannon saajalla.

Henkilötietolain 6 §:n mukaisesti työnantajalla on velvollisuus suunnitella henkilötietojen käsittely. Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua työnantajan toiminnan kannalta. Säännös edellyttää muun muassa **määrittelemään henkilötietojen käsittelyn tarkoituksen,** joka tulee ilmetä 10 §:n mukaisesti laaditusta ja saatavilla pidettävästä rekisteriselosteesta ja josta työnantajan on 24 §:ssä edellytetyllä tavalla, muiden säännöksessä mainittujen tietojen lisäksi informoitava työntekijöitä. Lain edellyttämällä tavalla laadittu, henkilölle esitetty tai annettua rekisteriselosteasiakirja on eräs tapa täyttää informointivelvoite. Käsitellä saa 9 §:n mukaan vain määritellyn käsittelyn tarkoituksen kannalta tarpeellisia henkilötietoja, joiden virheettömyydestäkin on huolehdittava.

Työnantajan ja mikäli työnantaja on ulkoistanut toimeksiannon perusteella (ks. 8.1 §:n 7 kohta) automaattisesti käsiteltyjen henkilötietojen ja henkilörekisteriin talletettujen henkilötietojen käsittelyyn liittyvät tietojenkäsittelytoimenpiteet itsenäisen ammatin- tai elinkeinonharjoittajan suoritettavaksi, tulee myös tämän toimeksiannon saajan 32 §:n mukaisesti huolehtia henkilötietojen suojaamisesta. Asiattomat eivät saa päästä käsiksi henkilötietoihin. Lain vastainen käsittely on ehkäistävä. Toimeksiannon saajan kanssa tehtävässä kirjallisessa sopimuksessa on tuotava esille muun muassa toimeksiannon saajan palveluksessa olevien henkilöiden vaitiolovelvollisuus ja hyväksikäyttökielto. Tietoturvallisuustoimenpiteiden laatu ja laajuus tulee arvioida henkilötietoihin ja organisaatioon kohdistuvien riskien ja käytettävissä olevien suojaamiskeinojen pohjalta.

Ellei työnantaja henkilötietolaissa säädetyn perusteen nojalla toisin katso, on työntekijällä ja muulla rekisteröidyllä oikeus saada pyynnöstä itselleen joko kirjallisesti tai nähtäväkseen häntä itseään koskevat, mihin tahansa henkilörekisteriin talletetut henkilötiedot salassapitosäännösten estämättä. Tästä tarkastusoikeuden käyttämisestä, siihen liittyvistä menettelytavoista ja sen toteuttamisen poikkeamismahdollisuuksista on säädetty 26-28 §:ssä.

Harkittaessa henkilörekisteriin talletettujen henkilötietojen siirtämistä sähköpostiviestin välityksellä EU:n jäsenvaltioiden tai ETA:n ulkopuolelle, on siirtäjän varmistettava lain 22, 22a tai 23 §:ssä säädetyn siirtoedellytyksen olemassaolo.

Henkilötietolain säännösten noudattamisen tehostamiseksi on laissa säädetty joukko rangaistavia tekoja ja laiminlyöntejä. Henkilötietolain 48.1 §:n mukaan henkilörekisteriin kohdistuvasta tietomurrosta säädetään RL 38 luvun 8 §:ssä. Säännös on toissijainen ja syrjäytyy, jos tietomurto liittyy yritysvakoiluun (RL 30: 4 §), vahingontekoon (RL 35: 1-4 §) tai viestintäsalaisuuden loukkaamiseen (RL 38: 3 §). Henkilörekisteririkkomukset on lueteltu henkilötietolain 48.2 §:ssä ja henkilörekisteririkokset rikoslain 38 luvun 9 §:ssä.

Henkilörekisteriselostelomake on saatavissa tietosuojavaltuutetun toimistosta ja myös osoitteesta http//www.tietosuoja.fi/1582.htm..

4.4 Laki viranomaisten toiminnan julkisuudesta

Lain 4 §:n mukaan **viranomaisella** tarkoitetaan tässä laissa muun muassa valtion hallintoviranomaisia sekä muita valtion virastoja ja laitoksia; tuomioistuimia ja muita lainkäyttöelimiä; valtion liikelaitoksia; Suomen Pankkia mukaan lukien Rahoitustarkastus, Kansaneläkelaitosta sekä muita itsenäisiä julkisoikeudellisia laitoksia; eduskunnan virastoja ja laitoksia. Myös näiden viranomaisten toimeksiannon saajien on tunnettava tämän lain säännökset.

Lain 5 §:ssä on säädetty siitä, mikä on em. **viranomaisen asiakirja**. Säännöksen 1 momentin mukaan asiakirjalla tarkoitetaan tässä laissa kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta (vrt. henkilörekisterin määritelmä henkilötietolaista) tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.

Lain 5 §:n 2 momentin mukaan **viranomaisen asiakirjalla** tarkoitetaan viranomaisen **hallussa olevaa** asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta, ja viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten.

Lain 5 §:n 3 momentin mukaan **viranomaisen asiakirjana ei pidetä 5 momentissa säädetyin poikkeuksin:**

1) viranomaisen palveluksessa olevalle tai luottamushenkilölle **hänen muun tehtävänsä tai asemansa vuoksi lähetettyä kirjettä tai muuta asiakirjaa**;

2) viranomaisen palveluksessa olevan tai viranomaisen toimeksiannosta toimivan laatimia **muistiinpanoja** taikka sellaisia **luonnoksia**, joita laatija ei ole vielä antanut esittelyä tai muuta asian käsittelyä varten;

3) viranomaisen sisäistä koulutusta, tiedonhakua tai muuta niihin verrattavaa **sisäistä käyttöä varten hankittuja asiakirjoja;**

4) asiakirjaa, joka on **annettu viranomaiselle yksityisen lukuun suoritettavaa tehtävää varten tai laadittu sen suorittamiseksi;**

5) viranomaiselle löytötavarana jäänyttä tai toimitettua asiakirjaa.

Lain 5 §:n 4 momentin mukaan lakia sovelletaan viranomaisissa työskentelevien sekä viranomaisten ja niiden lukuun toimivien yksityisten ja yhteisöjen välisiä neuvotteluja, yhteydenpitoa ja muuta niihin verrattavaa viranomaisten sisäistä työskentelyä varten laadittuihin asiakirjoihin vain, **jos asiakirjat sisältävät sellaisia tietoja, että ne arkistolainsäädännön mukaan on liitettävä arkistoon.** Jos asiakirjat kuitenkin liitetään arkistoon, viranomainen voi määrätä, että tietoja niistä saa antaa vain viranomaisen luvalla.

Lain 5 §:n 5 momentin mukaan se, mitä asiakirjan salassapidosta tämän lain 24 §:ssä tai muussa laissa säädetään, sovelletaan myös 3 momentin 2 kohdassa ja 4 momentissa tarkoitettuihin asiakirjoihin.

Lain tarkoittama viranomaisen asiakirja voi sisältää sekä julkisia että salassa pidettäviä tietoja. Julkisuuslaissa salassa pidettäviksi säädetyt tiedot mukaan lukien tunnistettavia henkilöitä koskevat henkilötiedot on lueteltu julkisuuslain 24.1 §:ssä. Kunkin viranomaisen on tunnettava omaa toimialaansa koskevat salassapito-säännökset tarkasti. Kyse voi olla esimerkiksi ulkovaltasuhteista, maanpuolustuksesta, yrityssalaisuuksista, työmarkkinaosapuolen tai työriidan osapuolena laadituista tai saamista tiedoista taikka henkilön terveydentilaa koskevista tiedoista. On otettava kantaa, onko ylipäätään mahdollista lähettää sähköpostiviestinä salassa pidettäväksi säädettyjä henkilötietoja ja muita tietoja käyttämättä salausmenetelmää.

Julkisuuslain 9–12 §:ssä on säädetty o**ikeudesta saada tieto asiakirjasta** ja 13–15 §:ssä **menettelytavoista asiakirjan pyytämisessä, sen antamisesta tai antamisesta kieltäytymisestä ja siirrosta toiselle viranomaiselle.** Lain 16 §:ssä on säädetty **asiakirjan antamistavoista,** ei sen sijaan niiden julkisuudesta tai salassapidosta. Säännöksen 1 momentissa säädetty antamistapa soveltuu sähköpostiviestistä ilmenevien tietojen antamiseen. Säännöksen kolmannen momentin mukaan viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja (perusteet löytyvät joko erityislaista tai henkilötietolain 2.5 §:stä, 8.1 §:stä ja 12–18 §:stä sekä siitä, jos luovutuksensaajan toiminta jää kokonaan henkilötietolain soveltamisalan ulkopuolelle eli 2.3 §:ssä mainittu tilanne). Henkilötietoja saa kuitenkin luovuttaa suoramarkkinointia ja mielipide- tai markkinatutkimusta varten vain, jos niin erikseen säädetään tai jos rekisteröity (kuten viranomaisen palveluksessa oleva henkilö) on antanut siihen suostumuksensa.

Viranomaisen tulee arkistonmuodostamissuunnitelmassaan ratkaista, milloin viranomaiselle toimitettu tai viranomaisen palveluksessa olevan henkilön laatima sähköpostiviesti on organisaation arkistoon kuuluva asiakirja. Sähköpostiviestien käsittelyn etukäteissuunnittelu ja ohjeistaminen edellyttää niiden säilytysaikojen, -tavan ja muotojen osalta tukeutumista organisaation asiakirjahallinnosta vastaavan henkilön asiantuntemukseen.

Julkisuuslain soveltamisalaan kuuluvan viranomaisen on toteutettava viranomaisten toiminnan julkisuudesta annetun asetuksen 1 §:ssä säädetyt selvitykset hyvän tiedonhallintatavan toteuttamiseksi. Asetuksen 2 §:ssä on kuvattu erityissuojattavan tietoaineiston luokitus ja 3 §:ssä tällaista tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet. Nämä säännökset tulee ottaa huomioon myös sähköpostiviestinnän osalta.

Valtiovarainministeriö on antanut turvaluokiteltujen ja muiden salassa pidettävien asiakirjojen käsittelystä ohjeen (VAHTI 2/2000), joka löytyy osoitteesta: http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/vahti2.htm

4.5 Sähköisen viestinnän tietosuojalaki (516/2004)

Koska kyseessä on laki, jota viranomaisten tulee yhteisötilaajina soveltaa myös suhteessa työntekijöihinsä, jotka ovat lain tarkoittamia käyttäjiä, on tähän lakiin syytä perehtyä huolella. Alla lyhyt yhteenveto lain sisällöstä sekä poimintana muutama keskeinen pykälä.

Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. Lain 2 §:ssä on määritelty mitä muun muassa viestillä, viestintäverkolla, tunnistamis- ja paikkatiedoilla, yhteisötilaajalla ja käyttäjällä tarkoitetaan. Lain soveltamisala on määritelty 3 §:ssä. Lain 2 luku sisältää säännökset yksityisyyden ja luottamuksellisen viestin suojasta. 3 luvussa säädetään perusteet viestien ja tunnistamistietojen käsittelylle ja 4 luvussa paikkatietojen käsittelylle. 5 luvun säännökset viestinnän tietoturvasta velvoittavat myös yhteisötilaajia. 6 luvussa säädetään puhelupalveluista ja 7 luvussa suoramarkkinoinnista. 8 luku sisältää muun muassa säännökset viestintäviraston ja tietosuojavaltuutetun jaetusta toimivallasta. Luvussa 9 säädetään tiedonsaantioikeuksista, luvussa 10 tietoturvamaksuista ja luvussa 11 erinäisistä säännöksistä.

Kaksi poimintaa laista:

Yksityisyyden ja luottamuksellisen viestin suoja
4 §
Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuus

Viesti, tunnistamistiedot ja paikkatiedot ovat luottamuksellisia, jollei tässä tai muussa laissa toisin säädetä.

Viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Viestiin liittyvät tunnistamistiedot ovat kuitenkin luottamuksellisia. Verkkoviestin tunnistamistietojen luovuttamisesta säädetään sananvapauden käyttämisestä joukkoviestinnässä annetun lain (460/2003) 17 §:ssä.

Edellä 1 momentissa säädetty koskee myös verkkosivustojen selaamisesta kertyviä tunnistamistietoja.

5 §
Vaitiolovelvollisuus ja hyväksikäyttökielto

Se, joka on ottanut vastaan tai muutoin saanut tiedon luottamuksellisesta viestistä tai tunnistamistiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, tunnistamistietoa tai tietoa viestin ole-

massaolosta, ellei laissa toisin säädetä.

Se, joka on ottanut vastaan tai muutoin saanut tiedon paikkatiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman paikannettavan suostumusta ilmaista tai käyttää hyväksi paikkatietoa tai tietoa sen olemassaolosta, ellei laissa toisin säädetä.

Teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai viestintämarkkinalain 137 §:ssä tarkoitetun teleurakoitsijan palveluksessa oleva tai ollut ei saa ilman viestinnän osapuolen tai paikannettavan suostumusta ilmaista, mitä hän on tehtävässään saanut tietää viesteistä, tunnistamistiedoista ja paikkatiedoista, ellei laissa toisin säädetä.

Edellä 3 momentissa tarkoitettu vaitiolovelvollisuus on myös sillä, joka toimii tai on toiminut teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai teleurakoitsijan lukuun.

Näihin kohtiin liittyvä rangaistussäännös on 42§:ssä.

Viestinnän tietoturva

19 §

Velvollisuus huolehtia tietoturvasta

Teleyrityksen ja lisäarvopalvelun tarjoajan on huolehdittava palvelujensa tietoturvasta. Yhteisötilaajan on huolehdittava käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Nämä toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Teleyritys ja lisäarvopalvelun tarjoaja vastaa tilaajille ja käyttäjille 1 momentissa tarkoitetusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun. Edellä tässä momentissa tarkoitettu koskee yhteisötilaajaa käyttäjien tunnistamistietojen ja paikkatietojen käsittelyn osalta.

Viestintävirasto voi antaa teleyritykselle tarkempia määräyksiä 1 ja 2 momentissa tarkoitetusta palvelun tietoturvasta.

20 §

*Toimenpiteet tietoturvan toteuttamisek*si

Tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi teleyrityksellä, lisäarvopalvelun tarjoajalla tai yhteisötilaajalla ja näiden lukuun toimivalla on oikeus ryhtyä välttämättömiin toimiin 19 §:ssä tarkoitetun tietoturvan varmistamiseksi:

1) estämällä sähköpostiviestien, tekstiviestien ja muiden vastaavien viestien välittäminen ja vastaanottaminen;

2) poistamalla tietoturvaa vaarantavat haittaohjelmat viesteistä; sekä

3) toteuttamalla muut näihin rinnastettavat teknisluonteiset toimet.

Edellä 1 momentissa tarkoitettuihin toimiin saa ryhtyä vain, jos toimet ovat välttämättömiä verkkopalvelujen tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi.

Viestin sisältöön saa puuttua ainoastaan teknisin keinoin viestin tarkastamiseksi ja poistamiseksi, jos on todennäköisiä syitä epäillä viestin sisältävän sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, jota tarkoitetaan rikoslain (39/1889) 34 luvun 9 a §:n 1 kohdassa tai jos on todennäköisiä syitä epäillä, että viestiä käytetään rikoslain 38 luvun 5 §:ssä säädettyyn tietoliikenteen häirintään.

Toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä verkkopalvelujen tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Toimenpiteet on lopetettava heti, kun niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

Viestintävirasto voi antaa tarkempia määräyksiä tietoturvaloukkausten tässä pykälässä tarkoitetusta teknisestä torjumisesta ja tietoturvaan kohdistuvien häiriöiden poistamisesta.

4.6 Laki yksityisyyden suojasta työelämässä ja eräät siihen liittyvät lait

Laki yksityisyyden suojasta työelämässä (759/2004) ja eräät siihen liittyvät lait löytyvät selityksineen osoitteesta www.mol.fi/ammatit/tietosuoja.html . Lain 6 luvussa säädetyistä perusteista hakea esille ja avata työnantajalle kuuluvia sähköpostiviestejä on kerrottu kohdassa 2.8. Lain 21 §:ssä säädetään yhteistoiminnasta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä seuraavasti:

Työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa ja yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.

Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä.

Lain 24 §:n mukaan työnantaja tai tämän edustaja, joka tahallaan tai törkeästä huoli-

mattomuudesta vastoin 19 §:n säännöksiä hakee esille tai vastoin 20 §:n säännöksiä avaa työntekijälle lähetetyn tai työntekijän lähettämän viestin (10 kohta) tai rikkoo 21 §:n 2 momentin säännöksiä määrittely- tai tiedottamisvelvollisuudesta (11 kohta), on tuomittava, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, yksityisyyden suojasta työelämässä annetun lain rikkomisesta sakkoon. Rangaistus henkilörekisteririkoksesta, tietomurrosta, salakatselusta, salakuuntelusta, viestintäsalaisuuden loukkauksesta, salassapitorikoksesta ja virkarikoksista säädetään rikoslaissa (39/1889).

4.7 Rikoslaki

Seuraavassa käsitellään eräitä rikoslaissa rangaistaviksi säädettyjä tekoja.

38:3 § Viestintäsalaisuuden loukkaus

Joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla tavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä, on tuomittava viestintä-salaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.
Yritys on rangaistava.

Joka oikeudettomasti hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.

Säännöksestä on tärkeää huomata, että viestin sisällön lisäksi lähettäjä- ja vastaanottajatietojen oikeudeton hankkiminen on kriminalisoitu. Mikäli tekoon syyllistynyt on käyttänyt tiedon hankinnassa hyväksi luottamusasemaansa tai teknistä apuvälinettä on teko säädetty ankarammin rangaistavaksi. Mikäli rikoksen tekijänä on virkamies, voi tekoon soveltua lisäksi rikoslain 40 luvun säännökset virkavelvollisuuden rikkomisesta.

Säännöksen 1 momentti antaa suojaa suljetulle lähetykselle, joka sisältää vastaanottajalle tarkoitetun viestin. Sen ei tarvitse olla kirjallinen, vaan se voi muodostua esimerkiksi atk-tallenteista. Lähetyksen päällä on ilmettävä, että se on tarkoitettu vain nimeltä mainitun vastaanottajan avattavaksi. Suojaa saavat perinteisen kirjeen lisäksi myös sähköpostiviesti sekä viestit, joita ei siirretä mihinkään, vaan tallennetaan tietokoneen muistiin tietyn henkilön tai henkilö-piirin luettavaksi. Edellytyksenä on, että viesti on teknisin keinoin suojattu ulkopuolisilta ja tiedon hankkiminen viestistä tapahtuu tämä suojaus murtaen. Tietylle henkilölle hänen nimellään osoitetun sähköpostiviestin avaaminen suojauksen murtaen eli käyttämällä esimerkiksi urkkimalla saatua käyttäjätunnusta ja salasanaa on mitä ilmeisimmin rangaistavaa.

Rikoslain 38 luvun 4 §:ssä on säädetty **rangaistus törkeästä viestintäsalaisuuden rikkomisesta.** Se tulee sovellettavaksi muun muassa viraston käyttämän teleyrityksen palveluksessa olevan syyllistyessä viestintäsalaisuuden rikkomiseen.

Rikoslain 38 luvun 5-7 §:ssä on säädetty **eriasteisten tietoliikenteen häirintään liittyvistä rangaistavista teoista.**

RL 38:8 § Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelmän 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.

Rangaistavaa on jo yrittää selvittää tietojärjestelmää suojaavat tunnistetiedot tai murtaa muu turvajärjestely. Tietomurron kohteena on atk:lla ylläpidetty tietojärjestelmä, jolla säännöksen perustelujen mukaan yleensä tarkoitetaan tietyssä organisaatiossa käytettävää tietojenkäsittely- ja siirtolaitteiden muodostamaa kokonaisuutta, mutta joka voi olla myös toiminnallinen kokonaisuus niiden tuottamien palvelujen perusteella. Tietomurto voi kohdistua myös atk:lla ylläpidettyyn tietojenkäsittelykokonaisuuteen kuten henkilörekisteriin. Rangaistava teko edellyttää turvajärjestelyn, käyttäjätunnuksen, salasanan tai muun tunnistusmenetelmän murtamista nimenomaisella toimella, joten sellaisen järjestelyn satunnaisesta epäkunnosta aiheutunut pääsy ei kuulu säännöksen piiriin. Kuitenkin myös sattumalta onnistunut tunnusten selville saaminen on rangaistava, jos tarkoituksena on ollut oikeudeton tunkeutuminen. Teon rangaistavuuden kannalta ei ole merkitystä sillä, kuinka oikean käyttäjätunnuksen tai vastaavan hankkiminen on tapahtunut. Se voi olla esimerkiksi oikealta käyttäjältä urkittu tai löydetty oikean käyttäjän tietokoneen lähistöltä olevalta muistilapulta. Rangaistavuus edellyttää, että tekijä tietää tunkeutuvansa järjestelmään oikeudettomasti. Tunkeutumiselta ei edellytetä mitään erityistä tarkoitusta tai sitä, että henkilötietoja käytetään. Rikos on tapahtunut, kun tunnistuskontrolli on läpäisty.

RL 35:1.2 § Vahingonteko

Vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

RL 34:9a § 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.*

7 LIITTEET

Liite 1: Sähköpostin suodatusohje

Tässä ohjeessa täsmennetään, miten sähköpostiviestejä organisaatiossa suodatetaan. Suodatuksen tulee aina tapahtua ohjelmallisesti ja viestintäsalaisuuden säilyttäen.

Tämä ohje on julkinen ja sen tulee olla julkisesti saatavilla.

Suodatetut viestit voidaan tapauskohtaisesti jättää välittämättä (kohdat 1-7), tuhota (kohta 9), eristää erilliselle karanteenialueelle määräajaksi, jonka jälkeen ne voidaan tuhota (kohdat 8-11), tai välittää vastaanottajalle roskapostiksi merkittynä (kohta 11). Haittaohjelmat tulee poistaa välitettävistä viesteistä. Suodatetuista viesteistä lähettäjälle tai lähettävälle postipalvelimelle ja/tai vastaanottajalle lähetettävien virheilmoitusten tulee olla RFC 2821 -standardin mukaisia. Virheilmoitukseen voidaan myös liittää käyttäjäystävällinen kuvaus virheestä silloin kuin se on mahdollista.

Suodatusmenetelmät

1. Third party open relay -esto, eli releointihyökkäysten esto organisaation koneiden kautta.

Organisaation ei välitä ulospäin sellaisia viestejä, jotka eivät ole lähtöisin organisaation osoiteavaruudesta ja joiden vastaanottajan osoite ei ole organisaation sähköpostiosoite. Lisäksi organisaatio estää palomuurikonfiguraatiossaan SMTP-yhteydet muihin kuin pääasiallisiin postipalvelimiinsa internetistä käsin.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Relaying denied”*

2. Postin välitys tuntemattomista toimialueista tai koneista

Organisaation postipalvelin tekee nimipalvelutarkastuksen lähettäjätoimialueen tai -koneen olemassaolon varmistamiseksi. Mikäli lähettävä toimialue tai kone ei selviä nimipalvelukyselystä, voidaan postitus estää tilapäisesti kunnes lähettävän koneen tai toimialueen nimipalvelutietueet ovat kunnossa.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”451 *Sender domain must resolve”*

3. Mustat listat (Black Lists)
Organisaatio ei välitä postia sellaisista postikoneista, joita voidaan käyttää releointihyökkäyksiin (ks. kohta 1). Organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja.

Esimerkkejä alla:
MAPS (Mail Abuse Prevention System)
ORDB (Open Relay DataBase)
DSBL (Distributed Server Boycott List)
SPAMHAUS (The Spamhaus Project)

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.käytettävä_musta_lista.domain”*

4. Postin välitys sellaisista postikoneista, joiden kautta tunnetusti lähetetään roskapostia
Organisaatio ei välitä postia sellaisista koneista, joiden kautta tunnetusti lähetetään roskapostia tai joita ylläpitävä organisaatio tunnetusti tukee roskapostittajia. Tähän organisaatio saa käyttää apunaan kansainvälisten, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkiksi NJABL-tietokantaa (Not Just Another Bogus List).

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.njabl.org”*

5. Postin välitys sellaisista koneista, joilla on dynaamisesti varattu verkko-osoite
Organisaatiolla on oikeus olla välittämättä postia sellaisista koneista, joiden verkko-osoite kuuluu dynaamisesti varattaviin osoiteavaruuksiin. Organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja, esimerkiksi NJABL Dynablock.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.njabl.org/dynablock.html”*.

Kohdissa 3, 4 ja 5 organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja.

Tietokantoja käytettäessä tulee varmistua niiden asianmukaisuudesta mm. tarkastamalla periaatteet, joilla osoitteita kantaan lisätään. Tietokantoja ylläpitävän palveluntar-

joajan on tarjottava helppokäyttöinen mekanismi, jolla osoitteita voi pyytää poistettavaksi kannasta. Poistopyynnöt on käsiteltävä kohtuullisen ajan kuluessa niiden tekemisestä.

Tietokantoja käytettäessä tarkastus voi olla reaaliaikainen tai organisaatio voi ylläpitää omaa kopiotaan tietokannoista, jota kuitenkin tulee päivittää kohtuullisin väliajoin.

6. Palvelinkohtainen pääsylista

Organisaatio käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsylistoja (access list). Listan avulla voidaan sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja, mikäli se on muun liikenteen turvaamiseksi välttämätöntä.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam” tai*
”550 Access Denied”

7. Liikennemääriin perustuva suodatus

Liikenneanalyysisuodatuksessa voidaan esimerkiksi sähköpostipalvelimen lokeja reaaliaikaisesti tarkkailemalla huomata poikkeamat normaalissa postinkulussa. Tällaisia roskapostitukseen viittaavia poikkeamia voivat olla epätavallisen pitkät yhteysajat postipalvelimeen, poikkeuksellinen määrä viestejä samasta isännästä tai suuri määrä vastaanottajia samassa viestissä. Liikennemääriä voi kontrolloida myös proaktiivisesti esimerkiksi hidastamalla yhteysnopeuksia tai rajoittamalla yhteysaikaa. Rajoituksia tulee kuitenkin aina käyttää harkiten, jotta esimerkiski sähköpostilistojen toiminta ei häiriytyisi.

8. Viestien koko ja liitetiedostojen määrä

Organisaatiolla on oikeus rajoittaa välittämiensä viestien kokoa ja niiden mahdollisesti sisältämien liitetiedostojen määrää. Tiedon viestin kokoon ja liitetiedostojen määrään liittyvistä rajoituksista tulee olla julkisesti saatavilla.

9. Haittaohjelmien poistaminen

Organisaatio poistaa välittämistään viesteistä haittaohjelmat mahdollisuuksiensa mukaan tai tarpeen vaatiessa tuhoaa koko haittaohjelman sisältävän viestin.

10. Liitetiedostojen tiedostotyypit

Organisaatiolla on oikeus olla vastaanottamatta / välittämättä riskialttiita, haittaohjelmien kuljetukseen tyypillisesti käytettäviä tiedostotyyppejä sisältäviä viestejä. Esimerkkejä tiedostotyypeistä.

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh

Ajantasainen lista tiedostotyypeistä, joita organisaation postipalvelin ei vastaanota /

välitä, tulee aina olla julkisesti saatavilla. Välittämättä jätettävät tiedostot on eristettävä määräajaksi karanteenialueelle ja ne on saatettava vastaanottajan tai lähettäjän tietoon ennen niiden tuhoamista. Tiedosto voidaan toimittaa vastaanottajalle tämän sitä pyytäessä, edellyttäen että tiedosto ei sisällä esim. haitalliseksi katsottua koodia.

11. Sähköpostin sisältöön perustuva suodatus

Organisaatio voi suodattaa roskapostia ohjelmallisesti sisällölliseen automaattiseen analyysiin perustuen, esimerkiksi pisteytykseen perustuvilla suodatusohjelmilla (Spam Assassin, IMF).

Sisällöllisessä analyysissa roskapostiksi luokiteltu viesti tulee aina merkitä roskapostiksi ja toimittaa vastaanottajan sähköpostilaatikkoon, suodattaa erilliselle karanteenialuelle, josta se on vastaanottajan luettavissa tai muutoin saattaa vastaanottajan tietoon kohtuullisen ajan kuluessa viestin vastaanottamisesta.

12. Viivästäminen

Organisaatiolla on oikeus tarvittaessa viivästää viestien toimittamista kohtuullisen ajan tunnistaakseen mahdolliset liikenteen mukana tulevat haittaohjelmat.

13. Muuta

Organisaation tulee palomuurikonfiguraatiossaan tai muutoin, mahdollisuuksiensa mukaan, estää sähköpostin lähettäminen muihin toimialueisiin muiden kuin virallisten postipalvelimiensa kautta.

Postin suodatusta on mahdollista tehdä sähköpostiasiakkaaseen asennettavassa lisäohjelmassa, keskitettyssä suodatuspalvelimessa tai yhdyskäytävässä. Suodatusohjeen kohdat 1–8 suositellaan tehtäväksi jo sähköpostiyhdyskäytävässä, kohta 9 keskitetyssä suodatuspalvelimessa ja asiakkaassa, kohta 10 keskitetyssä suodatuspalvelimessa sekä kohta 11 keskitetyssä suodatuspalvelimessa ja / tai asiakkaassa.

Suodatussuosituksen tekohetkellä ei-suositeltaviksi suodatusmenetelmiksi katsottiin sellaiset menetelmät, jotka olennaisesti rajoittavat sähköposti-arkkitehtuurin luontaista avoimuutta, esim. challenge/response, graylisting tai jotka ovat vielä toistaiseksi kokeellisessa käytössä, esim. RMX, SPF, DMP. Edellisten käyttö on hyväksyttävää arviointimielessä, mutta niitä ei tulisi käyttää pääasiallisina suodatusmenetelminä.

Sähköpostipalvelua tarjoavan organisaation tulee huolehtia siitä, että sähköpostitoimialueen ylläpitoon liittyvät sähköpostiosoitteet ovat olemassa ja että ne ohjautuvat oikealle taholle. Tällaisia osoitteita ovat mm. postmaster@toimialue.fi ja abuse@toimialue.fi.

Tiedon organisaation käyttämistä suodatusmenetelmistä tulee aina olla julkisesti saatavilla.

Sähköpostin käsittelysäännöt

Organisaation johto on vahvistanut säännöt XX.X.200X. Säännöt tulevat voimaan X.X.200X.

1. Yleistä

Sähköisten asiakirjojen käsittelyssä sovelletaan organisaatiossa kirjesalaisuuden, yksityisyyden suojan ja hyvän hallintomenettelyn periaatteita samalla tavalla kuin muussakin virallisten asioiden hoidossa. Käyttäjiä koskevat vaitiolovelvollisuudet ja hyväksikäyttökiellot on kuvattu myöhemmin tässä dokumentissa sekä [Tietojärjestelmien käytön säännöissä] ja [Tietojärjestelmien ylläpitosäännöissä].

Sähköpostiviestin perillemenosta varmistuminen on lähettäjän vastuulla. Sähköisessä asioinnissa lähettäjä voi varmistua viestin perille saapumisesta viranomaisen lähettämästä kuittauksesta viestin vastaanottamisesta.[1]

Organisaatiolla on oikeus määrätä, mihin sähköpostia ja tietoverkkoa käytetään, ja käyttöoikeuksia voidaan rajoittaa puhelinsoiton estojen tapaan.

Sähköpostijärjestelmää ei ole tarkoitettu tiedostojen massajakeluun eikä suurten tiedostojen välittämiseen.

Ohjeet ja suositukset sähköpostin käsittelyssä huomioitavista asioista perustuvat voimassaolevaan lainsäädäntöön, valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI, http://www.vm.fi/vahti) ohjeisiin sähköpostin käsittelystä.

Tämä sääntö ja muita ohjeita organisaation tietojärjestelmien käytöstä on saatavilla organisaation www-palvelimelta [URL] sekä [MISTÄ PAPERILLA].

2. Sähköpostiviestien ja -osoitteiden määritelmät sekä käsittely

2.1 Määritelmät ja käyttötarkoitukset

Sähköpostiviestit on tässä säännössä jaettu neljään eri luokkaan sen mukaisesti millaiseen osoitteeseen ne liittyvät. Säännössä sekä lähetetyt että vastaanotetut viestit määritellään seuraavasti:

[1] Sähköisellä asioinnilla tarkoitetaan hallintoasiain sähköistä vireillepanoa ja sen täydentämistä, käsittelyä (ml. ratkaisu) ja päätöksen tiedoksiantoa tai oikeudenkäyntiasiakirjan lähettämistä sähköisenä viestinä yleiselle tuomioistuimelle tai sen määräämälle henkilölle.

- organisaation sähköpostiviesti on organisaation tai yksikön organisaatio-osoitteeseen (esim. kirjaamo@[DOMAIN.fi,valinta@DOMAIN.fi]) liittyvä viesti.
- virkasähköpostiviesti liittyy sekä organisaation työntekijälle työkäyttöön antamaan henkilökohtaiseen virkasähköpostiosoitteeseen (esim. vili.virta@DOMAIN.fi) että työntekijän työtehtäviin.
- henkilökohtainen sähköpostiviesti on organisaation antamaan sähköpostiosoitteeseen (yleensä sama kuin virkasähköpostiosoite) liittyvä henkilökohtainen viesti.
- muu sähköpostiviesti on käyttäjän organisaation ulkopuoliseen sähköpostiosoitteeseen esim. vili.virta@omakaytto.fi tai vili.virta@muuorganisaatio.fi) liittyvä viesti.

[Virka- ja henkilökohtaiset sähköpostiosoitteet muodostuvat käyttäjän nimestä. Muotoon etunimi.sukunimi@DOMAIN.fi tekevät poikkeuksen samannimiset henkilöt, joiden kaikkien osoitteisiin lisätään erotteleva osa. Myös sähköpostiviestin lähetysosoitteen tulee olla joko organisaatio-osoite tai nimimuotoinen virkasähköpostiosoite].

Luonnollisen henkilön sähköpostiosoite on henkilötietolain (523/1999) mukaan henkilötieto. Henkilötiedot on rekisteröity organisaation henkilötietorekistereihin, joista on laadittu henkilörekisteriselosteet. Henkilötietoja käsitellään organisaatiossa henkilörekisteriselosteiden mukaisella tavalla ja tarkoituksessa.

Organisaatiolla ja sen yksiköillä tulee virallisten asioiden hoitoa ja palveluiden tarjoamista varten olla organisaatio-osoitteet (esim. kirjaamo@[DOMAIN.fi tai humanistinen.tiedekunta@DOMAIN.fi]). Organisaation palveluita tulee lähestyä ensisijaisesti organisaatio-osoitteiden, eikä yksittäisten työntekijöiden virkasähköpostiosoitteiden kautta.

2.2 Sähköpostiosoitteiden julkaiseminen

Julkaisemisella tarkoitetaan sähköpostiosoitteen ilmaisemista muun muassa organisaation puhelinluettelossa tai muussa julkaisussa, organisaation julkisilla www-sivuilla, käyntikortissa ja hakemistopalvelussa.

Organisaatio julkaisee organisaatio-osoitteet sekä työntekijöidensä virkasähköpostiosoitteet, niiltä osin kuin se on tarpeen palveluiden käytön ja tehtävien hoidon kannalta. Organisaatio ei julkaise organisaation ulkopuolisia sähköpostiosoitteita.

[Sähköpostiosoitteena tulee käyttää aina nimimuotoista osoitetta niin sähköpostiohjelmien asetuksissa kuin muutoinkin osoitetta julkaistessa].

2.3 Organisaation sähköpostiviestien käsittely

Jokaiselle organisaatio-osoitteelle tulee nimetä vähintään yksi vastuuhenkilö. Organisaation tulee huolehtia osoitteeseen saapuvien viestien säännöllisestä käsittelystä.

Organisaatiosähköpostin välittäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen on kiellettyä tietosuojan ja tiedonhallinnan vuoksi.

Jos saapuneessa viestissä on kuittauspyyntö, lähetetään kuittausviesti ilman tarpeetonta viivettä. Sähköisessä asioinnissa viranomaisen on viipymättä ilmoitettava sähköisen asiakirjan vastaanottamisesta lähettäjälle kuittausviestillä. Automaattikuittauksia ei tule käyttää muissa kuin erityisesti sitä varten suunnitelluissa asiointijärjestelmissä.

Työntekijän lähettämästä organisaation vastauksesta tulee ilmetä, että se on lähetetty vastauksena organisaatio-osoitteeseen tulleeseen viestiin. Vastauksessa on myös korostettava tai asetettava paluuosoite siten, että yhteydenotot jatkossakin tapahtuvat organisaatio-osoitteeseen.

Tarvittaessa sähköpostiviestiin voidaan lisätä luottamuksellisuutta osoittava lopputeksti (malli liitteenä 1).

Organisaation sähköpostiviestejä käsitellään lain viranomaisten toiminnan julkisuudesta (julkisuuslain, 621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa, mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta. Lisätietoja julkisen hallinnon sähköpostisuosituksesta JHS 132 (http://www.intermin.fi/juhta).

Organisaation sähköpostiviestejä käsitellään ja ne arkistoidaan tarvittaessa arkistonmuodostussuunnitelmassa ilmenevällä tavalla.

2.4 Virkasähköpostiviestien käsittely

Virkasähköpostin välittäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen on kielletty tietosuojan ja tiedonhallinnan vuoksi.

Organisaatio kohtelee virkasähköpostiosoitteella toimitettua viestiä pääsääntöisesti vastaanottajalle osoitettuna henkilökohtaisena viestinä, koska vastaanottaja ei voi estää henkilökohtaisten viestien saapumista.

Työnantajan oikeudesta hakea esille tai avata työntekijälle lähetettyjä tai tämän lähettämiä sähköpostiviestejä (HE 162/2003, XXX/2004) säädetään tarkemmin luvussa 4.3

Jos saapuneessa viestissä on kuittauspyyntö, lähetetään kuittausviesti ilman tarpeetonta viivettä. Sähköisessä asioinnissa viranomaisen on viipymättä ilmoitettava kuittausviestillä lähettäjälle sähköisen asiakirjan vastaanottamisesta. Kuittausviestin lähettää asiaa käsittelevä henkilö, automaattikuittauksia ei tule käyttää. (Automaattikuittauksista säädetään tarkemmin luvussa 4.1).

Työntekijän lähettämästä virkasähköpostiviestistä tulee ilmetä, että sen lähettäjä on viranomainen, ei yksittäinen työntekijä, esim. liittämällä allekirjoitukseen asema ja yksikön nimi. Mikäli kysymyksessä on hakemus tms. viranomaistoimenpiteitä edellyttävä toimenpide, tulee paluuosoite asettaa siten tai muistuttaa asiakasta siitä, että jatkoyhteydet hoidetaan organisaatio-osoitteen kautta.

Tarvittaessa sähköpostiviestiin voidaan lisätä luottamuksellisuutta osoittava lopputeksti (malli liitteenä 1).

Virkasähköpostiviestejä käsitellään lain viranomaisten toiminnan julkisuudesta (julki-

suuslain, 621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta.

Virkasähköpostiviestejä käsitellään ja ne arkistoidaan tarvittaessa arkistonmuodostamissuunnitelmassa ilmenevällä tavalla.

2.5 Henkilökohtaisten sähköpostiviestien käsittely

Työntekijän henkilökohtaiset viestit tulee erottaa selvästi organisaatiolle kuuluvista viesteistä. Työntekijän tulee siirtää virkasähköpostiosoitteeseensa tulevat henkilökohtaiset viestit välittömästi omiin kansioihinsa, joiden nimestä yksityisyys on nähtävissä (private, yksityisasiat tms.). Tämä koskee sekä saapuvia että lähteviä viestejä.

Organisaation sähköpostiosoitteen käyttö työntekijän henkilökohtaisiin tarkoituksiin on luvallista vähäisessä määrin ja siten, että se ei haittaa organisaation toimintoja. Kuitenkin käyttö kaupalliseen tai poliittiseen tarkoitukseen, kuten yksityiseen yritystoimintaan tai organisaation ulkopuolisten vaalien ehdokasmainontaan, on ehdottomasti kiellettyä lukuunottamatta henkilökunnan ammattiyhdistysten toimintaa.

Ketjukirjeitä tai massapostituksia ei saa lähettää organisaation sähköpostipalvelimilla. Organisaation tarve laajaan tiedotukseen organisaatioyhteisön jäsenille harkitaan tapauskohtaisesti.

2.6 Muiden sähköpostiviestien käsittely

Organisaation ulkopuolinen sähköpostiosoite (eli muu osoite kuin @[DOMAIN.fi]) on yksityisasia, jota ei tässä tarkemmin ohjata. Työntekijä ei saa käyttää organisaation ulkopuolista sähköpostiosoitetta organisaatioon liittyviin työtehtäviin.

Organisaation ulkopuoliseen sähköpostiosoitteeseen liittyvillä käyttäjätunnuksilla ei saa käyttää samoja salasanoja kuin organisaation tarjoamilla käyttäjätunnuksilla.

Organisaation ulkopuolisen sähköpostiosoitteen ja –palvelun käyttöä organisaation työasemilta käsin ei suositella.

3. Erityistoimenpiteitä edellyttävät viestit

3.1 Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen

Organisaatiolla on oikeus ohjelmallisesti tarkistaa sähköpostiviestit ja niiden liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta sekä rajoittaa mahdollisesti haitallisten tai liian suurien liitetiedostojen vastaanottamista ja lähettämistä. Organisaatiolla on oikeus myös poistaa viruksia ja muita haittaohjelmia sisältävät viestit ja liitetiedos-

tot. Organisaation ei tarvitse tiedottaa yksittäisen viestin suodattamisesta tai tuhoamisesta viestin lähettäjälle. Suodatus tapahtuu sähköpostijärjestelmässä automaattisesti. Käyttäjille tiedotetaan näistä rajoituksista sähköpostin suodatusohjeessa.

3.2 Roskapostiviestien käsittely

Roskapostilla tarkoitetaan tarkemmin määrittelemättömälle vastaanottojoukolle suunnattuja massapostituksia. Organisaatio saa estää roskapostin vastaanottamisen.

Organisaatio vähentää käyttäjiensä roskapostiongelmaa suodattamalla viestit, jotka saapuvat tunnetuista roskapostia välittävistä palvelimista tai jotka luokitellaan roskapostiksi otsikkotietojensa tai automaattisen sisältöanalyysin perusteella. Esto toteutetaan teknisin menetelmin sähköpostipalvelussa. Organisaatio voi myös tuhota suodatetut viestit käyttäjän puolesta.

Organisaation ei tarvitse tiedottaa yksittäisen roskapostiviestin suodattamisesta tai tuhoamisesta viestinnän osapuolille tai palauttaa tuhottua viestiä lähettäjälle. Suodatuksessa käytetyistä metodeista organisaatio tiedottaa [sähköpostin suodatusohjeessaan].

Roskapostiin ei pidä vastata, koska näin vain lisätään roskapostin saapumista. Vastaamalla osoittaa sähköpostiosoitteensa toimivaksi, ja se lisätään roskapostittajien osoitelistoille.

Käyttäjä voi ilmoittaa häiritsevästä roskapostista ylläpitohenkilöstölle tai atk-tukihenkilölle. Käytännössä ylläpito voi pyrkiä puuttumaan vain Suomesta lähetettyihin viesteihin.

3.3 Perille menemättömän sähköpostiviestin käsittely

Sähköpostiviestin lähettäjällä on vastuu viestin luettavuudesta, viestin perillemenosta, mahdollisen määräajan ylittymisestä ja muista näihin verrattavista seikoista, kunnes hän on saanut tiedon viestin onnistuneesta perillemenosta.

Mikäli saapuvan viestin osoite ei ole sähköpostijärjestelmän tiedossa, lähetetään viestin lähettäjälle automaattisesti virheilmoitus. Ilmoitus lähetetään lähettäjälle myös, jos vastaanottajan sähköpostin tilakiintiö on täynnä. Käyttäjät vastaavat itse tilakiintiöstään.

Lähetys- ja palautusvelvollisuudet eivät koske haittaohjelmaviestejä eivätkä roskapostia.

3.4 Väärään osoitteeseen saapunut sähköpostiviesti

Mikäli käyttäjä saa toiselle henkilölle tarkoitetun sähköpostiviestin, käyttäjällä on vaitiolovelvollisuus ja hyväksikäyttökielto niin viestin sisällöstä kuin olemassaolostakin.

Toiselle henkilölle (esimerkiksi kaimalle) tarkoitettu sähköpostiviesti on ohjattava edelleen oikeaan osoitteeseen, jos osoite on tiedossa. Mikäli osoitetta ei ole tiedossa, on

viestin vastaanottajan lähetettävä alkuperäiselle lähettäjälle tieto epäonnistuneesta toimituksesta ja hävitettävä saapunut viesti.

Organisaation tai virkamiehen toimivaltaan kuulumaton, ilmeisestä erehdyksestä tai tietämättömyydestä lähetetty sähköpostiviesti on siirrettävä hallintolain (434/2003) 21 §:n mukaisesti toimivaltaiseksi katsotulle viranomaiselle, jos se on tiedossa; siirrosta on ilmoitettava viestin lähettäjälle. Ellei siirto ole mahdollinen, viesti palautetaan ja hävitetään organisaation palvelimilta.

Lähetys- ja palautusvelvollisuudet eivät koske haittaohjelmaviestejä eivätkä roskapostia.

4. Sähköpostin käsittely erityistilanteissa

4.1 Automaattiset vastaukset viesteihin

Automaattisten vastausten käyttöä ei suositella. Jos automaattivastaus kuitenkin katsotaan välttämättömäksi (esimerkiksi työntekijöiden pitkät lomat tai virkavapaudet tai palvelussuhteen päättyminen), tulee siinä kehottaa lähettäjää ottamaan yhteyttä ensisijaisesti sopivaan organisaatio-osoitteeseen.

4.2 Palvelussuhteen päättyminen

Henkilön käyttöoikeus organisaation antamaan sähköpostiosoitteeseen päättyy palvelussuhteen tai opiskeluoikeuden päättyessä. Organisaation ulkopuolisten henkilöiden käyttöoikeuksien voimassaolosta vastaa käyttöoikeutta puoltaneen yksikön esimies. Käyttöoikeuden päättymisen jälkeen organisaatio ei ota vastaan henkilölle lähetettyjä viestejä vaan ilmoittaa automaattisesti lähettäjälle osoitteen toimimattomuudesta.

Ennen palvelussuhteen päättymistä työntekijän tulee ilmoittaa viestintäkumppaneilleen sähköpostiosoitteensa poistumisesta ja poistaa henkilökohtaiset viestinsä. Muut viestit jäävät organisaation haltuun. Jos työntekijä lakkaa hoitamasta tehtäviään jo ennen työsuhteen päättymistä, tulee sähköpostin vastaanotto estää jo siinä vaiheessa. (Automaattisista vastauksista katso luku 4.1.)

Tarkemmat ohjeet löytyvät [erillisistä ohjeista].

4.3 Menettelysäännöt työntekijän ollessa väliaikaisesti poissa

Kun kyse on ennakoidusta poissaolosta, työntekijän ja esimiehen on huolehdittava työntekijän sähköpostin asianmukaisesta hoidosta. Suositeltavin tapa on postilaatikon lukuoikeuden antaminen tehtäviä poissaolon aikana hoitavalle henkilölle pääsyoikeuslistojen avulla. (Automaattisista vastauksista katso luku 4.1.)

Organisaatiolla on oikeus lain yksityisyyden suojasta työelämässä (HE 162/2003, XXX/2004, 18-20§) asettamissa rajoissa saada käyttöönsä organisaatiolle kuuluvat, sen toiminnan jatkumisen kannalta välttämättömät viestit työntekijän estyneenä ollessa. Työntekijälle virkasähköpostiosoitteella lähetettyjen tai tämän lähettämien viestien sekä selville saaminen että niiden avaaminen perustuu ensisijaisesti työntekijän suostumukseen sekä siihen että työntekijän luottamukselliset henkilökohtaiset viestit ovat erotettavissa organisaatiolle selvästi kuuluvista viesteistä. (viestien erottelusta ks. luku 2.5).

Mikäli työntekijä ei ole antanut toiselle työnantajan hyväksymälle henkilölle suostumusta, että tämä saa etsiä ja avata työntekijän poissa ollessa tämän sähköpostiviesteistä työnantajalle kuuluvat viestit, tai vakavan sairauden takia häneltä ei voida suostumusta saada, voi hallintojohtaja määrätä henkilön esimiehen postipalvelimen pääkäyttäjän avulla selvittämään ja avaamaan työntekijän poissa ollessa yllä määritellyt virkasähköpostiviestit. Viestien etsinnän ja avaamisen syy, siihen osalliset ja ajankohta sekä kenelle avatusta viestistä on annettu tieto, on kirjattava ja ilmoitettava ilman aiheetonta viivytystä työntekijälle.

4.4 Sähköpostijärjestelmää haittaavat tai vaarantavat viestit ja postilaatikot

Sähköpostijärjestelmän ylläpidon oikeudesta puuttua sähköpostin kulkuun sähköpostijärjestelmän palvelutason tai turvallisuuden takaamiseksi säädellään tarkemmin [Tietojärjestelmien ylläpitosäännöissä].

5. Sähköpostiviestin salaus ja todentaminen

Käyttäjällä on oikeus salata sähköpostiviestinsä salausmenetelmää käyttäen.

Erittäin salaisiksi tai salaisiksi turvaluokiteltuja asiakirjoja ei saa lähettää sähköpostilla.

Muita kuin julkisia tietoja ja julkisia henkilötietoja sisältäviä asiakirjoja ei tule siirtää sähköpostina tai muuna tietoverkon yli tapahtuvana tiedonsiirtona ilman salausta.

Salassa pidettäviä henkilö- ja muita tietoja voidaan kuitenkin siirtää sähköisesti, mikäli tiedon salaukseen käytetään riittävän vahvoja salausalgoritmeja tai koko tiedonsiirtoväylää voida pitää riittävän turvallisena.

Käytettävien salausohjelmien tulee organisaatio- ja virkasähköpostiviestien osalta olla organisaation hyväksymiä ja käyttöönottamia.

Sähköpostilla vastaanotetun asiakirjan alkuperäisyys ja eheys on tarvittaessa varmistettava.

Jos virkasähköposti on salattu siten, että vain vastaanottaja voi avata sen, se on avattava välittömästi siirron jälkeen. Tarvittaessa se voidaan salata uudestaan siten, että se on

muidenkin asian käsittelijöiden avattavissa. [Velvollisuus ei koske haittaohjelmia sisältäviä viestejä eikä roskapostia].

6. Sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen

Sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen on ohjeistettu [Tietojärjestelmien ylläpitosäännöissä] ja [Lokien käsittelysäännöissä].

7. Näiden sääntöjen valvonta

Näiden sääntöjen valvonnasta vastaavat organisaation [atk-keskus, muiden mahdollisten organisaation yksiköiden sähköpostipalvelinten omistajat] sekä työnjohdollisesti esimiehet. Sääntörikkomusten käsittely tapahtuu [Tietotekniikkarikkomusten seuraamuskäytännön] mukaisesti.

Sääntöjä päivitetään tarvittaessa tai organisaatioden yhteisen sääntösuosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö].

Malli sitoumuslomakkeesta:

SALASSAPITOSITOUMUS

Sitoudun siihen, etten Viraston palveluksessa tai harjoittelijana ollessani, tai muuten laitoksessa tai sen toimeksiannosta toimiessani, paljasta sivulliselle asiakirjojen salassa pidettävää sisältöä enkä muutakaan tietoon saamaani seikkaa, josta lailla tai asetuksella on säädetty vaitiolo- tai salassapitovelvollisuus.

Lisäksi sitoudun olemaan väärinkäyttämättä tehtävieni vuoksi saamiani ei-julkisia ja salassa pidettäviä tietoja ja jättämättä niitä sivullisten nähtäville tai muuten helposti saataville.

Salassapidon piiriin kuuluvia tietoja ovat esimerkiksi liike- ja ammattisalaisuudet, henkilötiedot ja turvallisuusjärjestelyihin liittyvät tiedot. Sivullisiksi tässä yhteydessä katsotaan myös ne Virastossa tai sen yhteistyökumppaneilla työskentelevät henkilöt, jotka eivät heille määrättyjen tai sovittujen tehtävien perusteella tarvitse asiaa tietoonsa.

Palvelus- tai toimeksiantosuhteen päättyessä luovutan haltuuni annetut tai tehtävien vuoksi valmistamani Virastoa tai sen asiakkaita tai yhteistyötahoja koskevat ei-julkista tai salassa pidettävää tietoa sisältävät asiakirjat ja tietovälineet sekä niiden mahdolliset kopiot Virastolle, ellei asiasta erikseen muuta sovita. Lisäksi hävitän hallinnassani oleviin tietojärjestelmiin tallentamani vastaavat tiedot, ellei asiasta ole Viraston kanssa muuta sovittu. Vaitiolo- ja salassapitovelvollisuus on voimassa vielä palvelus- tai toimeksiantosuhteen päättymisen jälkeen.

Olen perehtynyt minulle esitettyihin, tällä hetkellä voimassaoleviin laissa säädettyihin vaitiolovelvollisuus- ja hyväksikäyttökieltosäännöksiin, Viraston tietoturvapolitiikkaan ja koko henkilöstön tietoturvaohjeisiin sekä tietosuojavelvoitteisiin. Sitoudun noudattamaan niitä samoin kuin muita erikseen annettuja ohjeita tai määräyksiä. Niiden rikkominen saattaa eräissä tapauksissa muodostaa rikokseksi katsottavan teon. Jos em. säännöksissä tapahtuu muutoksia, työnantaja tulee kertomaan niistä minulle.

Olen lukenut ja ymmärtänyt edellä kuvatun vaitiolo- ja salassapitovelvollisuuteni ja sitoudun mainittuja velvollisuuksia noudattamaan.

_____ _____

päiväys allekirjoitus

_____

nimen selvennys

Malli tarvittaessa käytettävästä luottamuksellisen sähköpostiviestin lopputekstistä:

LUOTTAMUKSELLISUUSILMOITUS

Tämä sähköpostiviesti saattaa sisältää tietoa, jonka hallintaoikeus, luottamuksellisuus ja/tai julkistaminen on rajattua sovellettavissa olevan lain mukaan.

Sisältö on tarkoitettu ainoastaan vastaanottajan käyttöön.

Jos tätä sähköpostiviestiä ei ole tarkoitettu Sinulle, sen käyttö, kopiointi, muuttaminen tai hallussapito on kiellettyä.

Jos Sinulla on syytä uskoa, että tätä viestiä ei ole tarkoitettu Sinulle, ole hyvä ja poista se ja kaikki sen kopiot laitteistostasi. Muista, että tällaisen viestin osalta olet lain mukaan vaitiolovelvollinen, etkä saa myöskään käyttää viestiä hyväksesi.

Malli suostumuksesta sähköpostiviestien lukemiseen:

SUOSTUMUS

Annan suostumukseni siihen, että

Nimetty Henkilö / Nimetyt Henkilöt

on oikeus lukea minulle lähetetyt työtehtäviin liittyvät sähköpostiviestit seuraavissa tilanteissa:

– vuosilomani aikana, sen kestäessä yli ___ päivää
– virkavapauteni, sen kestäessä yli __ päivää
– työmatkani aikana, sen kestäessä yli __ päivää
– koulutuksessa oloni aikana, sen kestäessä yli ___ päivää
– sairastettuani ja sen kestäessä yli__ päivää
– kuoltuani

Tiedän, että sillä, joka lukee minulle osoitettuja sähköpostiviestejä, on vaitiolovelvollisuus ja hyväksikäyttökielto sellaisten viestien osalta, jotka ovat tarkoitettu minulle henkilökohtaisesti.

Tiedän, että minulla on oikeus peruuttaa tämä suostumus.

päiväys

allekirjoitus

nimen selvennys

Valtiovarainministeriön ja VAHTIn voimassaolevaa tietoturvaohjeistoa

- Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005
- Information Security and Management by Results, VAHTI 1/2005
- Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004
- Datasäkerhet och resultatstyrning, VAHTI 4/2004
- Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
- Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003 (suomeksi, ruotsiksi, englanniksi)
- Valtionhallinnon tietoturvallisuuskäsitteistö, 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 4/2002
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tunnistamisperiaatteet valtionhallinnon verkkopalveluissa VM 2002
- 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 .
- 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
- 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
- Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998

VAHTI

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

2/2005

VALTIONHALLINNON SÄHKÖPOSTIEN KÄSITTELYOHJE

ISBN 951-804-515-1
ISSN 1455-2566