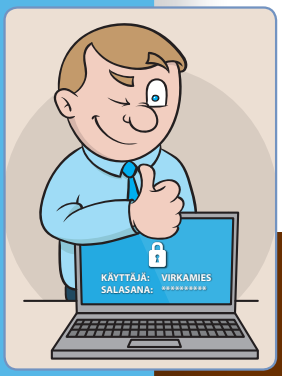
VALTIOVARAINMINISTERIÖ

Henkilöstön tietoturvaohje



4/2013

VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Henkilöstön tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2013 VAHTI

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

ISSN 1455-2566 (nid.)
ISBN 978-952-251-513-1 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-514-8 (PDF)

Juvenes Print - Suomen Yliopistopaino Oy, 2013

VALTIOVARAINMINISTERIÖ **Ohje** VM /2588/00.00.00/2013

22.11.2013

Ministeriöille, virastoille ja laitoksille

Henkilöstön tietoturvaohje

Oheisen Valtiovarainministeriön antaman henkilöstön tietoturvaohjeen tavoitteena on tukea, ylläpitää ja kehittää valtionhallinnon tietoturvallisia työskentelytapoja. Ohje korvaa aikaisemman Henkilöstön tietoturvaohjeen (VAHTI 8/2006). Ohje on osa Suomen kyberturvallisuusstrategian ja valtioneuvoston periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä toimeenpanoa.

Ohje on valtion henkilöstön tietoturvallisuuden yleisohje. Ohjeessa on tiiviisti kuvattu tietoturvallisuuden perusasiat ja siinä annetaan käytännön neuvoja tietoturvallisuuden toteuttamiseen osana henkilöstön perustyötä ja tehtävien hyvää hoitamista. Ohje tukee myös kuntien ja niiden henkilöstön tietoturvatyötä.

Valtionhallinnon organisaatioiden johdon tulee huolehtia henkilöstön tietoturvaosaamisen sekä tietoturvakulttuurin ja -tietoisuuden jatkuvasta kehittämisestä. Johdon vastuulla on varmistaa, että jokaisella työntekijällä on tehtäviensä edellyttämä tietoturvallisuuden osaaminen.

Valtionhallinnon tietoturvallisuusasetus (681/2010) edellyttää, että viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi, ja että henkilöstölle annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä. Asetus edellyttää myös, että annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Tätä ohjetta voidaan käyttää sellaisenaan tai organisaatioiden omien ohjeiden tukena. Ohje julkaistaan VAHTIn internet-sivuilla. Lisätietoja antavat tietoturvallisuusasiantuntija Aku Hilve ja vaatimusten hallinnan asiantuntija Iiro Henttinen (etunimi.sukunimi@vm.fi).

Hallinto- ja kuntaministeri — Henna Virkkunen

Yksikön päällikkö — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite — Henkilöstön tietoturvaohje (VAHTI 4/2013)

TIEDOKSI — Kunnat

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Sisältö

1 Johdanto

Tietoturvallisuus perustuu lainsäädäntöön, normiohjaukseen sekä sopimuksiin. Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle, myös sinulle. Turvallisuus ja tietoturvallisuus kokonaisturvallisuuden osana muodostuvat suurelta osin yksilöiden tekemistä valinnoista erilaisissa arkipäivän tilanteissa.

Tämä tietoturvaohje on tarkoitettu

- koko julkishallinnon henkilöstölle noudatettavaksi niin työvälineiden kuin palveluiden käytössä,
- julkishallinnon toimeksiannosta työskenteleville (esim. palvelutoimittajat) ja
- julkishallinnon tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. harjoittelijat, opiskelijat).

Ohjetta voidaan soveltaen käyttää myös muissa kuin julkishallinnon organisaatioissa.

Ohjeeseen on koottu keskeisimmät tietoturvallisuuden perusasiat. Se antaa neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Tätä ohjetta tukemaan on kehitetty sähköinen verkkokoulutus, jonka tarjoaa Valtion IT-palvelukeskus. Toistaiseksi koulutus on tarkoitettu vain valtionhallinnon organisaatioille. Voit kysyä sen käytöstä oman organisaatiosi tietoturvavastuuhenkilöltä.

Kun saat hyvän idean tietoturvallisuuden parantamisesta, tee siitä aloite organisaatiosi tietoturvavastaavalle tai omalle esimiehellesi!

Tietoturvallisuus ja jatkuvuuden hallinta ja varautuminen ovat osa suurempaa turvallisuus-kokonaisuutta.

2 Tietoturvallisuuden ohjeet pähkinänkuoressa

2.1 Tiedottaminen ja koulutus

- Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.
- Noudata organisaatiosi tietoturvaohjeita.

2.2 Toimitilaturvallisuus

- Noudata organisaatiosi kulunvalvontaohjetta. Pidä kuvallinen henkilökorttisi tai muu sinulle annettu tunniste aina esillä.
- Tarkista ilman henkilö- tai vierailijatunnistetta olevien henkilöiden kulkuoikeus tiloissa.
- Ohjaa ilman kulkuoikeutta olevat henkilöt ulos.
- Älä jätä työvälineitä valvomatta neuvottelutiloihin.
- Älä jätä vieraita yksin neuvottelu- tai työtiloihin. Saata vieraat aulaan tai ulos kokouksen jälkeen.

2.3 Päätelaitteet

Päätelaitetta (kannettava tietokone, pöytäkone, älypuhelin, tabletti jne.) käytetään yhä useammin maksu- ja tunnistautumisvälineenä. Suojele sitä kuten lompakkoasi.

- Älä anna ulkopuolisen henkilön, edes tutun, käyttää päätelaitettasi.
- Estä päätelaitteesi, esimerkiksi puhelimen, luvaton käyttö asettamalla siihen laitteen käyttöohjeen mukaiset automaattiset lukitukset.

2.4 Tietoaineistojen käsittely

- Merkitse asiakirjaan sen salassapidosta kertova tunniste. Niitä ovat mm. ”salassa pidettävä”, ”suojaustaso” ja ”turvaluokiteltu”. Noudata asiakirjojen merkitsemisessä oman organisaatiosi ohjeistusta.
- Käsittele (mm. tallenna, siirrä, tulosta, lähetä, kopioi, kuljeta, säilytä, arkistoi, hävitä) salassa pidettäviä tietoja organisaatiosi antamien ohjeiden mukaisesti.
- Salassa pidettävää tietoa voidaan tallentaa, siirtää ja arkistoida usealla eri tallennusvälineellä ja tavalla. Noudata tietoaineistojen ja tallennusvälineiden hävittämisessä organisaatiosi ohjeita. Selvitä, missä sijaitsevat lähimmät salassa pidettävän materiaalin hävittämiseen tarkoitetut tietoturvalliset säiliöt.
- Noudata tulostamisessa ja tulosteiden noutamisessa organisaation antamia ohjeita. Selvitä mahdollisuus tietoturvalliseen tulostukseen PIN-koodilla, kun tulostat arkaluontoisia ja salassa pidettäviä asiakirjoja.
- Ole erityisen varovainen työskennellessäsi julkisissa tiloissa ja huomioi, että joku voi nähdä syöttämiäsi tunnuksia tai muita tietoja huomaamattasi tai salakuunnella keskusteluitasi.
- Julkista tietoa voi välittää internetin kautta tavallisella salaamattomalla sähköpostilla. Salassa pidetävän tiedon välittämisessä internetin kautta on käytettävä turvasähköpostia.
- Älä anna ulkopuolisten nähdä tietokoneesi näyttöruutua, kun käsittelet salassa pidettävää tietoa, tai näppäimistöä, kun syötät käyttäjätunnuksia ja salasanoja. Pyri käyttämään päätelaitteissasi tietoturvakalvoa

2.5 Tunnukset ja salasanat

Pankkiautomaatillakin suojaat tunnuslukusi ja tarkkailet ympäristöäsi. Noudata vastaavaa varovaisuutta työpaikallasi ja erityistä varovaisuutta sen ulkopuolella.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi toisen henkilön käyttöön. Älä edes tietohallintohenkilöstölle, koska he eivät tarvitse niitä työtehtäviensä hoitamiseen.
- Käytä eri salasanaa eri palveluissa – työkäyttöön liittyviä tunnuksia tai salasanoja ei saa koskaan käyttää vapaa-ajan palveluissa.
- Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja, jotka ovat mahdollisimman pitkiä. Vaihda salasanasi silloin kun sitä edellytetään tai kun epäilet sen paljastuneen.
    - Vahvassa salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Se on helppo muistaa, mutta vaikea arvata.

2.6 Työvälineiden ja internetin käyttö

- Käytä työhösi liittyviä tietoaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen.
- Älä selaa sellaisia www-sivustoja, jotka eivät liity työtehtäviisi. Sivujen kautta saatetaan yrittää siirtää päätelaitteeseesi haitta- tai vakoiluohjelmia.
- Ole varovainen – valitse tarvittaessa ”Peruuta”, jos www-sivu ei vaikuta luotettavalta ja sivusto ehdottaa tai edellyttää tiedoston lataamista tietokoneellasi! Pyydä tarvittaessa apua.
- Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi.
- Käytä vain organisaatiosi tietohallinnon hyväksymiä muistitikkuja tai muita lisälaitteita.
- Salaamaton muistitikku soveltuu vain julkisen tiedon siirtämiseen.
- Salatulla muistitikulla voit siirtää salassa pidettäviä tietoaineistoja vain organisaatiosi tietoaineistojen käsittelyohjeistuksen mukaisesti.
- Lahjaksi saatuja tai löydettyjä muistitikkuja ei saa liittää päätelaitteeseen.

- Tallenna laatimasi asiakirjat organisaatiossa ohjeistetulla tavalla sellaiseen paikkaan, josta tiedot varmistetaan keskitetysti.

Huom! työpöydällä olevat kuvakkeet, kansiot ja tiedostot eivät kuulu varmuuskopioinnin piiriin.

2.7 Sosiaalinen media

Muista, että aina kun käytät oman työorganisaatiosi laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa organisaatiosi edustajana.

- Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.
- Käsittele palveluissa vain sellaista tietoa, jonka käyttöön palvelu on organisaatiossasi hyväksytty (huomioi mikä tieto on julkista, mikä salassa pidettävää).
- Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.
- Käytä työsähköpostia vain työtehtäviesi hoitamiseen. Käytä muuhun kuin työtehtävien hoitamiseen vapaa-ajan sähköpostiasi.

Tiedätkö, mitä tietoa sinusta on kertynyt sosiaalisen median palveluihin?

- Hae tietoja nimelläsi ja säädä palveluiden yksityisyydensuoja-asetuksia tarvittaessa tiukemmiksi.
- Tarkista erityisesti sosiaalisen median verkkopalveluissa yksityisyyden suojaa koskevat asetukset. Muuta käyttäjäprofiilisi suojausasetuksia tarvittaessa siten, etteivät tietosi näy tai leviä laajemmalle kuin haluat. Testaa eri vaihtoehtoja yksityisyyden suojaa koskevissa asetuksissa. Voit pyytää samaa palvelua käyttävää kaveria tarkistamaan miltä tietosi ja profiilisi näyttävät.

2.8 Havaitsitko ongelman?

- Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan. Älä luota siihen, että joku muu ilmoittaa tai korjaa ongelman.
- Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietoturvavastaavalle tai esimiehellesi. Heidän velvollisuutenaan on ryhtyä toimenpiteisiin.

Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi. Peruskäyttäjänä sinulla näitä oikeuksia ei tulisi olla. Jos huomaat, että sinulla on johonkin palveluun tai toimintoon liikaa oikeuksia, velvollisuutesi on pyytää niiden korjaamista.

3 Tietoturvallisuus – mitä se on?

3.1 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuus on osa organisaation toiminnan laatua.

Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon.

Käytännössä tämä merkitsee mm. sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään.

Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, tapahtumien tai häiriötilanteiden vuoksi.

Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin kun niitä tarvitaan. Etenkin sähköisissä asiointipalveluissa tarve käyttää palveluita ympärivuorokautisesti ja paikasta riippumatta on lisääntynyt, kun virkamiesten ja kansalaisten käyttötavat ovat muuttuneet. Palveluiden täytyy kyetä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tarvittavaa lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää.

3.2 Miksi tietoturvallisuus on tärkeää?

Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Siksi tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys.

Yhteiskunnan toiminnot ovat suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta. Verkottuneessa toimintaympäristössä harva organisaatio on enää vastuussa yksinomaan omasta tietoturvallisuudestaan.

Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen sekä muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin.

Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki. Tämä ei koske vain tekniikkaa, vaan myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat – vahvin lenkki on oikealla tavalla toimiva yksilö!

Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta.

Mitä paremmin häiriötilanteiden hallinta on otettu huomioon organisaation toiminnassa, sitä nopeammin toiminta saadaan palautettua vakiotasolle ja tiedotettua häiriöstä asiakkaille.

3.3 Lainsäädäntö tietoturvallisuuden perustana

Julkishallinnossa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Julkisuuslainsäädännön mukaan tieto on julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole erikseen määrätty salassa pidettäväksi.

Suomen lainsäädännössä on paljon tietoturvavelvoitteita – toisin sanoen myös lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin muihin lakeihin. Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) määrätään tietoaineistojen käsittelystä sekä perus-, korototetun ja korkean tietojenkäsittely-ympäristön toteuttamisesta. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Tietojen lainmukaisesta käsittelystä on aina huolehdittava.

Joitakin keskeisiä laeissa asetettuja tietoturvavelvoitteita ovat:

- "Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä." (Laki viranomaisten toiminnan julkisuudesta 18 §, Hyvä tiedonhallintatapa)
- "Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä." (Henkilötietolaki 32 §, Tietojen suojaaminen)
- "Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot voidaan luokitella sen mukaan, minkälaisia tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelu voidaan suorittaa myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoi-

menpiteet ovat suojattavan edun vuoksi tarpeen." (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 8 §, Luokituksen perusteet)

Tietoturvallisuuteen keskeisesti liittyvien säädösten luettelo on listattu tämän ohjeen liitteessä 1.

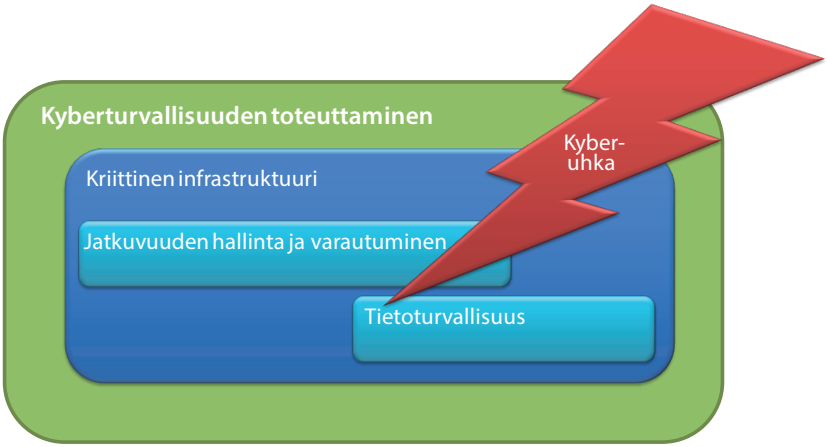
3.4 Kyberturvallisuus keskittyy yhteiskunnan toimivuuden takaamiseen

Suomen kyberturvallisuusstrategia julkaistiin tammikuussa 2013. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa sähköisessä muodossa olevaan tiedonkäsittelyyn tarkoitettuun, yhdestä tai useammasta tietojärjestelmästä koostuvaan, palveluun tai ICT-järjestelmään voidaan luottaa ja jossa sen toiminta turvataan (= kybertoimintaympäristö). Tämä edellyttää myös sitä, että tiedonkäsittelyyn liittyvät fyysiset rakenteet suojataan tarkoituksenmukaisesti.

Kyberturvallisuus keskittyy ensisijaisesti yhteiskunnan toimivuuden kannalta elintärkeiden toimintojen kokonaisvaltaiseen suojaamiseen (esimerkiksi sähkönjakelu, kriittisten tietoliikenneyhteyksien ylläpito), kun tietoturvallisuus keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen.

Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on hallita ennakoivasti ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia. Kyberuhkien toteutuminen voi aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.

Kyberturvallisuuteen liittyy myös sotilaallista tiedustelu- ja vaikuttamiskykyä, joka tarkoittaa kyberpuolustuksen kehittämistä osana muun sotilaallisen voimankäytön kehittämistä. Tästä päävastuu on puolustusvoimilla.



Siinä missä tietoturvallisuus keskittyy tietoaineistojen suojaamiseen, kyberturvallisuus kattaa kaiken infrastruktuurin tuottamisessa tarvittavat osa-alueet. Pääpaino kyberturvallisuuden puolella on tietoverkkojen kautta tulevien uhkakuvien pienentämisessä ja torjumisessa. Lisätietoa löydät esimerkiksi yhteiskunnan turvallisuusstrategiasta ja Suomen kyberturvallisuusstrategiasta.

3.5 Kohdistetut hyökkäykset

Viestintävirasto on tiedottanut kohdistetuista hyökkäyksistä 5.8.2011 Tietoturva nyt -artikkelissa seuraavaa:

”Kohdistettu hyökkäys on tiettyyn toimijaan tai toimijajoukkoon suunnattu kohteen erityispiirteet huomioiva tietoturvaloukkaus. Hyökkääjä valikoi kohteensa tarkasti tämän hallussa olevien tietoaineistojen tai muiden vastaavien seikkojen perusteella. Hyökkääjän motiivina voi olla esimerkiksi yritysten tai valtioiden arkaluontoisten tietojen varastaminen. Kohteiden valikoimisesta johtuen hyökkäyksestä voi aiheutua merkittäviä vahinkoja.

Kohdistettu hyökkäys käynnistyy usein lähettämällä kohteelle räätälöity sähköpostiviesti. Sähköpostissa on haitallista koodia sisältävä liitetiedosto tai linkki haittaohjelmaa levittävälle web-sivustolle. Jos käyttäjä avaa liitetiedoton tai seuraa linkkiä, voi haittaohjelma saastuttaa hänen koneensa. Asennuttuaan haittaohjelma ottaa yhteyden hyökkääjän ylläpitämään haittaohjelman ohjaamiseen

käytettävään komentopalvelimeen. Tämän jälkeen hyökkääjällä on käytännössä suora tietoliikenneyhteys hyökkäyksen kohteena olevaan tietokoneeseen. Hyökkääjä voi kerätä tietoja kohteen tietokoneelta ja mahdollisesti laajentaa hyökkäystä kohteen sisäverkon muihin osiin. Joissain tapauksissa hyökkäyksiä on yritetty ulottaa julkisesta verkosta irrallisiin tietokoneisiin saastuttamalla tiedonsiirtoon käytettyjä USB-tikkuja.

Hyökkääjä pyrkii räätälöimään sähköpostiviestin sellaiseksi, että vastaanottaja pitää viestiä mahdollisimman luotettavana ja päivittäiseen toimintaan liittyvänä. Usein sähköpostin lähettäjätiedot on väärennetty siten, että viesti näyttäisi tulevan kohteen kollegalta tai muulta luotetulta osapuolelta. Joissakin hyökkäyksissä on myös hyödynnetty luotetuilta tahoilta kaapattuja sähköpostitilejä. Hyökkääjä voi myös yrittää huijata vastaanottaja avaamaan liite lähettämällä ensin vaarattoman tiedoston liitteenä ja heti perään ”korjatun”, esim. haittaohjelmaa sisältävän PDF-tiedoston.”

Miten kohdistetun hyökkäyksen voi välttää?

- ole erityisen varovainen, jos saat vieraskielisen sähköpostiviestin, jonka mukana on liitetiedosto tai linkki ulkoiselle www-sivustolle, vaikka lähettäjä olisi hyvin tuntemasi henkilö, vaikka viestin asiasisältö vaikuttaa tai liitetiedoston nimi ja tyyppi vaikuttavat työtehtäviisi liittyviltä
- uusimmat kohdistetut hyökkäykset tapahtuvat suomenkielellä, joten ole huolellinen aina avatessasi organisaation ulkopuolelta saapuvia myös suomenkielisiä liitetiedostoja
- pyydä tarvittaessa organisaatiosi tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista – noudata tässä organisaatiosi ohjeistusta.

3.6 Sosiaalinen media ja tietoturvallisuus

Sosiaalisen median verkkopalveluita (esimerkiksi Facebook, Twitter, LinkedIn) hyödynnetään aktiivisesti julkishallinnossa. Niihin osallistutaan joko organisaation nimissä, virkamiehen tai yksityishenkilön roolissa.

Sosiaalisen median palvelut sisältävät samanlaisia uhkia ja riskejä kuin muutkin perinteiset internetin kautta käytettävät palvelut, mutta erityisesti tietosuojaan, henkilön yksilöivään tietoon liittyvät asiat nousevat näissä palveluissa esille.

Noudata seuraavia Sosiaalisen median tietoturvaohjeen (VAHTI 4/2010) ohjeita:

1. Selvitä ja noudata organisaatiosi sosiaalisten medioiden käyttöpolitiikkaa.
2. Jos epäilet, että olet joutunut huijatuksi tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua. Älä jätä tekemättä asiasta rikosilmoitusta, vaikka taloudellinen menetys saattaa osaltasi jäädä vaatimattomaksi.
3. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin organisaatiosi (epävirallisena) edustajana. Muista käyttäytyä sen mukaisesti!
4. Varo syöttämästä liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia itsestäsi. Huomaa, että palvelun tarjoaja voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti. Tutustu huolellisesti käyttämiesi palveluiden sopimusehtoihin.
5. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle.
6. Kunnioita perheesi ja ystäviesi suhtautumista sosiaalisiin medioihin. Vaikka olisit itse niistä innostunut, eivät kaikki sitä kuitenkaan ole. Jos kanssaihmisesi eivät halua sinun laittavan kuvia tai tietoa heistä sosiaaliseen mediaan, noudata heidän toiveitaan.
7. Älä hyväksy tuntemattomia yhteydenottoyrityksiä verkostoosi äläkä napsauta vieraita, hämäräperäisiä linkkejä.
8. Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa. Ole erityisen huolellinen salassa pidettävän tiedon suhteen. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon.

Sosiaalinen media on ensisijaisesti tarkoitettu julkisten asioiden käsittelyyn ja keskusteluun.

4 Asianhallinta ja tietojen käsittely

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

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

Tiedolla tarkoitetaan tässä yhteydessä eri muodoissa talletettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai puhelimen muistissa, ääni- tai kuvanauhassa tai vaikkapa yksittäisen ihmisen muistissa. Tietoa on tarkasteltava sen koko elinkaaren ajalla, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen. Tietoja käsiteltäessä tulee huomioida, että käsiteltävät tiedot ovat usein merkittävästi arvokkaampia kuin tietojen käsittelyyn mahdollisesti liittyvä tekninen väline.

4.1 Työhön liittyvät tiedot

Valtionhallinnon viranomaisen tulee antaa henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä. (Tietoturvallisuusasetus 5 §)

- Selvitä itsellesi tietojen ja asiakirjojen luokittelu ja siihen liittyvät käyttöä, luovutusta, käsittelyä ja arkistointia koskevat säännöt ja rajoitukset.
- Ole erityisen huolellinen salassa pidettävän tiedon käsittelyssä.
- Laatiessasi salassa pidettävää asiakirjaa, vastaat sen luokittelusta ja luokittelun merkitsemisestä.
- Osa salassa pidettävästä aineistosta kuuluu turvallisuusluokittelun piiriin. Turvallisuusluokitusmerkinnän voi tehdä, jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle. Lisätietoa: tietoturvallisuusasetuksen 11 § Turvallisuusluokitusmerkintää koskevat erityissäännökset.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Tallenna tekemäsi työ mahdollisuuksien mukaan palvelimelle tai työryhmätilaan, jonka varmuuskopioinnista tietohallinto-organisaatio huolehtii. Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella päätelaitteella tai tietovälineellä, jonka varmuuskopiointi on epäsäännöllistä tai sitä ei tehdä lainkaan.
- Jos aineistoa siirretään muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti. Varo tilannetta, jossa omalla tietovälineelläsi olisi siirrettävän tiedoston lisäksi muuta aineistoa salaamattomana.
- Varo toimisto-ohjelmilla (esim. tekstinkäsittely, esitysgrafiikka, taulukkolaskenta, PDF) tehtyjen tiedostojen piiloon jääviä tietoja (ns. meta-, jäännös- ja piilotiedot) erityisesti lähettäessäsi tiedostoja organisaation ulkopuolelle tai siirtäessäsi niitä tietovälineellä. Tiedosto voi sisältää siinä aiemmin ollutta tietoa tai muuta järjestelmässä olevaa tietoa, vaikka se ei näytöllä näkyisikään.

- Tarkista organisaatiosi ulkopuolelta tuotu muistitikku, CD-/DVD-levy tai muu tietoväline haittaohjelmien torjuntaohjelmalla ennen käyttöä, ellei torjuntaohjelma suorita sitä automaattisesti.
- Jos joudut lähettämään salassa pidettävää aineistoa sähköpostilla, salaa se organisaatiosi ohjeiden mukaisesti. Varmistu vastaanottajan oikeudesta lukea aineistoa sekä sen perille menosta.
- Telekopiota (faxia) voi poikkeustapauksissa käyttää salassa pidettävän aineiston lähettämiseen. Varmistu tällöin, että vastaanottaja on paikalla.
- Vältä tulostamista ja kopiointia. Ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet (kustannus- ja ympäristövaikutusten ohella) lisäävät tiedon vääriin käsiin joutumisen vaaraa. Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen. Tulostetta noudettaessa edellytettävä PIN-koodin syöttäminen pienentää väärälle tulostimelle tulostamisen sekä asiakirjan tulostimelle unohtamisen riskejä.
- Kun hävität salassa pidettäviä tietoja, käytä aina tiedon luokituksen mukaisia silppureita tai hävittämispalveluun kuuluvia keräyssäiliöitä (tietosuojasäiliö).

4.2 Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation viestintäpolitiikan mukaisesti. Pyydä tarvittaessa apua esimieheltäsi.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoa, ota yhteys esimieheesi.

4.3 Omat tiedot ja yksityisyys

- Käytä pääsääntöisesti henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi. Hanki yksityiskäyttöön työnantajasta riippumaton vapaa-ajan sähköpostiosoite.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.
- Olet vaitiolovelvollinen myös vahingossa saamistasi viesteistä tai kuulemistasi asioista.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, sähköpostiliikenteestä ja internet-selauksesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäytöksiin voidaan puuttua.

Opettele luokittelemaan käsittelemäsi ja luovuttamasi tieto. Tutustu ja noudata organisaatiosi tietoaineiston käsittelyohjetta.

5 Työpaikalla

5.1 Päätelaitteen käyttö

Päätelaitteella tarkoitetaan tässä ohjeessa työtehtävien hoitoon tarkoitettua elektronista laitetta, joka voi olla esimerkiksi puhelin, älypuhelin, kannettava-, tabletti-, pöytätietokone tai jokin vastaava laite. Käyttö sisältää sekä päätelaitteen että verkon kautta käytettävät palvelut.

- Vastaat käyttäjänä omasta päätelaitteestasi. Ole siis huolellinen.
- Vain tietohallinto-organisaatio saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää ohjelmia laitteisiin.
- Kirjaudu laitteelle aina omilla käyttöoikeuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (Windows-työasemalla paina Windows-näppäin + L) aina kun poistut työpisteestäsi. Lisävarmistuksena tulee käyttää salasanasuojattua näytönsäästäjää. Toimi organisaatiokohtaisen ohjeistuksen mukaisesti.
- Tallenna työsi käyttäen välitallennuksia. Laajemmissa asiakirjoissa tallenna asiakirja säännöllisesti uudelle nimelle. Muista tallentaa työsi poistuessasi työpisteeltä.
- Talleta kaikki tärkeä tieto sellaiselle palvelimelle tai työryhmätilaan, josta tietohallinto ottaa säännöllisesti varmuuskopiot.
- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku tai CD-/DVD-levy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Toimi organisaatiokohtaisen ohjeistuksen mukaisesti.
- Siirrä tietokone virranhallintatilaan tai sammuta se työpäivän päättyessä, ellei muuta ole ohjeistettu esimerkiksi tietoturvapäivitysten johdosta.
- Organisaatiosi ohjeistaa omien laitteiden käyttämisestä, mikäli se on sallittua (ns. BYOD-malli).

Kannettavat päätelaitteet muodostavat suuremman riskin kuin perinteiset pöytäkoneet niin vahingossa tapahtuvan kadottamisen kuin varastamisen näkökulmasta. Huolehdi tämän takia laitteiden automaattisesta lukittumisesta. Jos kadotat laitteen, toimi organisaatiosi antamien ohjeiden mukaan; tee välittömästi ilmoitus kadonneesta laitteesta, jotta sen väärinkäyttö voidaan estää.

5.2 Käyttöoikeudet ja salasanat

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

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön – älä edes lomien aikana. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiin. Myöskään tietohallintohenkilöstö ei tarvitse tehtäviensä hoitamiseksi salasanaasi.
- Vaihda salasanasi riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä. Hyvässä salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Hyvä salasana on helppo muistaa, mutta vaikea arvata.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.
- Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa internet-palveluihin rekisteröityessäsi tai niitä käyttäessäsi.
- Jos joissain tilanteissa tai järjestelmissä on pakko käyttää yhteiskäyttöisiä tunnuksia, siitä päättää järjestelmän tai tietojen omistaja. Yhteistunnusten käyttö on sallittu vain perustellusti omistajan luvalla.

5.3 Internet ja viestintäratkaisut

Internet ja viestintäratkaisut (sähköposti, kalenteri, pikaviestintä, sähköiset kokouspalvelut) ovat hyviä työvälineitä tiedon hakuun ja työskentelyyn ajasta ja paikasta riippumatta. On kuitenkin muistettava, että sähköpostissa tai internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Internetin ja viestintäratkaisuiden käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja viestintäratkaisut ovat työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintään yksityistä vapaa-ajan sähköpostia.
- Käytä vain sellaisia palveluita, jotka tiedät turvallisiksi ja joiden käytön organisaatiosi on sallinut.
- On lainvastaista välittää internetin kautta salassa pidettävää tietoa ilman asianmukaista salausta. Tällaiset viestit ja liitetiedostot on salattava organisaation hyväksymillä tuotteilla tai palveluilla. Organisaatiollasi saattaa olla salattuja tietoliikenneyhteyksiä keskeisimpien yhteistyötahojen kanssa.
- Opettele salaustuotteiden oikea käyttö, jotta tieto ei vahingossa siirry salaamattomana.
- Pääsääntöisesti ohjelmien lataaminen internetin kautta ja asentaminen on kiellettyä. Jos tarvitset tiettyä ohjelmaa työtehtäviesi hoitamiseen, pyydä tietohallintoa asentamaan se. Jos organisaatiokohtaisen ohjeistuksen ja työtehtäviesi perusteella lataat ohjelmia, pyri aina varmistumaan ohjelmiston ja lähteen luotettavuudesta ja varmistumaan ohjelmiston lisensoinnista.
- Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies). Pyydä tarvittaessa tietohallinnolta apua.
- Virkasähköpostia saa käsitellä vain oman organisaation tai mahdollisesti muun julkishallinnon organisaation omistamilla laitteilla.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan oman organisaation sähköpostijärjestelmään. Sitä ei saa ohjata tai jatkolähettää automaattisesti organisaation sähköpostijärjestelmän ulkopuolelle.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat ja vireille saatetut asiat organisaation määrittelemään sähköpostiin, asiointipalveluun tai muuhun vastaavaan sähköiseen palveluun.
- Muista, että vastaat henkilökohtaiseen sähköpostiin tulevasta työpostista virkavelvollisuuksien mukaisesti.
- Muiden kuin virkasähköpostin (esimerkiksi vapaa-ajan sähköpostipalvelu) käyttö töissä on sallittua vain oman organisaation luvalla. Siirrä tällainen viestintä vapaa-ajan sähköpostiisi.

- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana virkavelvollisuuksien mukaisesti.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä, vaan toimi organisaatiosi ohjeistuksen mukaisesti. Tarvittaessa voit ilmoittaa asiasta tietohallintoon.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se pitää poistaa.
- Suhtaudu terveen epäluuloisesti sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Varo ns. ”kalasteluviestejä”, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin. Vältä myös napauttamasta sähköpostiviesteissä olevia linkkejä, jos et tiedä minne kyseinen linkki johtaa tai jos viesti ei liity työtehtäviisi.
- Älä välitä ketjukirjeitä eteenpäin.
- Jos saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Jos oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo (sähköpostiosoitteita), jonka jokainen vastaanottaja saa tietoonsa. Se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiotoimintoa, jos haluat estää sähköpostin jakelussa olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä. Noudata joulutervehdysten tms. lähettämisessä oman organisaatiosi antamaa ohjeistusta. Ennen kuin napautat Lähetä (Send) –painiketta, varmista että Vastaanottaja (To:) ja mahdollisissa Kopio (Cc:) sekä Piilokopio (Bcc:) –kentissä olevat vastaanottajat ovat juuri ne henkilöt, joille tarkoituksesi on viesti lähettää.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä virkapostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit – noudata annettua ohjeistusta.

5.4 Toimitilojen turvallisuus

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

- Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.
- Noudata kulunvalvonnasta annettuja ohjeita. Käytä organisaation toimitiloissa kuvallista henkilökorttiasi (jos sellainen on annettu).
- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Jokaisella vieraalla tulee olla isäntä. Isäntä vastaa vieraidensa oleskelusta ja kulkemisesta toimitiloissa.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai henkilökunnan tiloihin.
- Pyri käyttämään vierailuihin niihin tarkoitettuja neuvottelutiloja.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaan liittymätöntä materiaalia. Huolehdi neuvottelun päättyessä, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä salassa pidettäviä aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvallisessa paikassa, tarpeen mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa päätelaitetta ilman valvontaa. Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata "puhtaan pöydän" periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Kuvaaminen organisaation tiloissa voi olla kiellettyä – noudata organisaatiokohtaista ohjeistusta. Valvo myös vieraidesi toimintaa ja esimerkiksi kameroiden käyttöä.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi. Huolehdi myös siitä, että toimitilan ulko-ovi lukittuu poistuessasi.
- Ohjaa vieraat tai "eksyneet" henkilöt oikeisiin paikkoihin, tarvittaessa saata henkilö aulaan tai ulos. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä auki kulunvalvonnassa olevia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina.

Lisätietoa: Toimitilojen tietoturvaohje (VAHTI 2/2013).

Tietomurto voi tapahtua teknisten keinojen sijaan ihan perinteisin menetelmin. Kiinnitä huomiota tuntemattomiin, ilman henkilökorttia kulkeviin henkilöihin niissä toimitiloissa, joissa kulkukorttia edellytetään. Saata myös vieraasi vierailun jälkeen ulos.

6 Työskentely oman organisaation ulkopuolella

Myös julkishallinnossa työskennellään yhä useammin oman toimipisteen ulkopuolella toisessa virastossa, työmatkalla tai kotona. Kaikkia asioita ja kaikkia tietoja ei ole mahdollista käsitellä oman organisaation ulkopuolella.

Lisätietoa: Päätelaitteiden tietoturvaohje (VAHTI 5/2013).

6.1 Tunne päätelaitteesi ominaisuudet

Nopeasti kehittyvät päätelaitteet ja tietoliikenneyhteydet mahdollistavat teknisesti samat palvelut kuin työpisteessäsi. Kannettavat päätelaitteet sisältävät samat, jopa nykyaikaisemmat toiminnallisuudet kuin perinteinen pöytäkone.

- Huolehdi työnteossa käyttämiesi kannettavien päätelaitteiden turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin, joita ovat mm. PIN- tai salasanakyselyt, laitteen automaattinen lukitus ja suojakoodikyselyt, tietoliikenneyhteyksien käyttäminen ja salaaminen.
- Huolehdi, että matkapuhelimessasi on päällä PIN- ja suojakoodikysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletuskoodit.
- Älä lataa tai asenna laitteisiin mitään työhön kuulumatonta.
- Käytä tietojen salausta silloin kun sitä edellytetään.
- Huolehdi tietojen varmuuskopioinnista ja/tai tarvittaessa automaattisesta synkronoinnista muuhun tietojärjestelmään organisaatiokohtaisen ohjeen mukaisesti.

6.2 Etätyö ja etäkäyttö

Etätyöllä tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä tehtävää työtä. Tyypillinen etätyö on kotoa tehtävää toimistotyötä. Etätyötä voidaan tehdä myös muusta vakituisesta paikasta (esim. organisaation järjestämä etätyöpiste) tai matkoilla (esim. hotelli tai toisen organisaation tilat), jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys.

Etäyhteys on tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknisten palvelujen käyttöä etäyhteyden avulla. Etätyöntekijän on kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Erityisen tärkeää tämä on silloin, kun toimit vakituisen työpisteen ulkopuolella. Etätyössä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi organisaation varsinaisissa toimitiloissa.
- Säännöllinen etätyö on sallittua vain, jos siitä on tehty erillinen sopimus. Noudata etäkäytöstä (esimerkiksi sähköposti ja kalenteri älypuhelimella) annettua ohjeistusta.
- Muista, että kaikkea organisaatiossa tehtävää työtä ei voida tehdä etätyönä. Joidenkin järjestelmien etäkäyttö voi olla kielletty tai estetty.
- Pääsääntöisesti työnantaja vastaa etäkäytössä vaadittavien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien hankinnasta.
- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
- Huolehdi, että käyttämäsi käyttäjätunnukset, salasanat, mahdolliset toimikortit ja muut tunnistusvälineet ovat vain sinun hallussasi ja tiedossasi.
- Käytä sovittuja haittaohjelmien torjuntaohjelmia ja opi tarkistamaan, että ne ovat ajan tasalla.
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
- Asiakirjojen käsittelyssä etätyössä on noudatettava samoja periaatteita kuin normaalisti, etätyön erityisriskit huomioon ottaen. Myös etätyössä on otettava huomioon aineiston luokittelu ja siihen liittyvät käyttösäännöt sekä luovutusta, käyttöä ja käsittelyä koskevat rajoitukset.
- Huolehdi tietoaineistosi varmuuskopioinnista sekä turvallisesta säilytyksestä ja hävittämisestä.

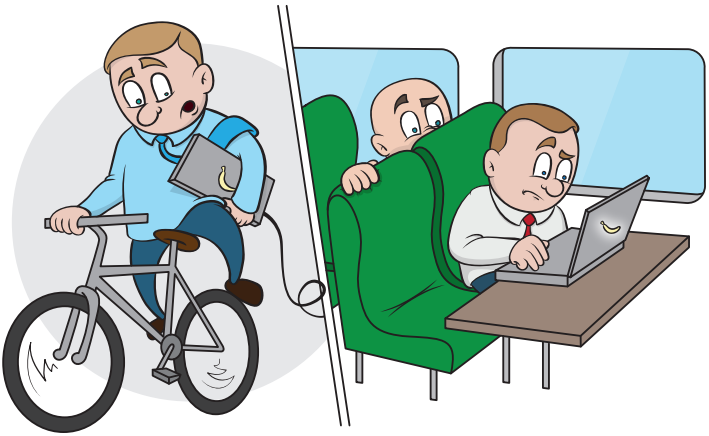
6.3 Matkoilla, julkisissa kulkuneuvoissa, nettikahviloissa…

- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä ml. henkilötiedot.
- Jos työskentelet julkisissa tiloissa, varmistu, etteivät muut henkilöt pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Käytä näyttösuojaa.
- Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita tai puhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Älä laita salassa pidettävää tietoaineistoa tai ICT-laitteita tai lentokoneessa ruumaan meneviin matkatavaroihin vaan kuljeta ne käsimatkatavaroissa.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.
- Jos käytät mobiili-internet-yhteyttä (älypuhelin, mokkula tai vastaava) ulkomailla, varmista etukäteen, millaisia tietoliikennekustannuksia on odotettavissa. Normaalisti 3/4G-yhteys kannattaa ottaa kokonaan päätelaitteesta pois päältä ja käyttää vain tarjolla olevia wlan-yhteyksiä.

6.4 Kotikoneella toimittaessa

Jos sinulla on kotona oma tietokone ja internet-liittymä, on tärkeää huolehtia myös niiden tietoturvallisuudesta, vaikka et käyttäisi niitä työtehtävien hoitamiseen. Kotikoneita käytetään apuna murtauduttaessa tietoverkkorikollisen mielenkiinnon kohteena oleviin palveluihin.

- Jos mahdollista, pyydä ajoittain luotettavaa tietotekniikka-asiantuntijaa (kaveri, sukulainen) tarkistamaan, että työasemasi ja nettiliittymäsi toimivat oikein ja turvallisesti.
- Tee jokaiselle käyttäjälle omat henkilökohtaiset tunnukset, joilla on vain ns. normaalikäyttäjän oikeudet.
- Käytä ylläpitäjän tunnusta (esim. Järjestelmänvalvoja, Administrator) vain ylläpitotehtäviin.
- Asenna vain virallisia, ajan tasalla olevia ohjelmistoja.
- Huolehdi käyttöjärjestelmän ja muiden ohjelmien jatkuvasta automaattisesta päivittymisestä.
- Käytä tunnettua ja hyvämaineista tietoturvaohjelmapakettia (sis. mm. virustorjunta, palomuuri, haittaohjelmientorjunta, roskapostisuodatus) ja huolehdi sen jatkuvasta automaattisesta päivittymisestä. Opettele tarkistamaan päivityksen toimivuus.
- Älä avaa epäilyttäviä sähköpostiviestejä tai niissä olevia liitteitä tai linkkejä.
- Tee säännöllisesti sinulle tärkeistä tiedoista (valokuvat, videot jne) varmuuskopiot (esimerkiksi usb-kiintolevy, vapaa-ajan pilvipalvelu) ja harjoittele niiden käyttöä.
- Kun kirjaudut internet-palveluihin ja teet esimerkiksi nettiostoksia, käytä vain luotettavia palveluita ja toimittajia.
- Ole varovainen sosiaalisen median palveluissa. Älä anna enempää henkilökohtaista tietoa kuin on tarpeen – älä anna työnantajaan liittyvää tietoa lainkaan.
- Kun et käytä tietokonetta, sammuta se tai käytä virranhallintatilaa.



Kaikkia työtehtäviä ei ole mahdollista tehdä työpaikan ulkopuolella! Sovi etätyöstä ja etäkäytöstä esimiehesi kanssa ja noudata näistä annettuja ohjeita.

7 Ongelmatilanteet

7.1 Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

Sinulla on aina velvollisuus kertoa, jos sinulla on ongelmia tietoturvallisuusasioissa.

- Jos hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi ko. asian vastuuhenkilölle tai päätelaitteen tukipalvelusta vastaavalla toimittajalle oman vastuusi rajaamiseksi ja mahdollisen vahingon pienentämiseksi.
- Ilmoita aina haittaohjelmista (esim. virushälytys päätelaitteella) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi tietoturvavastaavalle, tietohallinto-organisaatiolle tai omalle esimiehellesi.
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista ja kehitysideoista turvallisuudesta vastaaville tai omalle esimiehellesi.

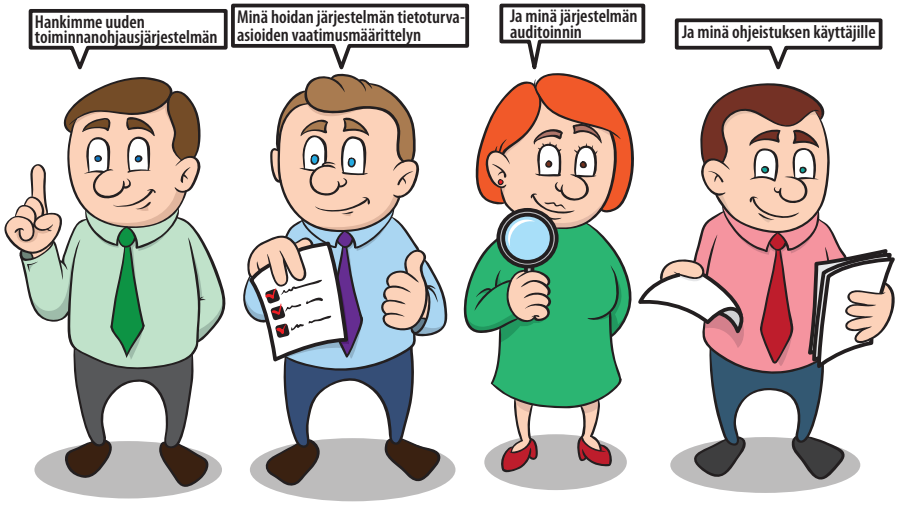
Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa

- Älä hätiköi.
- Älä sulje päätelaitetta, mutta irrota lähiverkkokaapeli tai katkaise langaton (wlan/3/4G) yhteys työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota siitä kuva kännykälläsi.
- Ota yhteyttä tietohallinto-organisaatioon ja/tai tietoturvavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

7.2 Seuraamukset

Lakien, määräysten ja ohjeiden rikkomisen seurauksena käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehellesi.

Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin tai rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös työsuhteen päättäminen.



Tietoturvallisuus on meidän kaikkien yhteinen asia!

8 Mistä saa lisätietoja?

Lisää tietoa tietoturvallisuudesta saat mm. seuraavista lähteistä:

- Organisaatiosi tietoturva- ja turvallisuushenkilöstö, oma esimies
- Organisaation omat ohjeet
- Lainsäädäntö – Valtion säädöstietopankki (www.finlex.fi)
- Tietoturvallisuutta ohjeistavat ja säätelevät organisaatiot, esimerkiksi
    - Valtiovarainministeriön VAHTI-ohjeet (www.vm.fi/vahti, www.vahtiohje.fi)
    - Arkistolaitoksen ohjeet (www.narc.fi)
    - Tietosuojavaltuutetun toimiston ohjeet (www.tietosuoja.fi)
    - Tietoyhteiskunnan kehittämiskeskuksen ohjeet (www.tieke.fi)
    - Viestintäviraston ohjeet (www.ficora.fi)
    - Julkishallinnon ja elinkeinoelämän yhteiset ohjeet (www.tietoturvaopas.fi)
    - Valtiokonttorissa toimivan Valtion IT-palvelukeskuksen tietoturva-sarjakuvat (www.valtiokonttori.fi/ttt)

Liite 1: Tietoturvallisuuteen keskeisesti liittyvät säädökset

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731/1999) 2.luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
- Suomen perustuslaki (731/1999) 2.luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999)
- Valtion virkamieslaki (750/1994) 17§: Säädös valtion virkasuhteesta
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM0024:00/02/99/1998)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): Arkaluonteiset kansainväliset asiakirjat
- Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
- Laki turvallisuusselvityksistä (177/2002): Henkilöiden taustat
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki sähköisistä allekirjoituksista (14/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
- Rikoslaki (39/1889) 34.luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
- Rikoslaki (39/1889) 38.luku 8 §: Tietomurto
- Rikoslaki (39/1889) 38.luku 9 § 1. kohta: Henkilötietorikos
- Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
- Vahingonkorvauslaki (41/1974)

- Asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
- Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki –sivustolta (www.finlex.fi).

Liite 2: Voimassa olevat VAHTI-julkaisut

VAHTI 5/2013	Päätelaitteiden tietoturvaohje
VAHTI 4/2013	Henkilöstön tietoturvaohje
VAHTI 3/2013	VAHTIn toimintakertomus vuodelta 2012
VAHTI 2/2013	Toimitilojen tietoturvaohje
VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007	Älypuhelimien tietoturvallisuus
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa

VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Uudistuva ja täydentyvä ohjeisto löytyy VAHTIn Internet-sivuilta (www.vm.fi/vahti) sekä www.vahtiohje.fi

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 16001
Telefaksi 09 160 33123
www.vm.fi

4/2013
VAHTI
Marraskuu 2013

ISSN 1455-7606 (nid.)
ISBN 978-952-251-513-1 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-514-8 (pdf)