VALTIOVARAINMINISTERIÖ

Tärkein tekijä on ihminen

– henkilöstö-turvallisuus osana tietoturvallisuutta

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2008 VAHTI

VALTIOVARAINMINISTERIÖ

Tärkein tekijä on ihminen

– henkilöstöturvallisuus osana tietoturvallisuutta

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2008

VAHTI

Taitto: Taina Ståhl
Kannen kuva: Pentti Nuortimo

ISBN 978-951-804-798-1 (nid.)
ISBN 978-951-804-799-8 (pdf)
ISSN 1455-2566
Painopaikka Edita Prima Oy
Helsinki 2008

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 10/01/2008

OHJE
30.1.2008

Ministeriöille, virastoille ja laitoksille

TÄRKEIN TEKIJÄ ON IHMINEN - HENKILÖSTÖTURVALLISUUS OSANA TIETOTURVALLISUUTTA

Valtiovarainministeriön tietoturvaohje *Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta* on yleisohje henkilöstöturvallisuuden järjestämisestä ministeriöissä, virastoissa ja laitoksissa.

Uudessa ohjeessa käsitellään henkilöstöturvallisuutta erityisesti tietoturvallisuuden näkökulmasta. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on ohjannut ohjeen valmistelun ja hyväksynyt ohjeen käytettäväksi valtionhallinnon tietoturvallisuuden kehittämisessä, ohjauksessa ja yhteistyössä. Ohje täydentää laajaa olemassa olevaa VAHTI-ohjeistoa.

Ohje on suunnattu ministeriöiden ja virastojen johdolle. Ohjeessa kuvataan hyviä henkilöstöturvallisuuskäytäntöjä tietoturvallisuuden näkökulmasta. Jokaisen organisaation johto päättää ja vastaa riittävien henkilöstöturvallisuusmenettelyjen käytöstä ja kehittämisestä organisaatiossa.

Ohjeessa painotetaan ennaltaehkäiseviä toimia ja yleisten etujen turvaamista virastojen johtamis- ja tietoturvakulttuurissa. Ohjeessa kuvataan keskeisiä henkilöstöturvallisuuden osa-alueita ja prosesseja sekä organisaatioiden avain- ja tukiprosesseihin liittyviä henkilöstöturvallisuustoimenpiteitä.

Henkilöstöturvallisuus ja siihen sisältyvät käytettävyys-, eheys- ja salassapitovaatimukset on otettava riittävästi huomioon organisaation tietoturvallisuutta ja toimintakulttuuria kehitettäessä. Henkilöstöturvallisuustyön kannalta keskeistä ovat suunnitelmallinen henkilöstön kehittäminen, johtaminen, käsittelyketjujen turvaaminen, riskikartoitukset, henkilöstön soveltuvuusarvioinnit, pääsyrajoitusmekanismit ja henkilöstöasioiden hallinto.

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää ja neuvotteleva virkamies Mikael Kiviniemi (sähköpostit: etunimi.sukunimi@vm.fi).

Hallinto- ja kuntaministeri Mari Kiviniemi

Neuvotteleva virkamies Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008)

Esipuhe

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTIn käsittelyn kohteina ovat kaikki tietoturvallisuuden osa-alueet.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (http://www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta.

VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on saanut kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

Tämän ohjeen on laatinut VAHTIn alainen henkilöstöturvallisuustyöryhmä. Työ on käynnistetty osana valtion tietoturvallisuuden kehitysohjelmaa. Ohje on viimeistelty laajan lausuntokierroksen palautteen pohjalta ja hyväksytty julkaistavaksi VAHTIn kokouksessa joulukuussa 2007.

Sisällysluettelo

Liitteet

1 Johdon tiivistelmä

1.1 Ohjeen kohderyhmä

Tämä ohje on suunnattu virastojen johdolle, jolla on vastuu viraston operatiivisesta toiminnasta. Ohje tukee myös henkilöstön perehdyttämistä tietoturvallisuuteen virastoissa. Henkilöstöturvallisuustyö on osa virastojen kaikkien toimialojen työtä, erityisesti henkilöstöhallintoa, toimitilapalveluja, tietohallintoa ja taloushallintoa.

Ohje on luonteeltaan yleinen ja kokonaisvaltainen, henkilöstöstä aiheutuvia riskejä tiedoille käsitellään **riippumatta tiedon muodosta tai käsittelytavasta**.

Ohje on tarkoitettu yleisohjeeksi henkilöstöturvallisuuden järjestämisestä virastoissa ja laitoksissa. Vaikka kaikkien virastojen toimintaan ei sisälly korkean turvallisuustason vaatimuksia, on tarpeen kuvata myös sellaisia henkilöstöturvallisuuskäytäntöjä, jotka ovat tarpeen eri turvallisuus- tai käyttöluokissa. Viraston johto päättää tarvittavien henkilöstöturvallisuusmenettelyjen käyttöönotosta siinä laajuudessa kuin se viraston toiminnan kannalta on tarkoituksenmukaista.

Ohjeessa on kuvattu laajemmin sellaisia osa-alueita, joita muissa ohjeissa ei ole käsitelty yksityiskohtaisesti. Ohjeen näkökulmana on ennaltaehkäisy ja yleisen edun turvaaminen virastojen johtamis- ja tietokulttuurissa. Ohjeessa on kuvattu keskeiset henkilöstöturvallisuuden tekijät ja prosessit sekä virastojen ja laitosten avain- ja tukiprosesseihin liittyvät henkilöstöturvallisuustoimenpiteet.

Työntekijöiden palvelussuhteen ehtoja ei ohjeessa käsitellä. Valtiovarainministeriö antaa valtion työnantajapolitiikkaa ja virkaehtosopimuksia koskevat ohjeet.

1.2 Henkilöstöturvallisuuden tavoitteet

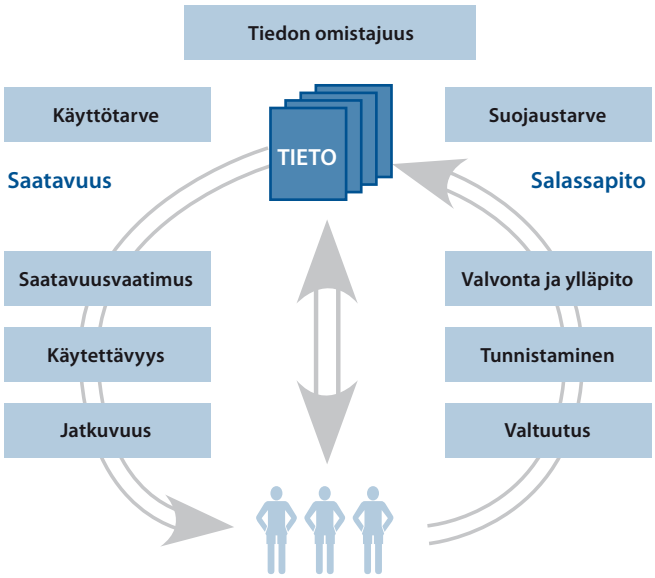
Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa; erotuksena henkilöturvallisuudesta, jolla tarkoitetaan henkilöihin kohdistuvien riskien hallintaa. Henkilöstöturvallisuus käsitetään osaksi

yleisempää turvallisuuskäsitettä. Tietoturvallisuuden alaterminä henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä.

Henkilöstöturvallisuuden merkitys tietojen turvaamiselle on keskeinen. Haasteena henkilöstöturvallisuustoiminnassa on ihminen. Henkilöstö käsittelee tietoja vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja niiden käsittelyn päätyttyä tuhoamalla niitä. Lisäksi henkilöstöllä on keskeinen rooli tietovarastojen ja -järjestelmien ylläpidossa.

Henkilöstöturvallisuus sisältää kaksi toisistaan riippuvaista vaatimusta:

- käytettävyysvaatimus ja tietojen eheysvaatimus
- salassapitovaatimus.



KUVA 1. Henkilöstöturvallisuuden haaste suojata tietoa ja turvata sen saanti

Tieto on immateriaalista, sitä voi monistaa ja lähettää ilman, että alkuperäinen tieto katoaisi. Toisaalta tieto voidaan helposti kadottaa tai hävittää vahingossa. Organisaatioiden sähköisesti ja paperimuotoon tallennettu tietomassa on valtava. Tiedon hallinnasta on tullut organisaatioiden toiminnan keskeinen haaste.

Henkilöstöturvallisuus on organisaation tietoturvallisuuden keskeinen alue ja se koskettaa kaikkia työntekijöitä. Henkilöstöturvallisuustyö on luonteeltaan ennalta ehkäisevää. Henkilöstöturvallisuuteenkin pätee turvallisuustoimintaa yleisesti kuvaava toteamus, että myös tällä osa-alueella maksetaan enimmäkseen siitä, että mitään ikävää ei tapahdu.

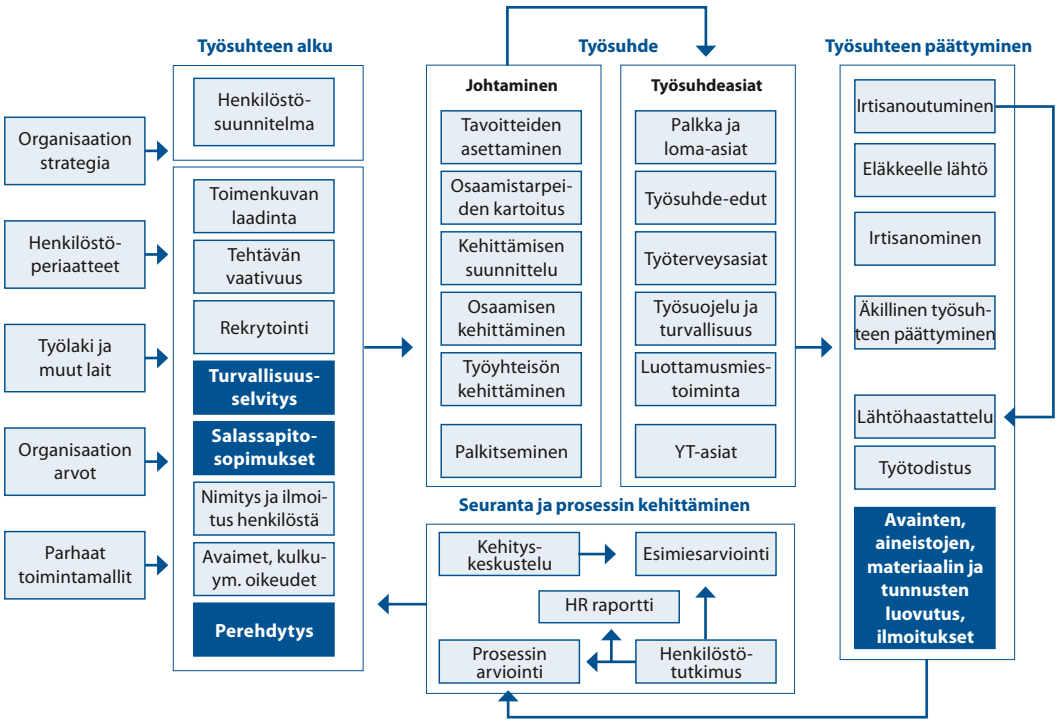
1.3 Johdon rooli virastokulttuurin kehittämisessä ja esimiestyössä

Henkilöstöturvallisuus on usein huomioitu puutteellisesti organisaation kokonaistietoturvaa kehitettäessä. Selkeämmin yksilöitäviin teknisiin tietoturva-alueisiin suuntautuminen ei ole riittävää. Henkilöstöturvallisuustyö edellyttää organisaatiokulttuuriin kajoamista.

Tyytyväinen henkilöstö on pysyvämpää, mikä vähentää henkilöongelmia. Organisaation maine miellyttävänä työpaikkana tuo myös kilpailuetua rekrytointiin. Puutteellisesta esimiestoiminnasta, työntekijöiden välisistä ristiriidoista tai sisäisestä kilpailusta johtuva stressi ja organisaation ilmapiirin huonontuminen, sekä tunne, että omaa työtä ei arvosteta, voivat johtaa työntekijän epätoivoisiinkin tekoihin.

Uutta henkilöä palkattaessa on tehtävästä riippuen syytä tehdä selvityksiä ja testejä henkilön taustojen selvittämiseksi.

Käytettävien **menettelyjen on oltava valtion työnantajapolitiikan ja virkaehtosopimusten mukaisia**. Toimintatavat henkilön irtisanomisen tai irtisanoutumisen yhteydessä on huolella harkittava. Irtisanomisperusteet on säädetty laissa.



KUVA 2. Esimerkki viraston henkilöstöprosessista. Henkilöstöturvallisuutta erityisesti koskevat osiot on merkitty tumman sinisellä.

1.4 Henkilöstöriskien hallinta

Tietoturvapolitiikka ja sen osapolitiikat ohjaavat viraston tietoturvatyötä, myös henkilöstöturvallisuutta virastossa. Henkilöstöhallinnon merkitystä tietoturvatyölle ei pidä väheksyä. Henkilöstöturvallisuustyössä on keskeistä suunnitelmallinen ja järjestelmällinen henkilöstön kehittämien, johtaminen ja henkilöstöasioiden hallinto. Puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin.

Johdon on tiedettävä, että ainoastaan laissa tarkoin määrätyillä valtuuksilla voidaan tehdä toimenpiteitä, jotka kohdistuvat henkilöiden perusoikeuksiin. Ohjeessa on esitetty keskeinen henkilöstöturvallisuutta koskeva lainsäädäntö sekä EU:n turvaluokiteltuja tietoja koskevat velvoitteet.

Viraston tietoturvallisuuden henkilöstöturvallisuutta käsittelevässä osapolitiikassa on määriteltävä periaatteet siitä, kenellä tai millä ryhmillä on oikeus käsitellä tietoja ja miten pääsyoikeusvaltuudet ratkaistaan. Virastojen on myös määriteltävä henkilöstönsä osaamisprofiilit. Tietoa on suojattava yhtäläisesti riippumatta siitä, kenen hallussa tai missä muodossa tieto on. Tiedon voi omistaa virasto tai laitos, yritys tai yhteisö, tai yksityinen henkilö. Tiedon omistaja voi olla muukin taho kuin virasto, jolloin virasto on ainoastaan tiedon haltija, jolloin omistaja päättää tietojensa luokituksesta ja siten niiden käsittelystä.

Henkilöstöturvallisuuden tilaa voidaan arvioida ja laatia riskikartoituksia. Kartoitusten ja tarkastuslistojen käytettävyydestä on hyvin konkreettisia ja mitattavissa olevia tuloksia. Henkilöstöturvallisuuden osa-alueiden mittaaminen on haasteellisempaa ja muihin tietoturvallisuuden osa-alueisiin verrattuna vaikeampaa.

Tietojen käsittelyn suoritukset muodostavat käsittelyketjuja. Käsittelyketjun turvaamiseksi on käytettävä *turvaohjausmekanismeja*, joilla ohjataan käsittelyketjujen turvallisuutta. Käsittelyketjut on suunniteltava turvallisiksi työprosessien suunnittelun yhteydessä

Viraston johdon on huolehdittava, että vain ne, joilla on tarve ja kyky käsitellä salassa pidettävää tietoa, saavat tiedon ja huolehtivat sen salassa pysymisestä. Henkilöstön tehtävän vaativuuksia määritettäessä tulee ottaa tarvittavassa laajuudessa huomioon salassapito- ja käytettävyystarpeet ja arvioitava henkilöiden soveltuvuutta työtehtävään. Viraston tulee tällöin määrittää henkilöstönsä tehtävänkuvauksiin niiden edellyttämät turvallisuusvaatimukset (*'tehtävän turvallisuusluokka'*). Henkilön sopivuutta selvitettäessä on arvioitava henkilön luonteen ominaisuuksia ja käytettävä taustaselvityksiä (*'henkilön arviointi'*). Tehtävän niin edellyttäessä on lisäksi pyydettävä poliisiviranomaiselta turvallisuusselvitys (*´turvallisuusselvitys´*). Oikeuksien myöntämisen eli valtuuttamisen edellytyksenä on ensisijaisesti työtehtävän edellyttämä tarve. Pääsyä on tarkoituksenmukaisesti rajoitettava vuorokauden ajan ja toistuvuuden perusteella sekä määritettävä pääsymenettelyt poikkeustilanteille.

Viraston tulee myös päättää, mitä pääsynrajoitusmekanismeja se käyttää. Pakollinen pääsyn rajoitusmekanismi soveltuu parhaiten korkean turvallisuustason resurssien turvaamiseen. Pääsyoikeuslistojen käyttö on yleistä, mutta niiden ylläpito ja muutosten hallinta on hankalaa. Rooliperusteinen pääsyn rajoitusmekanismi on yleisin, mutta se soveltuu matalan turvallisuustason resurssien turvaamiseen helpon hallittavuutensa ja yleispätevyytensä johdosta.

Ohjeessa on myös käsitelty riskikartoitusta, ostopalvelujen turvallisuutta, valtuuksien hallintaa ja tunnistamista.

Ohje ei käsittele teknisiä henkilöstöturvallisuuden toteuttamisessa tarvittavia teknisiä ratkaisuja muutoin kuin muutaman toimintokriittisen esimerkin valossa luvuissa 4.11 (käyttövaltuuksien hallinta tietojärjestelmäympäristössä) ja 4.12 (turvallisen pääsynvalvonnan toteuttaminen) sekä liitteessä 5 (henkilöiden fyysisiin tiloihin pääsyn valvonta).

2 Johdanto

2.1 Ohjeen käyttötarkoitus

Ohje on tarkoitettu yleisohjeeksi virastojen johdolle henkilöstöturvallisuuden järjestämiseksi virastoissa. Ohjetta voidaan käyttää myös henkilöstön tietoturvakoulutuksessa. Henkilöstöstä mahdollisesti johtuvia tietoriskejä käsitellään riippumatta tiedon muodosta tai käsittelytavasta.

2.2 Työn tausta ja tietoturvallisuuden kehitysohjelma

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) asetti 26.4.2005 henkilöstöturvallisuustyöryhmän, jonka tehtävänä oli henkilöstöturvallisuuden vahvistaminen hallinnon toiminnassa, henkilöstöturvallisuuden kehittäminen tietoturvallisuuden varmistamisen näkökulmasta ja valtionhallinnon ohjeen valmistelu. Näkökulmana oli henkilöstöriskien hallinta sekä rikos- että käytettävyysriskien osalta. Työssä on huomioitu lainsäädäntö, ohjeistus ja tekninen kehitys. Työryhmä tarkasteli alan menetelmiä, prosesseja ja henkilöstöturvallisuusmenettelyjen perusteita ja laati hyväksyttyihin toimintamalleihin perustuvan ohjeen virastoille.

2.3 Ohjeen laatiminen

VAHTIn alainen henkilöstöturvallisuustyöryhmä oli laaja-alainen henkilöstöturvallisuuden eri osa-alueita tuntevien ministeriöiden ja virastojen asiantuntijaryhmä, joka kokoontui määräajoin tarkastelemaan osaryhmien ja asiantuntijoiden toimittamia valmisteluaineistoja. Työryhmän puheenjohtajana toimi valtioneuvoston turvallisuuspäällikkö Jukka Sonninen valtioneuvoston kansliasta. Työryhmän jäseninä toimivat Erkki Väätäinen ulkoasianministeriöstä, Marja Isomäki ja Juhani Sillanpää valtiovarainministeriöstä, Seppo Juvonen sisäasiainministeriöstä, Jaana Palmunoksa Ilmatieteen laitoksesta, Terhi Vira ja Hannu Koivisto Pääesikunnasta, Tiina Mantere, Ilkka Hanski ja Heli Malmi suojelupoliisista, Reijo Aarnio (varapuheenjohtaja), Lauri Karppinen

ja Lauri Vuorivirta tietosuojavaltuutetun toimistosta, Mika Ahvenniemi Tullista ja Seppo Sundberg Valtiokonttorista.

Työssä käsiteltiin periaatteita, menettelyjä ja nykyisiä ongelma-alueita sekä etsittiin keinoja, joilla voidaan tehostaa valtionhallinnon henkilöstöturvallisuustyötä. Työryhmällä on hallussaan laajemminkin aihepiiriä koskevia toimintamalleja ja asiakirjamalleja, jotka ovat saatavilla käytettäväksi virastojen tietoturvatyössä.

Työryhmän valmistelema luonnos oli laajalla lausuntokierroksella kesällä 2007. Lopullinen ohje valmisteltiin lausuntojen perusteellla ja VAHTI hyväksyi sen sisällön joulukuussa 2007.

3 Henkilöstöriskien hallinnan perusteet

3.1 Uhkat ja riskien hallinta

Henkilöstö ja siitä johtuvat tietoturvatekijät ovat mahdollisesti tietojen eheyden, luottamuksellisuuden ja käytettävyyden uhkana. Usein uhkana pidetään henkilöstön aiheuttamia vahinkoja, tahallisia (ei-tuottamuksellisia) tai tahattomia (tuottamuksellisia), mutta myös organisaation rakenteella ja sen panostuksella tietotekniikkaan on suuri merkitys.

SHRM-mallissa (Strategic Human Resource Management) keskeistä on suunnitelmallinen ja järjestelmällinen henkilöstön kehittämien, johtaminen ja henkilöstöasioiden hallinto. Voidaan todeta, että karkeasti ottaen noin puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin. Torjuntasuositukset ovat tyypillisimmillään työn johtamiseen ja valvontaan sekä tiedonkulkuun ja yhteistyöhön liittyviä.

Henkilöstöturvallisuuden tarkastelun kohteena ovat teknologian, organisaation, ihmisen, työtehtävän ja työympäristön välinen yhteys.

Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa. Arvioitavia kohteita ovat mm. henkilöstön soveltuvuus, toimenkuvat, sijaisjärjestelyt, tiedonsaanti- ja käyttöoikeudet, suojaaminen, turvallisuuskoulutus ja valvonta.

Tietoturvatyössä teknisten ja toiminnallisten menetelmien käytön lisäksi suuri rooli jää henkilöstölle. Viraston on määriteltävä yksikäsitteisesti henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet. Tämä voidaan toteuttaa joko erillisten tehtävänkuvausten, työsopimusten tai muiden vastaavien järjestelyjen kautta. Vastuu- ja velvollisuuskuvauksista tulee ilmetä muun muassa salassapitovelvollisuuksiin, henkilöstö- ja asiakastoimintaan liittyvien tietojen käsittelyyn sekä muiden erityisluontoisten tietoaineistojen käsittelyyn liittyvät erityisvelvoitteet.

Henkilöstöturvallisuustyöllä vähennetään oman henkilöstön aiheuttamaa tuottamuksellista uhkaa muun muassa ohjeistamalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin.

Tietoturvallisuuden täytyy näkyä myös arjessa. Henkilöstö saattaa toimia tietoisesti organisaation sisältä vakoilemalla tai sabotoimalla. Rikoksen onnistumi-

sen mahdollisuus on voitava minimoida esimerkiksi henkilöiden taustaselvitysten, huolellisen tietojen luokittelun, raportoinnin, sisäisen valvonnan ja sisäisen tarkastuksen, kulunhallinnan ja johdonmukaisen seuraamusmenettelyn avulla.

Henkilön työsuhteen päättymiseen myös riitatilanteen seurauksena on varauduttava. Työntekijän, eronneen tai erotetun, pääsy viraston tietojärjestelmiin on estettävä välittömästi eroilmoituksen jälkeen sekä huolehdittava järjestelmien lokien tarkistamisesta järjestelmien tavanomaisesta poikkeavan käytön selvittämiseksi. Kuvatussa tulehtuneessa tilanteessa on työntekijä saatettava työpisteelleen, josta hän valvotusti kerää henkilökohtaisen omaisuutensa, minkä jälkeen hänet saatetaan ulos toimitiloista. Samalla on huolehdittava työntekijälle luovutettujen käyttäjätunnusten, kulkulupien, avainten ja muiden pääsyoikeuksien peruuttamisesta ja pois ottamisesta.

Vahinkojen määrän rajoittamiseksi virasto voi hyödyntää seuraavia riskienhallintatoimenpiteitä.

1. **Välttäminen** tarkoittaa henkilöstön sijoittelun ja toimenpiteiden suunnittelua niin, että vahingon tapahtumisen todennäköisyys pienenee. Organisaation rakenne ja käytettävissä olevat resurssit luovat rajoituksia sille, miten tehokkaasti tätä voidaan harjoittaa.

2. **Estämisellä** tarkoitetaan liikkumisen ja toiminnan rajoituksia. Tällaisia ovat esimerkiksi kulunvalvonta organisaation tiloissa sekä erilaiset käyttäjäroolit ja niiden mukainen tietojen saatavuus tietojärjestelmissä.

3. **Havaitseminen** sisältää toimenpiteet, joilla pyritään estämään tietojen väärinkäytön yritykset ja paljastamaan tapahtuneet väärinkäytökset. Menetelmiä ovat mm. tilojen valvontalaitteistot, tietojärjestelmien lokitiedostot ja niiden automatisoitu valvonta.

4. **Toipuminen** puolestaan kattaa keinot, joilla vahingoista, esimerkiksi avaintyöntekijän kuolema, pyritään toipumaan.

3.2 Henkilöstöriskien hallinnan periaatteita

Henkilöstöriskien hallinnassa on käytettävä useita menetelmiä. Lähtökohtaisesti tietoaineistoturvallisuus ja hallinnollinen turvallisuus, mm. tiedon omistajuus, luokitus, käsittelysäännöt, ohjeistus ja koulutus, ovat edellytyksiä henkilöstöturvallisuudelle, mutta niiden lisäksi henkilöstöturvallisuudessa on otettava huomioon muitakin mekanismeja. Työprosessit ja käsittelyketjujen tietovirrat on alun perin suunniteltava sellaisiksi, että henkilöstön tahallisia ja tahattomia virheitä voidaan ennalta estää. Näitä kutsutaan käsittelyketjujen turvaohjausmekanismeiksi.

Henkilöstöturvallisuustyön yleisperiaatteita ovat:

- monitasoisen turvajärjestelyn käyttö (in-depth defence)
- tietoja saa vain työtehtävään (need-to-know) ja lähtökohtaisesti vain vähimmäistarpeeseen (least privilege)
- tietojen lokerointi luokittain ja henkilöryhmittäin (compartmentalization)
- vaarallisten työyhdistelmien välttäminen (segregation of duties)
- usean henkilön yhtäaikainen läsnäolo kriittisissä toiminnoissa (dual control)
- pääsy-, valtuus- ja hallintatietojen salaisuuden jakaminen (split knowledge)
- henkilöstön tekemien toimenpiteiden valvonta ristiin- ja kaksoistarkistuksin (cross & double checks).

3.3 Henkilöstöturvallisuuden tilan arviointi ja riskikartoitus

Henkilöstöturvallisuudesta huolehtiminen alkaa rekrytoinnin yhteydessä tehtävistä taustatarkistuksista ja turvallisuusselvityksistä. Mukana voi tarpeen mukaan olla myös huumetestaus. Tarkistusten tavoitteena on varmistaa, että henkilö on sopiva erityistä luotettavuutta edellyttävään tehtävään. Joidenkin tehtävien osalta tällä täytetään lainsäädännön asettamat vaatimukset, esimerkiksi toimiminen lasten kanssa.

Henkilöstöhallinnolla tulee olla riittävä asiantuntemus erilaisia tarkistuksia ja testauksia koskevasta lainsäädännöstä sekä niissä käytettävistä menetelmistä. Tarkistuksia tulee tarpeen mukaan tehdä myös työsuhteen aikana, esimerkiksi toimenkuvien muuttuessa. Tiedot tarkistuksen tekemisestä on hyvä tallentaa henkilöstörekisteriin.

Henkilöstöhallintoon kuuluu tietoturvallisuuteen liittyvien vastuiden määrittely ja niistä tiedottaminen. Vastuut on kirjattava henkilöiden toimenkuviin. Esimiehillä on vastuu seurata tietoturvallisuuden toteutumista omassa yksikössään ja alaistensa toiminnassa. Myös erilaiset salassapitosopimukset ja niiden ajantasaisuudesta huolehtiminen kuuluvat tietoturvavastuiden hallinnointiin. Niistä on tehtävä kirjausmerkintä henkilöstörekisteriin.

Mikäli esimerkiksi tiedot turvaselvityksistä on viety henkilöstörekisteriin ja toisaalta tiedetään, keistä selvitykset tulisi tehdä, saadaan helposti tilannetta kuvaava prosenttiluku. Erilaisen ohjeistuksen olemassaolosta tai teknisistä järjestelyistä, kuten todentamisen toteuttamisesta tietojärjestelmissä, voidaan tehdä tarkistuslistoja, jotka kuvaavat organisaation henkilöstöturvallisuuteen panostamisen astetta. Näitä asioita pyritään mittaamaan henkilöstöturvallisuuden arviointilomakkeilla (VAHTI 8/2006).

Suurta osaa henkilöstöturvallisuuden lomakkeista arvioija ei kuitenkaan voi täyttää omatoimisesti, vaan vastausten saaminen edellyttää eri henkilöiden haastattelua, jolloin tulokset riippuvat monin paikoin haastateltavan omista mielipiteistä ja asenteesta tietoturvallisuuteen.

Henkilöstöturvallisuuden osalta tietoturvatason arviointi vaatiikin siten arvioijalta ihmistuntemusta ja näkemystä kyseisestä osa-alueesta.

Henkilöstöturvallisuuden arvioinnissa tulisi käsitellä seuraavia asioita ja prosesseja:

- tietoturvaohjeistus, sääntöjen tiedottaminen ja valvonta sekä koulutus
- avainhenkilöstön käytettävyys
- henkilöstöstä johtuvien riskien arviointi
- työsuhteen alkuun ja loppuun liittyvät toimet.

Tyypillisiä korjattavia kohteita ovat:

- taustaselvityksen puutteet
- riittämättömät tai sopimattomat henkilöt
- henkilöstön käytettävyyden arviointi
- varahenkilöjärjestelyt
- tietoturvaohjeistuksen, sääntöjen tiedottamisen ja valvonnan sekä koulutuksen puutteet.

Arvioinnissa syntyvässä analyysissä voidaan tarkastella seuraavia asioita:

- turvallisuusjohtaminen
- henkilöturvallisuus
- fyysinen turvallisuus
- tietoturvakulttuuri
- lainmukaisuus.

Riskikartoituksen laatimisesta on esimerkki liitteessä 1.

3.4 Tarkastuslistojen käyttö

Virasto voi käyttää tarkastuslistoja tukemaan henkilöstöriskien hallintaa, esimerkiksi arvioimalla, onko tarkasteltava kohde kunnossa, vaatiiko se kehittämistä, onko se tekemättä sekä kuka vastaa asioiden edistämisestä ja kehittämisestä. Esimerkkikohteita ovat:

- onko sovittu menettelytavoista taustatietojen tarkastamiseksi
- onko käytössä salassapitosopimus- ja alihankkijasopimusjärjestelyt
- onko ohjeita työsuhteen alkamiseen ja päättymiseen liittyvistä toimista

- onko työsopimuksissa ja tehtäväkuvauksissa määritelty tietoturvavelvoitteet
- onko avainhenkilöriskit kartoitettu ja varahenkilöjärjestelyt olemassa
- käytetäänkö työilmapiirikyselyjä

3.5 Keskeiset lainsäädännön velvoitteet

Henkilöstä aiheutuvan riskin hallinnassa haasteena on ihminen. Keskeiset henkilöstöturvallisuutta koskevat lainsäädännön osa-alueet ovat

- viranomaisten toiminnan julkisuus
- yksityiselämän suoja
- sähköisen viestinnän tietosuoja
- sähköisten allekirjoitusten käyttö ja tarjonta sekä sähköisen kaupankäynnin sekä sähköisen asioinnin tietosuoja ja tietoturva
- julkisrauhan rikkominen sekä tieto- ja viestintärikokset (rikoslaki)
- kansainväliset tietoturvavelvoitteet
- turvallisuusselvitykset

Ainoastaan laissa tarkoin määrätyillä valtuuksilla voidaan tehdä toimenpiteitä, jotka kohdistuvat henkilöiden perusoikeuksiin.

Henkilöstöturvallisuuteen liittyvä keskeinen lainsäädäntö on esitetty liitteessä 2.

3.6 Euroopan unionin neuvoston päätös turvallisuussäännöistä

Neuvoston päätös neuvoston turvallisuussääntöjen vahvistamisesta (Euroopan unionin turvallisuussääntö), jota Suomi noudattaa, velvoittaa huolehtimaan EU-luokitellun tiedon suojaamisen edellyttämästä henkilöstöturvallisuudesta. Sen mukaan ”Turvallisuusjärjestelmän tehokkuuden varmistamiseksi jäsenvaltioiden on liityttävä sen toimintaan ***toteuttamalla tarpeelliset kansalliset toimenpiteet*** tämän päätöksen säännösten noudattamiseksi, kun niiden toimivaltaiset viranomaiset ja virkamiehet käsittelevät EU:n turvaluokiteltuja tietoja.”

Edellä mainitun päätöksen artikla 2, kohta 2 toteaa, että ”Jäsenvaltiot toteuttavat asianmukaiset toimenpiteet ***kansallisten järjestelyjensä mukaisesti*** sen varmistamiseksi, että niiden yksiköissä ja tiloissa työskentelevät seuraavat henkilöt noudattavat 1 artiklassa tarkoitettuja säännöksiä käsitellessään EU:n turvaluokiteltuja tietoja:

1 Henkilöstön luotettavuuden selvittäminen

Kaikkien, jotka pyytävät saada CONFIDENTIEL UE tai sitä luottamuksellisemman turvaluokan tietoja, luotettavuus on selvitettävä asiaan kuuluvalla tavalla ennen luvan myöntämistä. Tällainen selvitys on tehtävä myös niiden henkilöiden osalta, joiden tehtäviin kuuluu turvaluokiteltuja tietoja sisältävien tieto- tai tietoliikennejärjestelmien tekninen käyttö tai kunnossapito. Selvitys on suunniteltava sellaiseksi, että tietystä henkilöstä voidaan sanoa, että

a) hän on ehdottoman **luotettava**,

b) hän on **luonteeltaan** ja **harkintakyvyltään** niin luja, että hänen käsiteltäväkseen voidaan epäilyksettä uskoa turvaluokiteltuja tietoja, tai että

c) hän saattaa olla altis ulkoiselle tai muista lähteistä peräisin olevalle painostukselle esimerkiksi sen vuoksi, että hän on asunut sellaisessa paikassa tai omannut sellaisia yhteyksiä, jotka saattavat muodostaa tietoturvariskin.

Erityisen perusteellisesti on tarkastettava sellaisten henkilöiden luotettavuus,

d) joille on tarkoitus sallia pääsy TRES SECRET UE/EU TOP SECRET -turvaluokan tietoihin,

e) jotka ovat sellaisessa asemassa, että heidän tehtäviinsä kuuluu päästä säännöllisesti huomattavaan määrään SECRET UE -turvaluokan tietoja, ja

f) joilla on tehtäviensä vuoksi oikeus päästä EU:n tehtävien kannalta oleellisiin tieto- tai tietoliikennejärjestelmiin ja joilla on näin tilaisuus päästä luvatta suureen määrään EU:n turvaluokiteltua tietoa tai aiheuttaa EU:n tehtäville teknisen sabotoinnin kautta vakavaa vahinkoa.

Edellä d, e ja f alakohdissa kuvattujen olosuhteiden ollessa kyseessä on käytettävä mahdollisimman tehokkaasti hyväksi taustatutkimustekniikkaa.

Jos henkilöitä, joilla ei ole tehtävien mukaista valtuutusta päästä tietoihin, on määrä ottaa palvelukseen tehtäviin, joissa he voivat päästä EU:n turvaluokiteltuihin tietoihin (kuten lähetit, turvamiehet, kunnossapitohenkilöstö ja siivoojat jne.), heidän luotettavuutensa on ensin asiaan kuuluvasti selvitettävä.

Suomessa kyseisen artiklan tarkoittama henkilöstön luotettavuuden selvittäminen toteutetaan pääasiallisesti turvallisuusselvitysmenettelyllä, laki turvallisuusselvityksistä (177/2002) mukaisesti. Menettelyä käsitellään tässä ohjeessa tarkemmin kohdissa ”turvallisuusselvitykset” ja ”kansainvälinen henkilöturvallisuustodistus”.

2 Luotettavuusselvitysrekisteri

Kaikkien yksiköiden, elinten tai virastojen, joissa käsitellään EU:n turvaluokiteltuja tietoja tai joissa käytetään tehtävien kannalta oleellisia tieto- ja tietoliikennejärjestelmiä, on pidettävä rekisteriä palvelukseen otetun henkilöstön luotettavuusselvityksistä. Luotettavuusselvitys on tarvittaessa tarkistettava sen varmistamiseksi, että se on kyseisen henkilön nykyisten tehtävien kannalta riittävä. Luotettavuusselvitys on tarkistettava uudelleen ensisijaisen kiireellisesti, jos saadaan uusia tietoja, joiden mukaan henkilön työskentely turvaluokiteltujen tietojen parissa ei enää ole turvallisuusetujen mukaista.

3 Henkilöstölle annettavat turvallisuusohjeet

Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat päästä turvaluokiteltuihin tietoihin, on annettava heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä. Yksi hyödyllinen menettely on edellyttää, että kaikki tällaiset henkilöt todistavat kirjallisesti vaitiolositoumuksella, että he ymmärtävät täysin tehtäviensä kannalta olennaiset turvallisuusvaatimukset.

4 Johdon velvollisuudet

Johdon velvollisuus on tietää, ketkä kyseisen johdon alaisuudessa olevasta henkilöstöstä työskentelevät turvaluokiteltujen tietojen parissa tai voivat päästä yksikön tehtävien kannalta olennaisiin tieto- ja tietoliikennejärjestelmiin. Johdon on pidettävä kirjaa ja raportoitava kaikista tapahtumista tai ilmeisistä puutteista, jotka voivat vaikuttaa turvallisuuteen.

5 Henkilöstön oikeudellinen asema turvallisuusasioissa

Henkilöä koskevien kielteisten seikkojen tullessa ilmi on selvitettävä, onko hän tekemisissä turvaluokiteltujen tietojen kanssa tai sallitaanko hänen päästä yksikön toiminnan kannalta olennaisiin tieto- ja tietoliikennejärjestelmiin ja onko kyseiselle viranomaiselle ilmoitettu asiasta. Jos henkilön todetaan olevan turvallisuusriski, häntä on estettävä suorittamasta tehtäviä, joissa hän voi vaarantaa turvallisuuden, tai hänet on siirrettävä suorittamaan muita tehtäviä.

4 Henkilöstoturvallisuuden järjestelyt virastossa

4.1 Henkilöstöturvallisuus tietoturvapolitiikassa

Työn edellyttämät tarpeet tiedon käsittelijöistä tulee kuvata *tietoturvapolitiikassa tai osapolitiikoissa*. Viraston tulee ottaa huomioon viraston käyttämien tietojen omistajuus. Omistajan tulee vastaavasti ilmaista tahtonsa määräämällä tiedon turvaluokka asiaryhmittäin.

Viraston on määriteltävä kenellä tai millä ryhmillä ja millä periaatteilla

- on oikeus saada tietoja haltuunsa ja käsitellä tietoja (pääsy tietoon)
- saa käsitellä keskeisiä välineitä, kuten esimerkiksi salausavaimia, palomuureja, reitittimiä tai palvelimia (pääsy materiaaliin ja järjestelmiin)
- on oikeus päästä järjestelmätiloihin (pääsy tilaan)
- on valtuus ratkaista pääsyoikeus.

Virastojen on myös määriteltävä henkilöstönsä osaamisprofiilit sekä määriteltävä

- kuka on avainhenkilö, jolla on oltava sijaisia
- kuka voi olla sijainen
- kuka on kykenevä toimimaan varahenkilönä
- miten järjestelmän ylläpitäjiä valvotaan ja estetään tekemästä virheitä tai rikkomuksia.

4.2 Omistajuuden tunnistaminen

4.2.1 Tiedon pääluokat eli asiaryhmät

Yhtenäisen suojan vaatimuksesta on tiedoille annettava arvo, jonka perusteella tiedon haltija suojaa sen alkuperää vastaavasti. Tiedoilla on siten oltava omistaja, joka määrittää tiedon suojausarvon.

Tietoa on suojattava yhtäläisesti riippumatta siitä, kenen hallussa tai missä muodossa tieto on.

Tiedon voi omistaa virasto tai laitos, yritys tai yhteisö, tai yksityinen henkilö (henkilötiedot). Periaate ei ole aivan selkeä, sillä virkamiehet luovat tietoa jatkuvasti lisää yhdistelemällä saamiaan tietoja toisiinsa ja siten luomalla uutta tietoa. Uudellakin tiedolla on valtionhallinnossa omistaja, joka määräytyy valtioneuvostosta annetun lain (175/2003) ja valtioneuvoston ohjesäännön tehtävävastuiden mukaisesti. Virastojen oikeudet ja vastuut on määritetty lailla. Julkisuuslain (621/99) § 24.1 salassapitomääräykset varsin selkeästi osoittavat, mikä on tai on voitava pitää salassa. Kullakin kohdalla (*asiaryhmä*) on selkeästi määritettävissä tehtävävastuiden mukaisesti omistaja, joka määrää tietojen turvallisuusluokituksesta.

Omistaja voi olla muukin taho kuin virasto. Yritykset ja yhteisöt antavat virastoille tietoja, jotka sopimuksen tai muun perusteen johdosta eivät ole viraston omaisuutta, virasto on ainoastaan tiedon haltija.

Henkilötiedot ovat erityisen selkeä esimerkki omistajuudesta, joka ei ole virastolla. Virasto voi olla siten tiedon omistaja säädöksissä esitettyjen vastuiden perusteella, tai tiedon haltija.

Omistaja päättää tietojensa luokituksesta ja siten niiden käsittelystä

Omistajan tulee antaa yleisohjeet tietojensa käsittelystä. Yleisohje sisältää tietoluokkien käsittelysäännöt ja luokitusohjeen, jota käytetään tukena uutta tietoa luokitellessa.

4.2.2 Suojattavan arvon määrittäminen ja luokittaminen

Tiedot, kuten myös muut suojattavat resurssit (´objektit´), on luokitettava. Luokitus on perusta suojausmekanismeille.

Tiedoilla ei ole samaa suojaustarvetta, vaan se vaihtelee tiedon arvon mukaan. Tiedoille tai tiedon pääryhmille (*asiaryhmä*) on määrättävä **salassapitoluokka** ja **käytettävyysluokka**.

Tiedon suojausluokka ilmaisee tiedon haltijalle ja käyttäjälle tiedon arvon ja sen, miten sitä on käsiteltävä. Erityisesti tiedon haltijaviraston on tunnettava omistajan tahto siitä, mitä henkilöstöturvallisuusmenettelyjä tiedon käsittely vaatii.

Tiedon arvo on voitava välittää haltijalle, jonka tulee tuntea rajoitukset tiedon luovuttamisesta omalle henkilöstölle ja muulle henkilöstölle. Tiedon haltija on velvollinen huolehtimaan tiedoista omistajan antamien yleisohjeiden mukaisesti. Tiedon haltijan on huomioitava tiedon edelleen luovuttamiselle asetetut rajoitukset ja annettava käsittelyohjeet tiedoille. Tiedon käsittely on usein muista lähteistä saadun tiedon kokoamisesta ja jalostamisesta, jolloin yhteys

tiedon omistajaan on selkeä. Uutta tietoa tulee käsitellä lähdetietojen omistajuuden mukaisesti. Tiedon käyttäjän tehtäväksi jää käsittelyn asianmukaisuus omistajan ja haltijan yleisohjeiden perusteella. Tiedon käyttäjän on huomioitava tiedon edelleen luovuttamiselle asetetut rajoitukset.

4.3 Käsittelyprosessien turvaaminen

Tietojen käsittelyn suoritukset (transaction) muodostavat käsittelyketjuja. Käsittelyketjun turvaamiseksi on käytettävä *turvaohjausmekanismeja*, joilla ohjataan käsittelyketjujen turvallisuutta, ja valvotaan, että virheellisiä toimintoja ei tehdä tai että ne havaitaan (ISO 17799 kohta 10.1.3).

Käsittelyketjut on suunniteltava turvallisiksi työprosessien suunnittelun yhteydessä.

Turvaohjausmekanismien käytöllä varmistetaan suoritteiden valtuutuksien aitous (authorization), valvotaan suoritteiden toteuttamisen perustumista hyväksyttyyn valtuuteen (access), varmistutaan suoritteiden kirjaamisesta (recording) ja siitä, että kirjanpidossa käsitellään ainoastaan todellisia suoritteita tai resursseja (asset accountability).

Keskeisimmät turvaohjausmekanismit ovat:

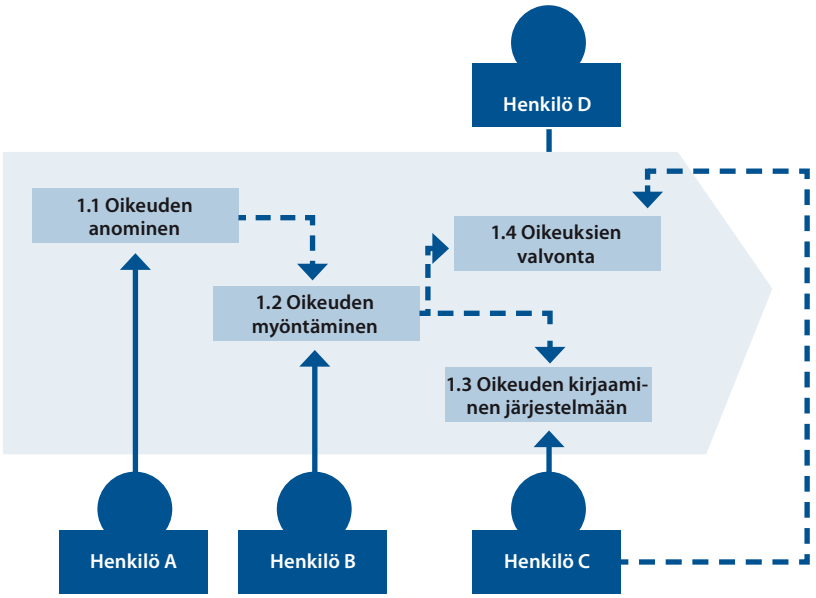
- **Usean henkilön läsnäolo** (dual control), jolla tarkoitetaan kahden tai useamman henkilön välttämätöntä läsnäoloa määrätyssä kriittisessä suorituksessa.
- **Jaettu valtuus** (split knowledge), jolla tarkoitetaan määrättyyn kriittiseen suoritukseen tarvittavan tiedon jakamista kahteen tai useampaan osaan ja osien luovuttamista kahdelle tai useammalle henkilölle.
- **Käyttövaltuuksien eriyttäminen** (segregation of duties), jolla tarkoitetaan käsittelyketjun kriittisten suoritteiden eriyttämistä usealle henkilölle, ns. vaarallisten työyhdistelmien estämistä.
- **Tietoaineiston lokerointi** (compartmentalization), jolla tarkoitetaan tietoaineiston eriyttämistä riittävän pieniin kokonaisuuksiin ja niiden käyttöoikeuden antamista ainoastaan tietylle henkilöryhmälle tietoaineistokokonaisuuden suojaamiseksi.
- Tietojen käsittelyn suoritteiden **kirjaaminen ja kirjanpidon valvonta** (cross & double checks).

Erityisen merkittävää turvaohjausmekanismien käyttö on poikkeus- ja hätätilanteissa, joissa ei voida toimia normaaliprosessien mukaisesti. Jos henkilö tarvitsee poikkeamatilanteissa välittömästi laajemmat valtuudet kuin normaalitilanteessa, edellytetään tällöin kahden henkilön läsnäoloa (=usean henkilön läsnäolo) ja valtuustieto on jaettu kolmannelle henkilölle (=jaettu valtuus),

joka itse ei voi tehdä toimenpidettä. Valtuuttaja myös muuttaa valtuustietoa toimenpiteen jälkeen. Lisäksi valtuuttaja raportoi valtuuden antamisesta neljännelle henkilölle (valvoja), joka kykenee seuraamaan järjestelmään tehtyjä muutoksia, muttei muuttamaan itse niitä (=tehtävien eriyttäminen).

4.3.1 Tehtävien eriyttäminen

Tehtävien eriyttäminen eli vaarallisten työyhdistelmien välttäminen on tärkein ja useimmin käytettävissä oleva turvaohjausmekanismi. Sen tarkoituksena on ehkäistä virheiden ja väärinkäytösten mahdollisuutta. Yksikään henkilö ei voi olla turvatussa käsittelyketjussa vastuussa **enempää kuin yhdestä käsittelyketjun kolmesta suorituksesta**, esimerkiksi valtuuttamisesta, hallussapidosta tai kirjanpidosta. Tietojärjestelmissä oikeuksien saamisen prosessissa on kolme eriytettyä toimijaa: oikeuden tarvitsija, oikeuden myöntäjä ja oikeuden järjestäjä.



PIIRROS 1. Tehtävien eriyttäminen prosessissa, joka sisältää väärinkäytön mahdollisuuden

4.3.2 Tiedon käsittelijät toimivat roolien kautta

Virkamiehellä on henkilöstöturvallisuuden kannalta useita rooleja, tehtävästä riippuen ne vaihtelevat perusroolista aina tiedon haltijaorganisaation päällikkyyteen ja tiedon omistajuuteen. Henkilöstöturvallisuustyöllä on huolehdittava, etteivät erilaiset roolit aiheuta riskejä.

Henkilöllä voi olla useita rooleja, esimerkiksi oikeuksien myöntäjän rooli, mutta myös peruskäyttäjän rooli. Tällöin on todettava rooliristiriita ja järjestettävä niin, ettei hän voi hakea oikeutta ja myöntää sitä itselleen.

4.3.3 Avainhenkilöiden käytettävyys

Käytettävyysriskien selvittämiseksi on arvioitava, mikä on henkilön merkitys organisaatiossa ja sen toiminnassa.

- Onko henkilön paikallaolo ja asema välttämätöntä keskeisten päätösten tekemisessä? (*päättäjä*)
- Onko henkilön toiminta välttämätöntä keskeisen järjestelmän käytettävyydelle, tai onko hänen paikallaolonsa ja asemansa välttämätöntä kriittisten toimenpiteiden käynnistämisessä tai toteuttamisessa? (*järjestelmän avainhenkilö*)
- Kohdistuuko henkilöön hänen työstään johtuen tavanomaista suurempi rikos- tai onnettomuusriski? (*henkilöriskihenkilö*)

Avainhenkiöiden tavoitettavuus on sovittava *tehtävänkuvauksessa*. Jos järjestelmä, jossa henkilö on avainhenkilö, on aikakriittinen, on saavutettavuus varmistettava varallaololla tai henkilön tavoitettavuus hätätyön teettämistä varten on varmistettava muulla tavoin.

Saavutettavuuden kannalta on tärkeää varmistua henkilön sijainnista, jotta saapuminen aikakriittiseen toimeen olisi mahdollista. Henkilön teknisen valvonnan toteuttaminen edellyttää asiasta sopimista sekä yhteistoimintamenettelyä virastossa.

Avainhenkilöstön käytettävyyttä on seurattava suunnittelemalla lomat ja muut poissaolot virkapaikalta siten, että sijaisuusjärjestelyt ovat mahdollisia. Erityisesti on kiinnitettävä huomiota työpäivinä tapahtuviin virkamatkoihin, jolloin henkilö ei tosiasiassa ole käytettävissä kriittiseen työtehtävään.

4.3.4 Sijaisuudet

Henkilötietolain 32 § edellyttää, että tiedot turvataan tarvittavin ”organisatorisin ja teknisin keinoin” ottaen huomioon tietojen laatu, määrä ja merkitys. Aikakriittiset palvelut (järjestelmäluokka 3), kuten oikea-aikaisesti tapahtuva palkanmaksu, edellyttävät jokapäiväisten sijaisuuksien järjestämistä. Sijaisuudet on määrättävä virastossa kirjallisesti ja ne tulee ilmetä tehtävänkuvauksissa.

Eräs keino sijaisuuksien järjestämiseen on hankkia ja kouluttaa virastoon **moniosaajia**, jotka pystyvät korvaamaan toisiaan. Moniosaajiin sisältyy kuitenkin riskejä, joista keskeisin on vastuiden epäselvyydet usean henkilön hoitaessa tehtävää. Erityisesti on varottava vaarallisten työyhdistelmien syntymistä.

Henkilövuokrauksen yleistyminen on nostanut esille henkilövuokrausyritysten käyttämisen sijaisuuksien hoitamisessa. Henkilövuokraus on varteenotettava mahdollisuus, mutta monimutkaisten järjestelmien ja palveluympäristöjen hallitseminen ei ole mahdollista tilapäisin voimin. Henkilövuokraukseen sisältyy myös turvallisuusriskejä, jotka on arvioitava palvelujen käytössä.

4.3.5 Jatkuvuus ja varahenkilöstö

Toiminnan jatkuvuuden varmistamiseksi on ennakolta suunniteltava, miten virasto varmistaa avainosaamisen. Tämä edellyttää varahenkilöiden etukäteen kouluttamista avaintehtäviin, ennen kuin avainhenkilö poistuu virastosta. Varahenkilöiden osaamista tulee harjoituttaa määräajoin. Jatkuvuuden varmistaminen pitkällä aikavälillä on suunniteltava ja määrätietoisesti toteutettava koulutusjärjestelmä, joka varmistaa toiminnan jatkuvuuden avaintehtävien henkilöstön siirtyessä mahdollisesti toisten työnantajien palvelukseen.

4.4 Työtehtävästä johtuva tarve tietoon

4.4.1 Tiedon saannin rajaaminen ja lokerointi

Tiedon tulee olla sitä tarvitsevien käytettävissä. Hallinnollisesti on huolehdittava, että vain ne, joilla on tarve ja kyky käsitellä salassa pidettävää tietoa, saavat tiedon ja huolehtivat sen salassa pysymisestä *(”tietoja saa vain työtehtävään”)*.

Kaikki tieto ei kuitenkaan ole tarkoitettu kaikkien tietoon. Salassapitovaatimus ei voi olla täysin ehdoton, sillä jonkun on kuitenkin voitava käsitellä tietoa (sic). Salassapito tarkoittaa siis tiedon salassapitoa ”yleiseltä joukolta, jolla ei ole tarvetta saada tietoa”. Salassapidon periaate on siten **rajata tiedon käsittelijöiden ja tiedon määrä vain työtehtävästä johtuvan tarpeen mukaan** ja lokeroida oikeudet **nimetylle henkilöryhmälle** *(”tietojen lokerointi luokittain ja henkilöryhmittäin”)*.

Julkisuuslaissa ja erityisesti sen 24 § määritellään, mikä tieto on tai voi olla salassa pidettävää.

4.4.2 Järjestelmien ylläpitohenkilöstö

Tietoa varastoidaan ja käsitellään tietojärjestelmissä. Järjestelmien luotettavuus ja niihin varastoidut tiedot on suojattu järjestelmien turvamekanismeilla. Turvamekanismeihin pätee edellä kuvattu sääntö rajata tietojärjestelmien ylläpitäjien määrä mahdollisimman pieneen joukkoon. Tietojärjestelmien ylläpitäjien vastuulla on toisaalta järjestelmän käytettävyys. Järjestelmät ja niistä muodostuva kokonaisuus on monimutkainen ja edellyttää erityisosaamista. Järjestelmille on asetettu korkea käytettävyysvaatimus. Näistä syistä on vält-

tämätöntä, että asiantuntijoilla ja päivystäjillä on sijaisia ja varahenkilöitä, jotka hallitsevat useita järjestelmiä. Ylläpitäjien ja heidän sijaistensa toimenpidemahdollisuuksia on rajoitettava turvallisuusohjausmekanismeilla. Ylläpitäjillä ei saa olla pääsyä käyttäjien tietosisältöihin.

4.4.3 Tehtävän turvallisuusluokitus

Henkilöstön tehtävät arvioidaan virastoissa ja tehtävälle määritetään palkkausjärjestelmän mukaisesti sen vaativuus. Tehtävän vaativuudessa tulee ottaa huomioon salassapito- ja käytettävyystarpeet ja arvioitava henkilöiden soveltuvuutta työtehtävään.

Tehtävän vaativuudessa on arvioitava henkilön osaaminen ja merkitys järjestelmien toiminnalle (*avainhenkilö*) sekä henkilön työtehtävissä tarvitsemien salassa pidettävien tietojen käsittelytarve. Salassapitotarve on eriteltävä sen mukaan, onko salassapidon perusteena valtion etu (*turva- ja käsittelyluokitus*), yritys tai yhteisö (*muu salassapitosyy*), tai yksityinen henkilö (*henkilötiedot*). Lisäksi voidaan arvioida kansainvälisten salassa pidettävien tietoaineistojen käsittelytarve.

Viraston tulee määrittää henkilöstönsä tehtävänkuvauksiin niiden edellyttämät turvallisuusvaatimukset (*”tehtävän turvallisuusluokka”*).

4.4.4 Tehtävän kuvaukset ja työjärjestykset

Palkkausjärjestelmässä kuvattujen tehtäväkuvausten tulee olla selkeitä ja niistä tulee ilmetä tehtävän edellyttämät vastuut ja velvollisuudet. Valtuutusmenettelyissä on kuvattava tarkasti päätösten teon edellyttämä tarkistusinformaatio, jonka perusteella tehdyt toimenpiteet voidaan todeta oikeiksi.

Virkamiehen tehtävän kuvaukseen on sisällytettävä kuvaus tehtävän käytettävyys- ja salassapitovelvoitteista sekä tehtävän edellyttämästä *turvallisuusluokasta*. Tehtävänkuvaus on selkeä perustelu haettaessa henkilölle turvallisuusselvitystä.

Tietoturvallisuuteen liittyvät vastuu- ja velvollisuuskuvaukset tulee päivittää säännöllisesti ja aina tarpeen vaatiessa. Jos esimerkiksi työntekijän työtehtävät muuttuvat oleellisesti, tulee tehtäväkuvausta muuttaa uusia työtehtäviä vastaaviksi.

Viraston tulee kartoittaa *avainhenkilönsä* ja varmistaa keskeisimmän henkilöstön tavoitettavuus esimerkiksi nimeämällä avainhenkilöille varahenkilöt.

Toiminnan kannalta vaarallisten tehtävä- ja vastuukokonaisuuksien muodostuminen tulee estää eriyttämällä *vaaralliset työ- ja valtuusyhdistelmät* eri henkilöille. Erityisesti pienissä toimintayksiköissä saattaa helposti tulla tilanteita, joissa työntekijät tekevät useita, eri organisaatiotasoille kuuluvia työtehtäviä. Nämä tilanteet eivät ole aina vältettävissä, mutta niiden riskejä voidaan vähentää esimerkiksi usean henkilön samanaikaista paikallaoloa edellyttämällä kriittisissä suoritteissa.

4.5 Valtuuttaminen

4.5.1 Valtuutuksen periaatteita

Pääsyoikeuden myöntämisen eli valtuutuksen (authorization) edellytyksiä ovat yleisperustelu pääsylle, esimerkiksi virkasuhde tai ostopalvelun turvaava turvallisuussopimus, työtehtävän edellyttämä tarve merkittävälle viraston palvelulle, henkilön arviointi ja hänestä tehdyt turvallisuusselvitykset.

Valtuuttamisessa huomioitavia periaatteita ovat:

- valtuuden on aina perustuttava viraston tarpeelle
- valtuudet myönnetään ”pienimmän oikeuden” -periaatteen mukaisesti ja oikeuksia rajoitetaan käsittely- ja toimintasäännöillä
- valtuutetut käyttäjät on määriteltävä heidän työtehtävärooliensa avulla henkilöryhminä
- aiempien käyttäjien valtuuden ”kopiointi” uudelle henkilölle ei ole sallittua
- etuoikeutettujen erityisryhmien määrä on rajoitettava vähimmilleen
- tietohallinnon ja muiden etuoikeutettujen ryhmien valtuuksien käyttöä on valvottava
- tietohallintohenkilöstöllä ei saa olla valtuutta käyttäjien dataan
- toimintayksiköillä, henkilöstöhallinnolla ja järjestelmien turvallisuusvastaavilla tulee olla kirjallinen kuvaus toimenpiteistä, joilla henkilöstön tehtävien muutokset ja työsuhteen päättymiset huomioidaan heidän valtuuksiensa muuttamisena tai perumisena. Käyttövaltuuksien ajantasaisuus tulee tarkastaa säännöllisesti
- järjestelmien hallintatietojen muutoksia on seurattava säännöllisesti
- käyttäjien dataa ja käyttövaltuustoimenpiteitä koskevien valtuuksien tulee perustua hyväksyttyyn tietojen luokitussuunnitelmaan (data classification scheme).

4.5.2 Valtuutuksen rajoituksia

Pääsyvaltuutta suojattaviin resursseihin (´objektit´) – tietoihin, tai suojattavia tietoja sisältäviin tietojärjestelmiin, tiloihin tai materiaaliin – tulee rajoittaa objektin turvaluokan mukaan. Pääsyn rajoituksia on tarpeen

a. rajoittaa vuorokauden ajan suhteen (virka-aika, liukuman puitteissa, virka-ajan jälkeen)
b. arvioida sen toistuvuuden perusteella (kertaluonteinen, tilapäinen, satunnaisesti toistuva tai pysyvä)
c. käsitellä tapauskohtaisesti, jolloin kullakin kerralla harkitaan pääsytarve erikseen ja lupa myönnetään kertaluonteisesti
d. arvioida myös sen suhteen, onko henkilöllä oikeus toimia isäntänä muille henkilöille sekä oikeutta päästää muita henkilöitä tietoon

e. asettaa myös pääsyn mahdollistaville välineille (pääsyavainten säilyttäminen ja käsittely)
f. arvioida myös vaarallisten työparien kautta ja rajoittaa henkiöiden oikeutta päästä yksin resursseihin ja edellyttää pääsyn edellyttämien välineiden tai tietojen jakamista useammalle henkilölle yksin tapahtuvan pääsyn estämiseksi.

Pääsyoikeusvaltuutuksen ja siihen liittyvän pääsynvalvonnan mekanismeja voidaan tarkastella henkilöiden kannalta (´subjektit´) ja suojattavien resurssien kannalta (´objektit´).

Pääsyn rajoitusmekanismit jaetaan kolmeen pääryhmään:

- pakollinen pääsyn rajoitus (mandatory access control, MAC)
- valinnainen pääsyn rajoitus (discretionary access control, DAC)
- rooliperusteinen pääsyn rajoitus (role based access control, RBAC).

Pakollisella pääsyn rajoitusmekanismilla (MAC) tarkoitetaan ulkopuolista muodollista valtuutusta suojattavaan objektiin, joka perustuu objektin turvaluokkaan ja asiaryhmään. Subjekti ei itse voi määrittää pääsyoikeuttaan objekteihin. Pakollisen pääsynrajoituksen oleellisin piirre on siis se, että subjektilla ei ole päätösvaltaa muiden tai omiin pääsyvaltuuksiinsa, ei edes subjektin itsensä luomiin tietoihin tai hallinnassaan oleviin tiloihin tai omaisuuteen. Pakollista pääsyn rajoitusmekanismia käytettäessä jokaisella objektilla ja myös subjektilla täytyy olla viiteasiaryhmä (label), jotka valtuutuksella voidaan liittää toisiinsa.

Pakollinen pääsyn rajoitusmekanismi soveltuu parhaiten korkean turvallisuustason resurssien turvaamiseen.

Valinnaisessa pääsyn rajoitusmekanismissa (DAC) objektin haltija päättää subjektien valtuuksista. Valinnaisen pääsyn rajoitusmekanismin edellytyksenä on, että jokaisella objektilla täytyy olla haltija. Valinnainen pääsyn rajoitusmekanismi toteutetaan yleisimmin pääsyoikeuslistoilla (access control list, ACL) tai rooliperusteisesti, joista jälkimmäistä voidaan tarkastella myös omana tyyppinään. Pääsyoikeuslista määrittää tarkasti kuka (´subjekti´) saa päästä mihinkin objektiin ja millaisin toimivaltuuksin.

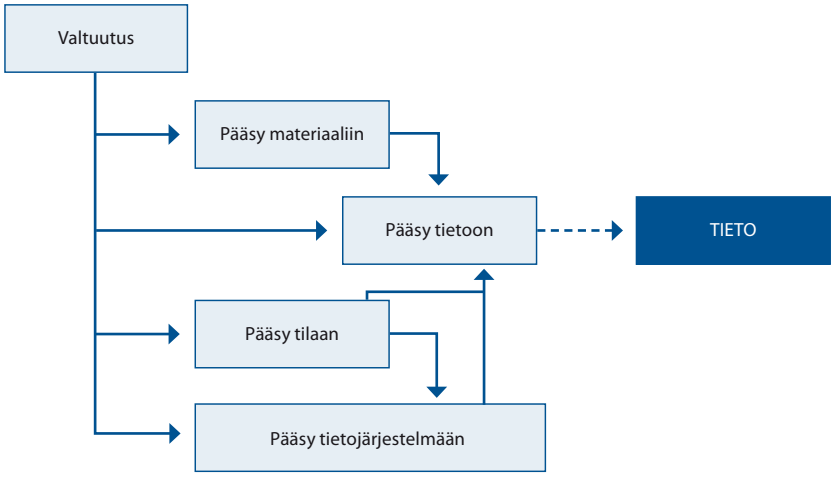
Pääsyoikeuslista on yleisesti käytössä oleva mekanismi, mutta sen ylläpito ja muutosten hallinta on hankalaa.

Rooliperusteinen pääsyn rajoitusmekanismi (RBAC) perustuu henkilöiden (subjektit) työtehtäviin. Kullekin työtehtävälle on määritetty työtehtävän sisältöön liittyvä yleisluonteinen pääsyoikeus. Pääsyoikeus on yleisluonteinen, eikä siinä yksilöidä jokaista objektia.

Rooliperusteinen pääsyn rajoitusmekanismi on yleisin mekanismi ja se soveltuu matalan turvallisuustason resurssien turvaamiseen helpon hallittavuutensa ja yleispätevyytensä johdosta. Rooliperusteinen pääsyn rajoitusmekanismin heikkoutena on vastaavasti sen yleisluonteisuus.

4.5.3 Luokituksen tarve

Kokonaisvaltainen turvallisuusjärjestelmä edellyttää, että tietoja suojataan yhtäläisesti riippumatta tiedon muodosta, käsittelytavasta tai haltijasta.



PIIRROS 2. Pääsy tietoon.

Tietojen luokitus perustuu kansainvälisten aineistojen osalta lakiin kansainvälisistä tietoturvavelvoitteista (588/2004) ja kansallisten aineistojen osalta julkisuuslakiin ja sitä täydentäviin hyvää tiedonhallintatapaa koskevaan asetukseen ja VAHTI-ohjeeseen tietoaineistojen käsittelystä (VAHTI 2/2000). Luokitusta ollaan kehittämässä siten, että kansainvälisten aineistojen jo voimassa oleva neliportainen luokitus on tarkoitus ottaa käyttöön myös kansallisissa aineistoissa. Tällöin turvallisuusluokat ovat

- käyttö rajoitettu -tieto (luokka IV)
- luottamuksellinen tieto (luokka III)
- salainen tieto (luokka II) ja
- erittäin salainen tieto (luokka I).

Tietojen luokitusjärjestelmä on lähtökohta muiden resurssien luokitukselle.

Tiedot voidaan luokitella seuraaviin kriittisyysluokkiin niiden käytettävyyden ja eheysvaatimusten perusteella

- ei-kriittiset tiedot
- merkittävät tiedot (kriittinen)
- erittäin merkittävät tiedot (erittäin kriittinen).

Tietojärjestelmien, tilojen, omaisuuden ja materiaalin sekä henkilöstön **turvallisuusluokat** ja niiden keskinäinen riippuvuus **sääntömatriisina** on esitetty liitteessä 3.

4.5.4 Valtuuspäätös, tarpeen ja sopivuuden selvittäminen

Valtuutus sisältää päätöksen siitä, miksi henkilö on valtuutettava pääsyyn (*tarve*) ja onko henkilö sopiva (*sopivuus*).

Henkilön mahdollisesti aiheuttaman riskin selvittämiseksi on arvioitava henkilön *sopivuus* tehtävään. Sopivuus arvioidaan määrittämällä henkilölle *henkilöstöturvallisuusluokka*.

Valtuus = Sopivuus x Tarve (asiaryhmittäin)

Tarve päästä salassa pidettäviin tietoihin ei ole yleinen, vaan **tarve tulee kohdentaa asiaryhmittäin** julkisuuslain 24.1 § kohdittain ja tarvittaessa yksilöimällä alaryhmittäin. Viraston arkistonmuodostamissuunnitelma (AMS) antaa tähän perusteet. Vaikka henkilöllä olisikin oikeus käsitellä tietyn asiaryhmän salassa pidettäviä tietoja, valtuuttaminen toisiin asiaryhmiin edellyttää tarvetta päästä niiden tietoihin.

Viraston tehtävien turvallisuusluokitus on peruste valtuuspäätökselle. Valtuuspäätös on kirjattava ja tieto päätöksestä on toimitettava asianosaisille. Valtuuspäätökseen tulee aina sisällyttää tarvittavat rajoitukset pääsylle ja pääsynhallinnalle, sen voimassaoloajalle ja aikarajoituksille sekä tunnistevälineiden käytölle ja käsittelylle.

Henkilöstöturvallisuusluokka määrää myös periaatteet, minkä turvaluokan tilaan, tietoon tai tietovarantoon hänellä on oikeus päästä tai perehtyä, sekä minkä turvaluokan laitetta, järjestelmää tai omaisuutta hänellä on oikeus käsitellä.

4.5.5 Valtuutus pääryhmien perusteella

Pääsyoikeuden kannalta henkilöstö voidaan jakaa viiteen henkilöstön pääryhmään heidän turvallisuusstatuksensa mukaisesti:

- Oma turvaluokiteltu henkilöstö (H)
- Turvaluokiteltu palveluntoimittajien henkilöstö (S)
- Turvaluokitellut muut virkamiehet (M)
- Pysyvän, määräaikaisen oikeuden saaneet vierailijat (P)
- Kertaoikeuden saaneet vierailijat (V).

Edellä mainittuja henkilöstöryhmiä on tarkasteltava alaryhmissä heidän senhetkisen työtilansa mukaisesti, onko henkilö työtehtävissä (t) vai vapaa-ajalla (v). Henkilökunnan pääsyoikeudet ja turvallisuusmenettelyt poikkeavat vapaa-aikana siitä, mikä heillä on työtehtävissä. Esimerkiksi työtehtävissä virkamies voi tuoda vieraita virastoon ja toimia heille isäntänä, mutta vapaa-aikana se ei välttämättä ole mahdollista. Samoin virkamies voi vierailla tut-

tavansa luona virastossa, vaikkei se liittyisikään työtehtäviin, mutta silloin se tapahtuu vierailijana. Tämä koskee myös muita henkilöstöryhmiä.

Vierailijat -ryhmän henkilöitä on tarkasteltava myös toiminnallisten tarpeiden mukaan. Vierailija voi olla satunnainen vierailija, jolle myönnetään kertaluonteinen pääsyoikeus (V-lupa) tai hän voi olla työtehtävissään satunnaisesti vieraileva henkilö, jolloin hänelle myönnetään pysyvä, mutta määräaikainen oikeus pääsyyn (P-lupa).

Vieraalla tulee aina olla isäntä, jonka suosituksesta (tarve) vieras valtuutetaan.

4.6 Henkilön sopivuuden arviointi

Henkilön mahdollisesti aiheuttamien riskien arvioinnissa on arvioitava henkilön luotettavuutta, lojaaliutta, vastuullisuutta ja osaamista. Henkilön sopivuuden arviointi sisältää kaksi osaa:

- henkilön arvioinnin ja taustaselvitykset (*henkilön arviointi*)
- poliisiviranomaisen turvallisuusselvityksen (*turvallisuusselvitys*).

Henkilön sopivuus on arvioitava ennen henkilön palvelukseen ottamista. Tarpeen arviointi on kuitenkin aina arvioitava ennen kuin arvioidaan henkilön sopivuutta työhön.

4.6.1 Henkilön arviointi

Henkilön arvioinnin tarkoituksena on selvittää kohteena olevan henkilön kykyä vastata työtehtävän asettamiin osaamis-, vastuullisuus- ja luotettavuusvaatimuksiin. Arvioinnissa voidaan ottaa huomioon

- työtehtäviin liittyvien säädösten tunteminen
- henkilön yleinen koulutustaso
- henkilön perehtyneisyys tehtävään
- henkilön aiempi kokemus ja työhistoria
- henkilön suosittelijoiden lausunnot
- henkilön saama tietoturvakoulutus.

Arviointi perustuu monilta osin yksittäistapauksittain tehtävään harkintaan. Työnantajalla voi olla olemassa myös tiettyjä oman toiminnan kannalta merkittäviä sisäisiä arviointikriteerejä, jotka voivat perustua työtehtävien sisältöön ja tehtävistä suoriutumisen erityisiin vaatimuksiin. Yhtenä tekijänä saattaa olla esimerkiksi– työntekijän oma tai mahdollisesti myös toisten työntekijöiden työturvallisuus. Lisäksi voidaan arvioida henkilön lojaaliutta eli työyhteisön yhteisen edun asettamista oman edun edelle. Arvioinnissa saattaa

olla tarpeen ottaa huomioon myös aikatekijä. Henkilöstöriski ei välttämättä ajan myötä vähene, vaan joidenkin arviointiin vaikuttavien seikkojen osalta tilanne voi olla päinvastoin.

Luotettavuutta ja soveltuvuutta voidaan arvioida myös henkilön työnantajalle toimittaman huumausainetestituloksen perusteella tai turvallisuusselvitysmenettelyssä saapuneen kirjallisen vastauksen kautta.

Henkilön arviointi voidaan toteuttaa pyytämällä kohdehenkilöltä selvityksiä hänen koulutus- ja työhistoriastaan ja järjestämällä ryhmähaastattelu sekä mahdollisesti hankkimalla hänestä asiantunteva psykologinen henkilöarviointi. Psykologisten arviointien käyttäminen tulee arvioida huolella.

4.6.2 Turvallisuusselvitykset

Turvallisuusselvitysmenettelyllä työnantaja pyrkii henkilöstöturvallisuuden varmistamiseen; ennaltaehkäisemään sellaisia rikoksia, jotka vakavasti vahingoittaisivat Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta, poikkeusoloihin varautumista tai edellä mainittujen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta (JulkL § 24.1 kohdat 1,2,5 ja 8-11).

Turvallisuusselvitys voidaan tehdä perusmuotoisena, suppeana tai laajana ja se voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä. Virkaa tai tehtävää jo hoitavasta henkilöstä selvitys tehdään kuitenkin yleensä vain, mikäli hänen työtehtävissään tapahtuu olennaisia muutoksia. Tällainen tilanne voi olla käsillä mm. silloin, kun henkilö pääsee käsiksi aikaisempaa suurempaan määrään turvaluokiteltua tietoa ja materiaalia.

Turvallisuusselvityksiä käytetään koulutukseen haun lisäksi kahteen päätarkoitukseen. Ensimmäinen on uuden palkattavan henkilöstön rekrytointi ja toista käytetään yleensä silloin, kun tilaan tai tietoon pääsyn tarve perustuu esimerkiksi ulkopuolisen yrityksen kanssa tehtyyn alihankintasopimukseen. Tällaisia sopimuksia yksityisten tahojen kanssa tehdään esimerkiksi tietoliikenteen, kiinteistöhuollon tai tavarantoimitusten hoitamisesta. Näissä tilanteissa on turvallisuusselvityslain edellyttämien kriteerien puitteissa mahdollisuus laatia turvallisuusselvitys niistä henkilöistä, joita ulkopuolinen sopimuskumppani käyttää sopimuksen täyttämiseen. Viimekädessä ratkaisun turvallisuusselvityksen laatimisesta tekee toimivaltainen viranomainen, eikä ratkaisu ole valituskelpoinen.

Turvallisuusselvitystä haetaan toimivaltaiselta viranomaiselta kirjallisesti siihen tarkoitukseen erikseen varatulla lomakkeella, jossa menettelyn kohteena oleva henkilö antaa selvitysmenettelyyn etukäteen kirjallisen suostumuksensa. Selvitystä tehtäessä siihen saadaan kirjata tietoja ainoastaan sellaisista viranomaisrekistereistä, jotka mainitaan turvallisuusselvityslaissa. Siinä ei saa käyttää vihjetietoa tai ilmiantoja, eikä merkintöjä joiden mukaan henkilön voidaan epäillä syyllistyvän rikokseen. Viranomaisen hallussa olevia muita tietoja koh-

dehenkilöstä voidaan käyttää eri rekistereistä löytyvän tietojen oikeellisuuden tarkistamiseksi, mikäli se yksittäistapauksessa on välttämätöntä. Selvityksessä ei myöskään käytetä kymmentä vuotta vanhempia tietoja tai tietoja alle viittätoista vuotta nuorempana tehdystä teosta, ellei niiden käyttäminen ole välttämätöntä selvityksen tarkoituksen saavuttamiseksi.

Toimivaltainen viranomainen harkitsee selvitystä laadittaessa tietojen käytettävyyden kussakin yksittäistapauksessa erikseen. Mikäli kohdehenkilöä koskevalla rekisterimerkinnällä ei ole tarkoituksenmukaista yhteyttä hakijan hakemuksessa ilmoitettuun tarkoitukseen, voidaan tieto jättää ilmoittamatta turvallisuusselvitysmenettelyssä annettavassa suullisessa tai kirjallisessa vastauksessa. Tämä tarkoittaa siis sitä, että turvallisuusselvityksestä saatava vastaus ei ole yhtä kuin kaikki kohdehenkilöstä löytyvä rekisteritieto.

Turvallisuusselvitys itsessään ei sisällä arvioita kohdehenkilön luotettavuudesta tai sopivuudesta, **eikä sen sisältö sido selvityksen hakijaa**. Henkilön luotettavuuden, lojaaliuden ja vastuullisuuden **arvioinnin tulee tapahtua ottamalla arvioinnissa huomioon muita näkökohtia**. Joidenkin tehtävien kannalta työnantajalla voi olla olemassa tiettyjä toiminnan kannalta merkittäviä sisäisiä arviointiperusteita. Turvallisuusselvityksessä ilmoitetut tiedot saattavat vahvistaa tai heikentää näitä arviointiperusteita, ja siksi selvitys tulisikin aina käsittää esimerkiksi rekrytoinnissa vain yhtenä tekijänä kokonaisarvioinnissa. Myös tämän näkökohdan vuoksi hakijan edustajan tulee olla nimetty ja tehtäväänsä koulutettu yhteyshenkilö. Tällä järjestelmällä pyritään takaamaan lisäksi kohdehenkilön yksityisyyden suojaa lain edellyttämällä tavalla, koska turvallisuusselvityslain mukaisesti selvityksiä saavat käsitellä vain ne, joiden työtehtäviin se kuuluu. Selvitystä voidaan käyttää vain turvallisuusselvityshakemuksessa ilmoitettuun tarkoitukseen. Selvitys on hävitettävä heti, kun se ei enää ole tarpeen selvitystä haettaessa ilmoitetun käyttötarkoituksen kannalta.

Mikäli selvitysmenettelyssä ei ole ilmennyt hakemuksen tarkoituksen kannalta merkittävää rekisteritietoa, voidaan vastaus antaa hakijalle suullisesti. Käytännössä se tapahtuu puhelimitse. Muussa tapauksessa toimivaltainen viranomainen toimittaa hakijalle vastauksen kirjallisesti. Hakija saa itse antaa kohdehenkilölle tiedon suullisen vastauksen sisällöstä, mutta mikäli vastaus on saapunut hakijalle kirjallisena, on kohdehenkilön tiedusteltava selvityksen sisältöä toimivaltaiselta viranomaiselta. Kysely tehdään aina kirjallisesti. Tiedonsaantioikeus ei kuitenkaan koske sellaista tietoa, joka on peräisin rekisteristä, johon rekisteröidyllä ei lain mukaan ole tarkastusoikeutta. Tällaisia rekistereitä ovat mm. Pääesikunnan tutkintaosaston turvallisuustietorekisteri sekä Suojelupoliisin toiminnallinen tietojärjestelmä. Tietosuojavaltuutetulla on kuitenkin aina oikeus tutustua turvallisuusselvitykseen sen lainmukaisuuden tarkistamiseksi.

Silloin, kun tilaan tai tietoon pääsyn tarve perustuu ulkopuolisen yrityksen kanssa tehtyyn sopimukseen, toimii turvallisuusselvityksen hakijana yhteisö,

jonka tilasta tai tiedosta on kysymys. Näissä tilanteissa ulkopuolisen sopimuskumppanin sopimuksen täyttämiseen käyttämästä henkilöstöstä tehdyt selvitykset palautuvat hakijalle, eikä varsinaisella työntekijän palkkaavalla ulkopuolisella yrityksellä ole oikeutta saada tietoa selvityksen sisällöstä.

Turvallisuusselvitysmenettelyn käyttö ei kuitenkaan korvaa työnantajan mahdollisuuksia käyttää rekrytoinnissa esimerkiksi lain yksityisyyden suojasta työelämässä mukaisia keinoja. Näiden tietojen keräämisen tulisi tapahtua ensisijaisesti työntekijältä itseltään ja tietojen sisällöstä keskustelemista ei ole rajattu samalla tavoin kuin turvallisuusselvityksessä olevien tietojen osalta on kyse.

Paikallispoliisin tekemät turvallisuusselvitykset ja hakeutuminen turvallisuusselvitysmenettelyyn on esitetty liitteessä 4.

4.7 Kansainvälinen henkilöturvallisuustodistus

Suomen kansainväliseen poliittiseen, sotilaalliseen, kauppapoliittiseen tai kehitysyhteistyöhön osallistumisen edellyttämät henkilöturvallisuusselvitykset kuuluvat ns. National Security Authority (NSA) sopimusjärjestelmän piiriin. NSA-järjestelmän peruspilarit ovat Suomen ja NATO:n välisen Partnership for Peace -sopimuksen turvallisuusosio, Euroopan Unionin turvallisuussäännöstö (luku 3.6), Euroopan avaruusjärjestön turvasopimus sekä Suomen tekemät kahdenväliset valtiotason turvallisuussopimukset. Mm. näiden kansainvälisten tietoturvavelvoitteiden voimaansaattamiseksi säädettiin vuonna 2004 laki kansainvälisistä tietoturvavelvoitteista (588/2004). Suomelle aiheutuvien velvoitteiden täyttämisestä vastaa ulkoasiainministeriön turvallisuusyksikköön sijoitettu National Security Authority (NSA) sekä Designated Security Authority (DSA) -viranomaisina puolustusministeriö, pääesikunta ja suojelupoliisi.

Jotta henkilö voi päästä kotimaassa käsiksi kansainväliseen turvaluokiteltuun tietoon tai osallistua ulkomailla järjestettäviin turvaluokiteltuihin kokouksiin, edellyttävät kansainväliset tietoturvavelvoitteet aina arviota henkilön luotettavuudesta ja sopivuudesta. Arvio pohjautuu turvallisuusselvitysmenettelyyn, jonka perusteella NSA tai DSA -viranomainen myöntää henkilölle turvallisuustodistuksen (Personal Security Clearance, PSC).

NATO- ja EU varmistavat säännönmukaisin tarkastuksin, että Suomessa noudatettu henkilöturvallisuustodistusmenettely täyttää sille asetetut kansainväliset vaatimukset. Menettelyssä mahdollisesti ilmenevät puutteellisuudet voivat johtaa ulkomaisen salassapitoluokitellun tiedon saannin oleelliseen vaikeutumiseen tai tiedonsaannin tyrehtymiseen.

Ulkoasianministeriön turvallisuusyksikkö koordinoi kansainvälisten henkilöturvallisuustodistusten myöntämismenettelyä.

4.8 Henkilöriskien tarkastuslista

Lainsäädäntö velvoittaa huolehtimaan työntekijöiden turvallisuudesta. Tähän huolehtimisvelvollisuuteen kuuluu, että avainhenkilöihin kohdistuviin riskeihin varaudutaan. Tällöin on kuitenkin huolehdittava, että yksityisyyden suojaa ei loukata.

Virastolla tulee olla selkeät ohjeet niistä toimenpiteistä, jotka on tehtävä henkilön työsuhteen päättyessä.

4.8.1 Työntekijän palvelukseen otto

1. määrittele tehtävä, vastuut ja oikeudet sekä velvollisuudet
2. selvitä hakijan soveltuvuus tehtävään (psykologiset testit edellyttävät työntekijän suostumusta)
3. tarkasta työhistoria henkilöltä itseltään ja pyydä työtodistukset
4. tarkasta koulutustausta koulu- ja tutkintotodistuksista
5. selvitä hakijan taloudellinen tilanne (edellyttää hakijan suostumusta)
6. tarkasta yrityskytkennät YTJ-rekisteristä
7. ota yhteyttä suosittelijoihin, jotka on mainittu työhakemuksessa
8. mahdollisesti lisäksi turvallisuusselvitys sekä huumausainetestaus, jos siihen on edellytykset

4.8.2 Palvelussuhteen aikana

Turvallisuusvastaavilla tulee olla kirjallinen kuvaus toimenpiteistä, joilla henkilöstön tehtävien muutokset ja työsuhteen päättymiset huomioidaan.

4.8.3 Työsuhteen päättyessä

1. järjestä lähtöhaastattelu
2. poista käyttö- ja kulkuoikeudet
3. velvoita palauttamaan materiaali ja muu omaisuus
4. muistuta salassapitovelvoitteesta
5. sähköpostin ja tietoaineistojen käsittely
6. siirrä tietopääoman sijaiselle, huolehdi dokumentoinnista
7. työtehtävien luovutus seuraajalle tai sijaiselle
8. tiedota henkilön lähdöstä viraston henkilöstölle

4.9 Valtuutusprosessin turvallisuus (luvitus)

Valtuutusprosessi on henkilöstöturvallisuusprosessi, joka on **turvattava erityisen huolellisesti käsittelyketjujen turvaohjausmekanismeilla**. Henkilöiden roolit on eriytettävä, kriittisiä suorituksia on valvottava kahden tai useamman henkilön toimesta, arkaluonteisimmat valtuustiedot on jaettava useamman henkilön kesken ja ketjun eriytetty valvonta on toteutettava.

Luvitusprosessi on esitetty yksityiskohtaisesti valtiovarainministeriön VAHTI-ohjeessa 9/2006 ”Käyttövaltuushallinnan periaatteet ja hyvät käytännöt”.

4.10 Ostopalvelujen turvallisuus

4.10.1 Palvelut ja alihankintaketjujen palveluntuottajat

Nykyisin yhä merkittävämpi osa virastojen palveluista tuotetaan ostopalveluina. Ostopalvelut muodostavat usein laajoja alihankintaketjuja, joissa varsinainen palvelun tuottaja ja sen henkilöstö saattavat jäädä huomioimatta. Palveluhenkilöstön turvallisuudesta varmistuminen on henkilöstöturvallisuustyön keskeinen haaste.

Palvelun tilaajalla tarkoitetaan tässä virastoa ja muita sen valtuuttamia toimijoita, jotka tilaavat huolto- ja ylläpitopalveluita.

Palvelun tuottajalla tarkoitetaan tässä huolto- ja ylläpitopalveluja tuottavia yrityksiä, joiden henkilöstö säännöllisesti tuottaa palvelua viraston tiloissa.

4.10.2 Turvallisuus- ja salassapitosopimukset

Palveluyritysten kanssa tulee tehdä turvallisuus- tai salassapitosopimus. Turvallisuussopimus on laajempi koko yritystä ja sen turvallisuutta koskeva sopimus ja salassapitosopimuksella huolehditaan erityisesti henkilöstöturvallisuusjärjestelyistä. Salassapitosopimus voidaan tehdä myös yksittäisten henkilöiden kanssa.

Sopimus on luonteeltaan viraston ja yrityksen välinen turvallisuusjärjestelyjä koskeva yleissopimus. Sopimuksessa määritellään sopijaosapuolten kesken noudatettavat turvallisuusjärjestelyt. Sopijaosapuolet sitoutuvat noudattamaan sopimusta kaikissa hankkeissa ja palveluissaan, joissa käsitellään salassa pidettävää tietoa, asiakirjoja ja materiaalia. Sopimuksen allekirjoittamisen jälkeen yrityksellä on mahdollisuus sopimuksen määrittämissä rajoissa valmistella ja toteuttaa viraston kanssa erikseen määritettäviä hankkeita.

Yritys sitoutuu pitämään salassa kaikki sille luovutetut ja sillä olevat salassa pidettäväksi säädetyt tai sellaisiksi lain nojalla määrätyt tiedot. Salassa pidettävästä tiedosta, asiakirjasta ja materiaalista saa antaa tiedon vain erikseen

nimetyille henkilöille. Salassapitovelvollisuus on voimassa myös sopimuksen päättymisen jälkeen.

Sopimuksessa yritys sitoutuu säilyttämään ja käsittelemään työhön liittyviä tietoja, asiapapereita, laitteita, koneita, valokuvia, työpiirustuksia, tietolevyjä ja vastaavia salassa pidettäviä tavaroita siten, että ne pysyvät vain käsittelyoikeuden omaavien hallinnassa, eivätkä joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

Sopimuksella pitää myös rajoittaa tietojen ja materiaalin valokuvaus, kopiointi, vieminen pois toimitiloista tai muistiinpanojen tekeminen salassa pidettävistä tiedoista. Sopimuksen päätyttyä yhteisesti sovittavana ajankohtana sopijaosapuolet mahdollisine alihankkijoineen palauttavat kaikki toimeksiantoon liittyvät dokumentit, tallenteet ja materiaalin tai tuhoavat ne sovitulla tavalla.

Yrityksen on huolehdittava, ettei viraston suojelukohteiden tai toiminnan turvallisuus vaarannu yrityksen henkilöstön huolimattomuuden, virheellisten työtapojen tai muun toiminnan johdosta.

Yritys saattaa viraston kanssa yhteistyötä tekevän ja sopimuksen vaikutusalaan kuuluvan henkilöstönsä tietoiseksi sopimuksen salassapitovelvoitteista sekä sitoutuu valvomaan, että henkilöstö noudattaa sopimusta. Yritys voidaan velvoittaa toimittamaan sopimuksen kohteena olevaan toimintaan liittyvän henkilöstönsä täyttämät ja allekirjoittamat henkilötiedot virastolle turvallisuusselvityksen tekemistä varten (laki turvallisuusselvityksistä, 177/2002) turvallisuusselvityshakemuslomakkeella. Selvitys tehdään henkilöistä, jotka käsittelevät työssään tämän sopimuksen kohteena olevia salassa pidettäviä tietoja tai joilla on pääsy sellaisiin viraston hallinnassa oleviin tiloihin, joissa liikkumista on turvallisuussyiden perusteella syytä rajoittaa. Yhteistyöhön nimettävän ja viraston hyväksymän henkilöstön tulee tehdä vaitiolovakuutus ennen kaupallisen pääsopimuksen syntyä.

Mikäli yritys käyttää alihankkijoita, aliurakoitsijoita tai muita palvelujen toimittajia viraston yhteishankkeissa, tulee sen hyväksyttää alihankkijat ja niiden yhteistoimintaan osallistuva henkilöstö sovittujen menettelyjen mukaisesti ennen aliurakointi- tai muun sopimuksen tekemistä sillä edellytyksellä, että alihankkija käsittelee salassa pidettävää tietoa tai toimii tiloissa, joissa käsitellään salassa pidettävää tietoa. Mikäli edellä kuvatut ehdot täyttyvät, yrityksen tulee tehdä alihankkijansa kanssa turvallisuussopimus. Yrityksen on tiedotettava alihankkijalleen, että turvallisuusjärjestelyjen saattamisesta viraston vaatimalle tasolle saattaa syntyä kustannuksia.

Yritys tai sen alihankkijat saavat mainita referenssinä tehneensä työtä virastolle ainoastaan, jos asiasta on erikseen kirjallisesti sovittu.

Yrityksen tulee toimittaa yrityksen turvallisuuskartoitus ja -ohjeistus virastolle.

Viraston tulee varata oikeus tarkastaa etukäteen ilmoitettuna ajankohtana yrityksen turvallisuusjärjestelyjä sitä koskevilta osilta. Yritys on myös velvollinen ilmoittamaan virastolle, jos sen omistussuhteissa, viraston kannalta kes-

keisissä toiminnoissa, henkilö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai yritykseen kohdistuu turvallisuutta tai poikkeusoloihin varautumista mahdollisesti uhkaavia toimenpiteitä, esimerkiksi yhteydenottoja tai tietomurtoyrityksiä.

Yrityksen kanssa tulee sopia tarkoin yhteyshenkilöt sopimuksen toteuttamiseen liittyvissä kysymyksissä. Yhteyshenkilöt vastaavat sopimuksen tarpeellisesta päivittämisestä. Päivittämistarve on arvioitava yhteyshenkilöiden kesken vähintään kahden vuoden välein.

Viraston kanssa erikseen sovittavissa hankkeissa ja yhteistoimintajärjestelyissä tulee määritellä yksityiskohtaisemmat turvallisuusjärjestelyt kunkin hankkeen edellyttämässä laajuudessa. Hankkeen sopimuspapereihin tulee liittää kyseistä hanketta koskeva turvallisuusliite.

4.10.3 Vaitiolositoumus

Palveluntuottajien henkilöstön, palveluhenkilöiden, tulee tehdä sitoumus vaitiolosta. Sitoumuksen tarkoituksena on varmistaa, että palveluhenkilö ymmärtää salassapitovelvoitteensa.

4.10.4 Palvelun tuottajien määräaikaiset pääsyluvat

Palveluntuottajien huolto- ja ylläpitohenkilöstölle on tarpeen myöntää määräaikaisia kulkulupia (P-lupa) silloin, kun henkilö säännöllisesti tarvitsee oikeuden liikkua viraston tiloissa. Tämän menettelyn piiriin eivät kuulu tapauskohtaiset käynnit ja vierailut (V-lupa).

Palveluja tuottavien yritysten osalta luvan myöntämisen edellytyksenä on

- palvelusopimus tai työtilaus
- siihen liittyvä turvallisuussopimus, salassapitosopimus tai vaitiolositoumus
- tarvittaessa turvallisuusselvitys
- todennettu palvelutehtäväntehtävän edellyttämä jatkuva tarve päästä tiloihin.

Pysyvä pääsylupa turvallisuusluokiteltuihin rajoitustiloihin edellyttää eräissä tapauksissa suppeaa turvallisuusselvitystä. Pääsy poikkeusolojen varalle ja erikoistarkoituksiin rakennettuihin tiloihin salassapito- ja turvallisuusjärjestelyistä johtuen edellyttää yleensä perusmuotoista turvallisuusselvitystä.

Palveluhenkilöt tulee rekisteröidä (akkreditointi).

Palvelun tuottajien tulee ilmoittaa palvelun tilaajalle tiedot niistä henkilöistä, joilla on palvelun tuottamiseksi välttämätön tarve päästä säännöllisesti viraston tiloihin. Palveluhenkilö täyttää turvallisuusselvityshakemuksen kohdan ”Selvityksen kohteena olevan henkilön tiedot” palvelun tilaajan antamien ohjeiden mukaisesti, allekirjoittaa hakemuksen ja toimittaa sen palvelun tilaajalle.

Palvelun tuottajalle ilmoitetaan lupapäätöksestä, jonka jälkeen pääsyyn oikeutettu henkilö rekisteröityy viraston rekisteröintipisteessä. Rekisteröitymisessä hänen henkilöllisyytensä ja tietonsa todennetaan, hänet kuvataan sekä hänelle valmistetaan kuvallinen henkilötunniste ja henkilökohtainen kulkukortti.

Palvelun tilaajalla on keskeinen rooli luvitusmenettelyssä. Palvelun tuottaja toimittaa tiedot palveluhenkilöistään palvelun tilaajalle, jonka tulee tarkastaa ne ja arvioida palveluhenkilön pääsyn tarpeellisuus viraston tiloihin. Pääsyyn oikeutettujen henkilöiden määrä on pidettävän kohtuullisen pienenä. Erityisesti on arvioitava päivystys- ja varalla olevan henkilöstön määrää.

Turvallisuusselvityshakemuksen asianmukainen täyttäminen on ehdottoman välttämätöntä sekä käsittelyn että henkilöiden oikeusturvan kannalta. Palvelun tilaajan tulee tarkastaa palveluhenkilön toimittaman turvallisuusselvityshakemuksen tiedot. Palvelun tilaaja täyttää hakemuksen kohdan ”Tehtävään liittyvät tiedot” ja määrittää henkilön tehtävänimikkeen ja merkitsee kohtaan ”Osasto tai yksikkö” oman virastonsa yksikön ja osaston. Kohta ”Tarkka tehtäväkuvaus” on täytettävä huolella siten, että siitä ilmenee **miksi tehtävä on niin merkittävä, että henkilöstä on tehtävä turvallisuusselvitys**. Palvelun tilaajan on liitettävä hakemukseen asiaa käsittelevä yksityiskohtainen liite. Kohta ”Arkaluontoisen tilan tai paikan kuvaus” on myös täytettävä. Tarvittaessa liitetään mukaan liiteasiakirja.

Selvityksen hakijan tiedot -kohta voi olla esitäytetty. Hakijalla tarkoitetaan virastoa, joka on sopinut turvallisuusselvitysmenettelystä poliisiviranomaisen kanssa.

Kiireellisessä tilanteessa palvelun tuottajan henkilöstölle voidaan myöntää tapauskohtaisesti poikkeuslupa päästä tiloihin. Palveluhenkilöllä tulee saapuessaan olla virallinen henkilöllisyystodistus tai muu sovittu tunniste.

4.11 Valtuutuksen siirtäminen ja hallinnointi

Pääsyoikeuden täytyy perustua valtuutukseen.

Yleensä valtuutettaessa voidaan antaa ainoastaan yleisvaltuutus, jota tarkennetaan luvitusprosessissa. Valtuuksien hallinnointi voi olla hajautettua, jolloin paikallisten käyttövaltuushenkilöiden tulee toimia keskitetyn valtuushallintapolitiikan mukaisesti ja heidän toimiaan on valvottava.

Valtuuttajana voi toimia ainoastaan tähän kirjallisesti valtuutettu henkilö, yleensä toimintayksikön päällikkö, joka joko omistaa tai toimii tiedon hallussapitäjänä virastossa. Valtuuttamisessa tulee käyttää vakioituja toimintatapoja ja valtuutus on vahvistettava kirjallisesti. Sähköisessä valtuutuksessa on käytettävä digitaalista allekirjoitusta valtuutuksen eheyden ja kiistämättömyyden takaamiseksi.

Valtuudet kirjataan *käyttäjä- ja valtuustietorekisteriin*.

Valtuutus voidaan siirtää kohdevirastolle tai kohdejärjestelmiin:

1. henkilökohtaisesti toimittamalla valtuuskirje (akkreditiivi) kohdevirastoon (*akkreditointi*)
2. välittämällä käyttäjä- ja valtuustiedot järjestelmien välityksellä (*provisionti*).

4.11.1 Käyttäjä- ja valtuustietorekisteri

Käyttäjä- ja valtuustiedot tallennetaan pääsynvalvontaa varten käyttäjä- ja valtuustietorekisteriin.

Käyttäjätiedot sisältävät tiedot käyttäjästä (identiteetti) ja hänen *tunnistetietonsa*, joilla henkilö voidaan tunnistaa. *Henkilöllisyys* eli identiteetti (identity) on joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan tunnistaa. *Valokuva*, josta henkilö on tunnistettavissa, on laissa tarkoitettu henkilötieto.

Valtuustiedot (crentials) ovat tietoja henkilön valtuuksista.
Käyttäjä- ja käyttövaltuusrekisteristä on laadittava tietosuojaseloste.

4.11.2 Akkreditointi ja rekisteröiminen

Akkreditoinnissa henkilön valtuus (akkreditiivi) saatetaan tiedoksi kohdevirastoon tai kohdejärjestelmästä vastaavalle. Akkreditoinnin kohdevirasto tai -järjestelmän vastaavalle luovutetaan valtuutus, kirjataan ja tarkistetaan *tunnistetiedot* ja viedään kohdejärjestelmään tai muun kulunvalvontajärjestelyn käyttöön tunnistamista varten.

Akkreditoinnin yhteydessä mahdollisesti luovutetaan tunnistamisessa ja todentamisessa tarvittava *tunnisteväline tai -tieto* rekisteröidylle. Rekisteröinnissä kirjataan kohdejärjestelmään vertailutieto, jota vertaamalla henkilön antamiin tietoihin voidaan todentaa henkilön aitous (autentikointi).

Viraston ulkopuolella valmistettujen tunnistevälineiden ja tunnistetietojen (salasana) toimittaminen rekisteröitymispisteeseen on turvattava. Lähtökohtaisesti ne toimitetaan eri kanavia käyttäen ja niiden antamaa käyttöoikeutta ei saa paljastaa rekisteröijälle.

4.11.3 Henkilörekisterin pitäminen

Henkilötiedolla tarkoitetaan ”kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi” (HetiL 3 § 1 kohta). Tämän määritelmän nojalla mm valokuvan, josta henkilö on tunnistettavissa, katsotaan olevan laissa tarkoitettu henkilötieto. Tämä tulkinnallinen lähtökohta on vahvistettu lainsäädännön esitöissä (HE 96/1998, s. 35) sekä tietosuojalautakunnan käytännössä (mm. tietosuojalautakunnan päätös 1/25.2.2002).

Tarkastuksen tekemisestä voidaan tehdä merkintä henkilötietojärjestelmään.

Tunnistettavuuden arviointia on tarkasteltava objektiivisesti. Koska arviointiin liittyen ei ole toistaiseksi olemassa laajaa ennakkokäytäntöä ja sitä on muutoinkin vaikea yleispätevästi soveltaa, voidaan arvioinnin jonkinlaisena lähtökohtana pitää Euroopan neuvoston hyväksymiin eri aloja koskeviin tietosuojasuosituksiin sisältyvää kriteeriä, jonka mukaan henkilöä ei pidetä tunnistettavissa olevana, jos tunnistaminen vaatii kohtuuttomasti aikaa, kustannuksia ja työtä (tietosuojalautakunnan päätös 13/4.6.1990).

Henkilötietolain soveltamisen kannalta merkitystä on myös henkilörekisterin käsitteellä ja vaatimuksella määritellä henkilötietojen käsittelyn tarkoitus (henkilörekisterin käyttötarkoitus). Henkilötietolakia sovelletaan kaikkeen henkilötietojen automaattiseen käsittelyyn sekä muuhun henkilötietojen käsittelyyn ”silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa” (HetiL 2.2 §). *Henkilörekisterillä* tarkoitetaan ”käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta” (HetiL 3 § 3 kohta). Henkilötietolain 6 §:n mukaan henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. Määritelty käsittelyn tarkoitus on keskeinen toiminnan laillisuuden arvioimisen kannalta (ks. kappale 3). Lain

nojalla **henkilötietolain säädöksiä sovelletaan lähtökohtaisesti siis kaikenlaiseen valokuvien käsittelyyn, jossa valokuvia, joissa esiintyy tunnistettavissa olevia henkilöitä, käsitellään tai järjestetään edellä kuvatulla tavalla**.

Henkilötietolain käsitteistön mukaan valokuvia edellä mainitulla tavalla käsittelevän tahon katsotaan olevan kuvia sisältävän henkilörekisterin *rekisterinpitäjä* (HetiL 3 § 4 kohta), jota koskevat laissa tarkemmin säädetyt velvollisuudet.

Henkilötietolaki sisältää myös luettelon **poikkeuksista**, jolloin lakia ei sovelleta. Tällaisia poikkeuksia ovat muun muuassa henkilötietojen käsittely henkilökohtaisiin tai tavanomaisiin yksityisiin tarkoituksiin, esimerkiksi kuvien, myös kännykkäkameran kuvien, ottaminen ja järjestäminen omaan valokuva-albumiin tai omaan tietokonetiedostoon, sanomalehdissä tai muissa tiedotusvälineissä julkaistujen kuvien kokoaminen (lehtileikkeiden kerääminen), valokuvien käyttäminen toimituksellista tarkoitusta varten sekä valokuvien käsittely taiteellisen tai kirjallisen ilmaisun tarkoituksessa (valokuvanäyttelyn järjestäminen tai kirjan kuvituksen toteuttaminen).

Valokuvien käsittely on oikeudelliselta kannalta sidoksissa useisiin eri perusoikeuksiin, kuten yksityisyyden suojaan, sananvapauden käyttöön, tekijänoikeuteen sekä julkisuusperiaatteeseen silloin, kun valokuva on osana viranomaisen asiakirjoja.

Valokuvien käsittelystä on myös nimenomaisesti säädetty joissakin erityislaeissa, jolloin näiden lakien säännökset syrjäyttävät siltä osin henkilötietolain soveltamisen. Erityislakeja ja säännöksiä ovat mm. laki henkilötietojen käsittelystä poliisitoimessa (761/2003), henkilökorttilaki (829/1999) ja laki ajoneuvoliikennerekisteristä (541/2003) ja valtioneuvoston asetus yleisistä turvallisuuspalveluista (534/2002).

Henkilötietolain 5 §:n huolellisuusvelvoitteen mukaan ”Rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa, sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta”. Yhtä tärkeänä yleisenä lähtökohtana **henkilötietolain 6 §:n suunnitteluvelvoitteen** nojalla on, että henkilötietojen käsittelyn tulee olla aina asiallisesti perusteltua rekisterinpitäjän laillisen ja hyväksyttävän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset, sekä säännönmukaiset tietolähteet ja tietojen luovutukset on myös suunniteltava ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. *Silloin kun kuvien saattaminen yleisesti saataville loukkaa jotakin nimenomaista lain säännöstä tai kuvan kohteena olevan henkilön jossain muussa laissa suojattua oikeutta, ei tämän henkilötietolain 6 §:n asettama tietojen käsittelyn asiallisen perusteltavuuden yleinen edellytys voi koskaan täyttyä*. Hyväksyttävän perusteen keskeisyyttä korostaa myös se, että tämän perusteen on oltava voimassa valokuvia ajatellen myös kuvaustilanteessa; esim. kunniaa loukkaavan sekä kärsimystä tai halveksuntaa kuvan kohteelle aiheuttaman valokuvan ottamista voi pitää jo lähtökohtaisesti lain vastaisena.

Valokuvien liittämistä rekisteriin tarpeettomasti, eli vastoin henkilötietolain **9 §:n 1 momentin tarpeellisuusvaatimusta,** ei pidetä hyvän tietojenkäsittelytavan ja henkilötietolain mukaisena.

Edellä mainittujen henkilötietolain yleisvelvoitteiden ohella on ensisijaisesti huomioitavaa myös se, että henkilötietolain **8 §:n 1 momentin mukaan henkilötietojen käsittely voi perustua ainoastaan laissa määriteltyyn perusteeseen**. Näitä perusteita ovat:

1) rekisteröidyn yksiselitteisesti antama suostumus (HetiL 8.1 § kohta 1)
2) asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen luoma asiallinen yhteys (Hetil 8.1 § kohta 5)
3) jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta (HetiL 8.1 § kohta 4).

Myös henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavia yleisesti saatavilla olevia tietoja on mahdollisuus käsitellä oikeuksien ja etujen turvaamisen tarkoituksessa. (HetiL 8.1 § kohta 8) Valokuviin henkilötietolaki liittyy yleensä tilanteissa, joissa kuva on osana henkilörekisteriä.

Lakiin perustuvasta oikeudesta on esimerkiksi kysymys, kun valokuvia kerätään ja talletetaan passilain nojalla passin myöntämistä varten.

Valokuvan tallettaminen henkilörekisteriin liittyy usein henkilötietolain 8 §:n 1 momentin 5 kohdan mukaisiin tilanteisiin, joissa rekisterinpitäjän ja rekisteröidyn välillä on *asiallinen yhteys*. Esimerkkinä voidaan mainita henkilöstöhallinnon rekisteri, joihin tietyillä edellytyksissä voi olla tarpeen tallettaa työntekijöiden tai tietyssä asemassa olevien työntekijöiden valokuvia. Valokuvan tulee olla tarpeellinen rekisterin käyttötarkoituksen kannalta. Valokuvan tallettamiselle rekisteriin tulee myös olla erityinen tarkoitus, kuten esim. henkilön tunnistaminen tai yksilöitävyyden parantaminen. Valokuvan käyttäminen voi olla tarpeellista tietyin edellytyksin esim. työpaikan kulkukorteissa tunnistettavuuden varmistamiseksi.

Tässä yhteydessä voidaan nostaa myös erityisesti esille *suostumus* henkilötietojen käsittelyyn oikeuttavana perusteena. Henkilötietolaissa määrääväksi periaatteeksi omaksutun itsemääräämisoikeuden mukaisella suostumuksella tarkoitetaan henkilötietolain 3 §:n 7 kohdan mukaan ”kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn”. Suostumuksen ei välttämättä tarvitse olla kirjallinen, mutta muun muassa suostumuksen tietoisuusvaatimuksen tueksi henkilötietolaissa on säädetty henkilötietojen kerääjälle/käsittelijälle **informointivelvoite.** Henkilötietolain 24 §:n mukaista informointivelvoitetta tulee noudattaa pääsääntöisesti aina kun henkilötietoja kerätään. Henkilötietolain 24 §:n 1 momentissa todetaan: ”Rekisterinpitäjän on henkilötietoja kerätessään huolehdittava siitä, että rekiste-

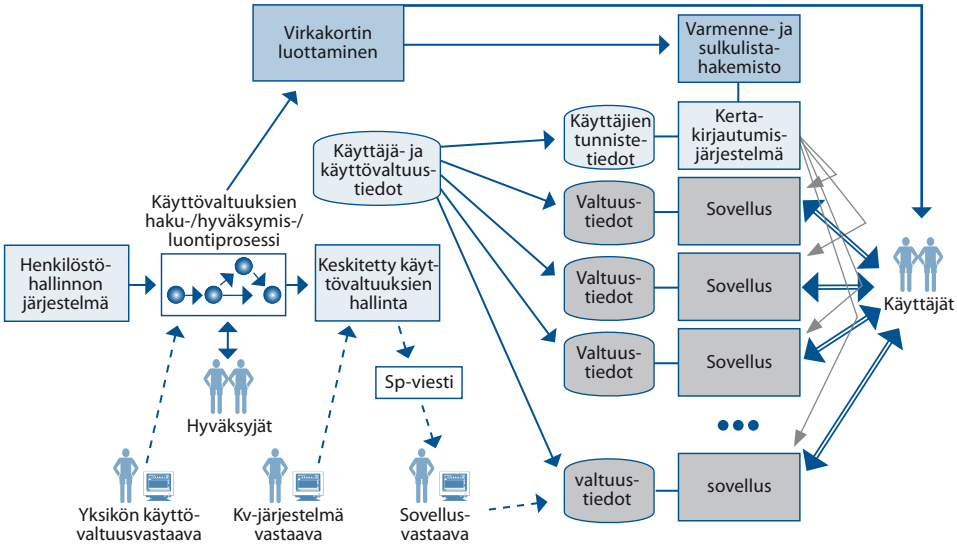
röity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan, samoin kuin ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä. Tiedot on annettava henkilötietoja kerättäessä ja talletettaessa tai, jos tiedot hankitaan muualta kuin rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kun tietoja ensi kerran luovutetaan". Suostumusta pyydettäessä informoinnin tulee sisältää lisäksi kaikki suostumuksen antajan kannalta olennainen tieto.

Henkilötietolainsäädännön taustalla vaikuttavana yleisenä lähtökohtana on, että henkilötietolain säännökset pyrkivät ennaltaehkäisemään mahdollisia ongelmatilanteita ohjaamalla kaikkia henkilötietoja käsitteleviä tahoja, julkishallintoa, yrityksiä, yhteisöjä ja muita rekisterinpitäjiä, hyvään tietojenkäsittely- ja tiedonhallintatapaan. Suostumuksen pyytämisen merkitys on tässä asiassa korostuneen tärkeää. Itsemääräämisoikeuden ja kielto-oikeuden käyttämisen mahdollistaminen valokuvia julkisesti käsiteltäessä ilmentää aina henkilötietolain 5 §:n asettaman hyvän tietojenkäsittelytavan noudattamista, jolloin tehokkaasti voidaan välttyä mahdollisilta jälkikäteen ilmeneviltä ongelmilta.

Yleisenä henkilötietolakiin sisällytettynä sääntönä on nostettava esille vielä **tarkastusoikeus**. Silloin kun valokuva on talletettu osaksi henkilörekisteriä, on rekisteröidyllä kuvaan sekä muihin itseään koskeviin tietoihin tarkastusoikeus henkilötietolain 26 §:n nojalla.

4.11.4 Provisiointi

Provisioinnilla välitetään käyttäjä- ja valtuustiedot järjestelmien välityksellä suoraan kohdejärjestelmään käyttäjä- ja käyttövaltuusrekisteristä.



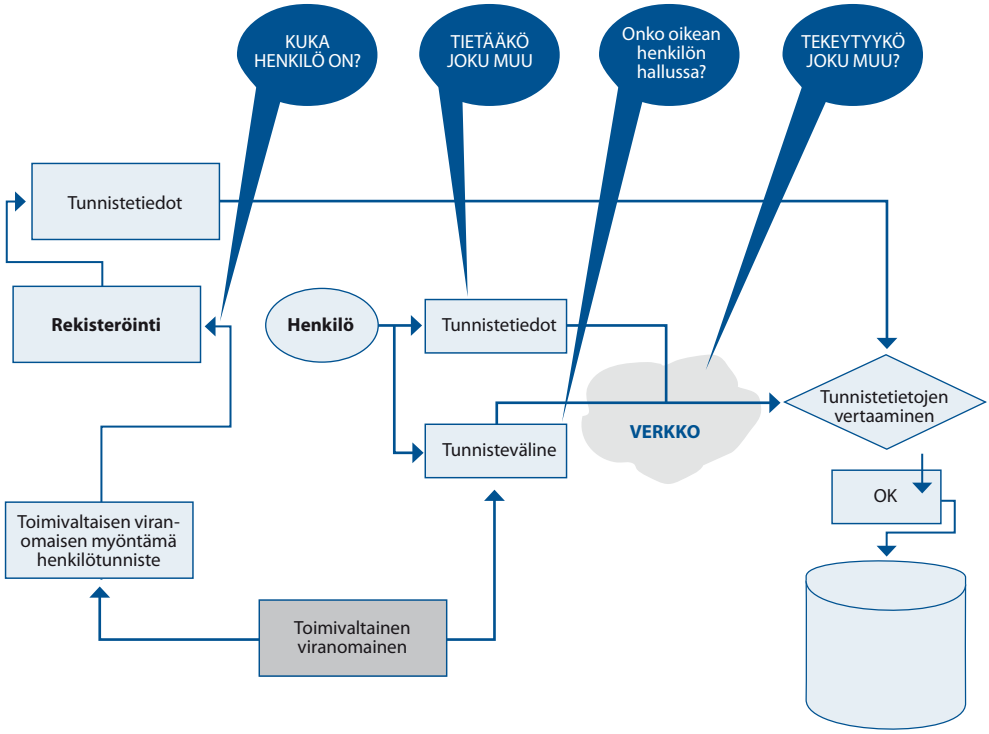
KUVA 3. Esimerkki viraston valtuuksien hallinnasta tietojärjestelmäympäristössä

4.12 Pääsyn hallinta ja tunnistaminen

4.12.1 Luottamusketju, aitouden todentaminen

Aitous (*authenticity*) on ominaisuus, jota tarvitaan käytettäessä apuvälineitä henkilöllisyyden todentamiseen. Todentamista ei tule käsittää ainoastaan henkilöllisyyden todentamiseksi. Aitouden todentaminen tulee kyseeseen aina, kun henkilöä ei ”tunneta” ja hänen tunnistamisessaan käytetään tunnistevälineitä tai tunnistevertailutietoja.

Todentamisen vahvuus riippuu apuvälineitä käytettäessä koko luottamusketjun luotettavuudesta. Jokaiseen sidokseen on pystyttävä luottamaan ja jokaisen apuvälineen aitoudesta on voita varmistua.



PIIRROS 3. Tunnistamisen luottamusketju ja siinä tarvittava aitouden todentaminen.

4.12.2 Tunnistaminen

Kulunvalvonta on henkilön tunnistamista. Henkilöllisyys on voitava todeta ja hänen pääsyvaltuutensa on voitava varmistaa todeksi.

Tunnistamisessa henkilö tunnistetaan siten, että hänet

1. tunnetaan henkilökohtaisesti
2. tunnistetaan biometrisesti (fyysinen vertailutieto; kuva tai muu ominaisuus)
3. tunnistetaan tiedosta (tiedollinen vertailutieto; salasana)
4. tunnistetaan jostakin esineestä, joka on hänen hallussaan (aitous ja hallussapitoketjun eheys; avain tai muu tunnisteväline).

Tunnistamisessa tarvittavat vertailutiedot hankitaan rekisteröidyttäessä. Tunnistamistilanteessa saatua vertailutietoa verrataan rekisteröidyttäessä annettuun henkilöllisyystietoon.

4.12.3 Tunnisteet

Tunnisteita ovat

- tunnistevälineet
- tunnistetiedot
- biotunnisteet.

4.12.4 Tunnistetieto

Tunnistevertailutieto on henkilön hallussa oleva tieto, jota vertaamalla tunnistajan hallussa oleviin vertailutietoihin voidaan varmistua henkilön aitoudesta.

Yleisimmin käytetävä tunnistevertailutieto on henkilökohtainen salasana (Personal Identification Code, PIN). Salasanan heikkous on sen tietoluonne; salasana voidaan siepata tai se voidaan kopioida. Henkilö ei voi olla varma siitä, että hänen henkilökohtainen salasanansa ei ole joutunut muiden tietoon, jolloin tiedon rinnakkainen kaksoiskäyttö on mahdollista.

4.12.5 Biotunnisteet

Biotunniste sisältää henkilön yksilöiviä ominaisuuksia. Yleisin on henkilön kasvovalokuva. Biotunnisteen vahvuus on siinä, että se liittää henkilön vahvasti biotunnisteen sisältävään valtuustietoon.

Biotunnisteiden ongelmana on kopioitavuus ja varsin suuret tunnistusvirheet; henkilöä ei joko voida tunnistaa tai tunnistetaan liian vähäisellä varmuudella.

4.12.6 Tunnistevälineet

Tunnistevälineitä ovat henkilötunnistekortit ja kulkukortit. Henkilötunnistekortin keskeiset turvaominaisuudet ovat aitoustodisteet ja vertailutiedot,

joista yleisemmin käytetään kasvokuvaa. Vertailutiedolla tunnisteväline liitetään henkilöön ja aitoustodisteella varmistutaan tunnistevälineen myöntäjästä ja siten pääsyvaltuutuksesta.

Tunnistevälineisiin voidaan liittää lisäksi tietoja pääsyoikeusprofiilista, esimerkiksi tilaryhmistä, joihin henkilöllä on oikeus päästä.

Tunnistevälineen heikkous on sen joutuminen väärän henkilön haltuun.

> **Tunnistevälineen** turvallisuusominaisuudet ovat aitoustodiste ja vertailutieto sekä mahdolliset muut tiedot, kuten henkilön yleisvaltuutuksen ilmaiseva henkilöryhmä.

4.12.7 Turvallisen pääsynvalvonnan toteuttaminen esimerkin valossa

Matkustusasiakirjojen aitouden, henkilön tunnistamisen ja hänellä olevien valtuuksien, mm. kansalaisuuden todentamiseksi on otettu käyttöön rfid-tunnisteen ja biometrisiä tunnisteita sisältävä sirupassi. Passi on fyysinen dokumentti, johon on tallennettu digitaalisessa muodossa tietoja passin haltijasta. Passin lukutapahtuma edellyttää kolmea erillistä vaihetta, joilla varmistetaan käsittelytapahtuman turvallisuus.

Kuvatussa käsittelytapahtumassa toteutuvat kaikki turvallisen pääsynvalvonnan vaatimukset: tunnisteen aitouden toteaminen, henkilön tunnistaminen ja valtuuksien toteaminen. Passin myöntämismenettelyn eli valtuutuksen turvallisuuteen sirupassi ei tuo lisäarvoa. Valtuutuksen turvallisuus toteutetaan viranomaisten välisen luottamusmekanismin avulla.

Peruspääsynvalvontavaiheessa optisella kuvalukijalla luetaan passin tietosivulla olevaa koneluettavaa aluetta. Tässä vaiheessa passin on oltava aukaistuna.

Fyysisen dokumentin aitouden varmistamiseksi lukijalaite luo istuntoavaimen edellä saatujen tietojen ja generoidun satunnaisluvun avulla. Istuntoavainta käytetään passin myöntäneen viranomaisen antaman digitaalisen varmenteen tarkistamiseen (passiivinen todentaminen) ja salatun yhteyden muodostamiseen. Varmenteen aitouden tarkistamisen jälkeen passin sisältämät henkilötiedot luetaan koneellisesti passista salattua tiedonsiirtoyhteyttä käyttäen. Tiedot tarkistetaan julkisen avaimen menetelmää käyttäen (PKI) siten, että lukija lähettää haasteen, johon passi vastaa lähettämällä allekirjoitetun ja salatun tiedoston (dokument security object). Tunnistetietoja vertaamalla selviää, ovatko passin tietosivu ja sirun sisältämät tiedot yhteneväiset. Aktiivinen todentaminen estää passin väärentämisen kopioimalla tietoja.

Tarkastusvaiheessa lukija ja passi muodostavat vahvan istuntoavaimen, jolla salataan kasvokuva ja siirretään se salatun yhteyden kautta lukijalaitteelle. Salaus puretaan lukijalaitteessa ja sitä verrataan passin haltijasta otet-

tuun kuvaan. Maahantulotarkastusta hoitava henkilö voi lisäksi itse verrata kuvaa passin tietosivuun ja passin haltijaan. Kasvokuvan tarkistuksen jälkeen lukija tekee haaste-vaste -menetelmällä tarkistuksen ja vasta sen onnistuttua passi luovuttaa biometrisiä tietoja lukijalaitteelle.

4.12.8 Henkilöstön fyysisen pääsyn hallinta

Yleisimmin käytetty ja usein myös tehokkain tapa rajoittaa pääsyä tietoihin on valvoa henkilöiden fyysistä pääsyä tiloihin, joissa käsitellään tietoa tai tietojärjestelmiä.

Pääsyn hallinnan toteuttaminen EU:n määräyksen mukaiseen standardoituun malliin on esitetty liitteessä 5.

Liite 1. Esimerkki henkilöstöriskikartoituksen laatimisesta

Toimenpide	Arvioitava kohde, esimerkiksi avainhenkilön käytettävyys
1	2.1 Arviointi, jolla voidaan tunnistaa organisaation avain henkilöt, on tehty
2	2.2 Riskiarviointi, jolla voidaan tunnistaa avainhenkilöön liittyvät uhat, on tehty
3	2.3 Avainhenkilöllä on varahenkilö(t)
4	2.4 Henkilöstöhallinnon prosessit ovat olemassa ja niitä noudatetaan
5	2.5 Henkilöstöstrategia ja kehittämissuunnitelmat ovat olemassa

Arvioitavan kohteen tila	Jos toiminta on määritelty ja sen mukaan toimitaan, niin se on		
	matalalla tasolla (1)	keskitasolla (2)	hyvin hoidettu (3)
2.1 Avainhenkilöiden tunnistus	toimintamallit olemassa mutta niitä ei käytetä	avainhenkilöt tunnistettu	tunnistus osataan, se on kattava ja sitä noudatetaan
2.2 Avainhenkilöön liittyvät uhat	toimintamallit olemassa mutta niitä ei käytetä	uhat osin tunnistettuja	uhkien tunnistus on kattava ja sitä noudatetaan
2.3 Avainhenkilöllä on varahenkilö(t)	asia tiedetään mutta sitä ei pidetä tärkeänä	tunnistetaan, että varahenkilö tarvitaan	asia tiedetään ja toimitaan suojattavan edun mukaisesti
2.4 Henkilöstöhallinnon prosessit ovat olemassa	toimintamallit olemassa mutta niitä ei käytetä	prosessit ovat osittain olemassa	prosessit kuvattu ja niitä noudatetaan
2.5. Henkilöstöstrategia ja kehittämissuunnitelmat ovat olemassa	ei tunnisteta suunnitelmia	tiedetään miten henkilöstöä johdetaan	toimitaan suunnitelmien mukaisesti ja toiminta on osa strategiaa

Henkilöstöturvallisuuden tasoa voidaan ilmaista prosenttiluvulla, joka saadaan, kun kullekin taulukon solulle annetaan pisteet 1–3. Pisteet lasketaan yhteen ja verrataan tulosta maksimipisteisiin, jotka ovat kyseissä taulukossa 15.

Jos esimerkiksi tulos on 10 pistettä, niin henkilöstöturvallisuuden tasoksi saadaan 67 prosenttia avainhenkilön käytettävyyden osa-alueella.

Riskiselvityksen perusteella on päätettävä, mitä riskejä hyväksytään ja mitä toimenpiteitä on toteutettava riskien hallitsemiseksi.

Liite 2. Henkilöstöturvallisuuteen liittyvä keskeinen lainsäädäntö

Perustan henkilötietojen käsittelylle luo **perustuslain 10 §** (731/1999) 10 §, jossa säädetään yksityiselämän suojasta. Pykälän 1 momentin ensimmäisen lauseen mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Momentin toisen lauseen mukaan henkilötietojen suojasta säädetään tarkemmin lailla. 1 momentti merkitsee yksilölle oikeutta siihen, että valtio turvaa yksilön suojan lailla ja että valtio huolehtii organisatorisista ja muista toimenpiteistä, jotka ovat tarpeen yksilönsuojan toteuttamiseksi, kuten valvontakoneistosta. Tämä perusoikeuden ulottuvuus merkitsee oikeutta lakisääteiseen yksilönsuojaan tietojenkäsittelyssä: jokaisella on siten oikeus saada henkilötiedoilleen riittävä suoja (HE 96/1998).

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun tai muun luottamuksellisen viestin salaisuus on loukkaamaton. Jokaisella on oikeus päättää omista asioistaan ja tehdä itseään koskevat henkilökohtaiseen elämään liittyvät valinnat vapaasti ilman ulkopuolisten puuttumista. Tietojenkäsittelyssä yksilöllä tulisi olla mahdollisuus vaikuttaa omien tietojensa käyttöön. Yksilöä koskevien tietojen laajamittainen tallettaminen yksilön personallisuutta kuvaavalla tavalla voi rajoittaa henkilökohtaista vapautta.

Perustuslain 10 §:n 3 momentin ensimmäisen lauseen mukaan lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Momentin toisen lauseen mukaan lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Lailla säädettävältä perusoikeusrajoitukselta vaaditaan täsmällisyyttä ja tarkkarajaisuutta. Rajoituksen olennaisen sisällön tulee ilmetä suoraan laista. Siitä tulee käydä selville esimerkiksi rajoituksen laajuus ja sen täsmälliset edellytykset. Perusoikeuksien rajoittaminen on sallittua vain hyväksyttävillä perusteilla (HE 309/1993).

Henkilöstöturvallisuustyössä on hyvä tuntea ainakin **rikoslain 38 luku** (578/1995), jossa säädetään tieto- ja viestintärikoksista.

Henkilötietolain (523/1999) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Lailla pyritään turvaamaan, ettei yksityiselämän suojaa tai muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta henkilötietoja kerättäessä, talletettaessa, käytettäessä, siirrettäessä, luovutettaessa tai muutoin käsiteltäessä.

Viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista rajoituksista sekä viranomaisten velvollisuuksista edistää lain tarkoituksen toteutumista.

Kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004) todetaan, että henkilön luotettavuuden arvioinnin perusteena oleva turvallisuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) säädetään. Turvallisuusselvitys voidaan tehdä myös suppeana, jos se on tarpeen kansainvälisen tietoturvavelvoitteen toteuttamiseksi.

Yksityisyyden suojasta työelämässä annetussa laissa (759/2004) säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostin hakemisesta ja avaamisesta.

Turvallisuusselvityksistä annetussa laissa (177/2002) säädetään turvallisuusselvityksestä, joka voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä.

Rikoslain 24:3 §:ssä, jossa säädetään julkisrauhan rikkomisesta, kielletään tunkeutumasta julkisiin rakennuksiin ja rajoitetaan niiden kuvaamista.

Sähköisen viestinnän tietosuojalain (516/2004) tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.

Laki sähköisistä allekirjoituksista (14/2003) edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa.

MUUTA HENKILÖSTÖTURVALLISUUTEEN LIITTYVÄÄ LAINSÄÄDÄNTÖÄ

Toiminnan ohjausta koskevat:

Valtioneuvoston ohjesääntö (262/2003)

- valtion tietohallinnon, tietojenkäsittelyn ja tietoturvallisuuden yleiset perusteet, hallinnon sähköinen asiointi ja valtioneuvoston yhteinen tietohallinto

TIETOAINEISTOA KOSKEVAT:

Perustuslain perusoikeussäännökset

- yksityiselämän suoja (10 §)
- sananvapaus ja julkisuus (12 §)

Laki viranomaisen toiminnan julkisuudesta (636/2000)
- julkisuusperiaate (1 §)
- velvoite hyvään tiedonhallintatapaan (3 §)
- tiedonsaanti salassa pidettävästä asiakirjasta (10 §)
- viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (17 §)
- hyvä tiedonhallintatapa (18 §)
- salassapitovelvoitteet (22 §-25 §)
- asiakirjasalaisuus (22 §)
- vaitiolovelvollisuus ja hyväksikäyttökielto (23 §)
- salassa pidettävät viranomaisen asiakirjat (24 §)
- salassapidosta poikkeaminen ja sen lakkaaminen (26 §–32 §)

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- selvitykset hyvän tiedonhallintatavan toteuttamiseksi (1 §)
- erityissuojattavan tietoaineiston luokitus (2 §)
- erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvatoimenpiteet (3 §)
- ohjeet, valvonta ja seuranta (4 §)
- selosteet tietojärjestelmistä (8 §)

Arkistolaki (831/1994)
- käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
- turvaaminen tuhoutumiselta, vahingoittamiselta ja asiattomalta käytöltä (12 §)

Laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
- velvollisuus hoitaa sisäinen valvonta (24 §)

Valtioneuvoston asetus valtion talousarviosta annetun asetuksen muuttamisesta (263/2000 ja 254/2004)
- sisäinen tarkastus ja valvonta (69 §, 69a §, 70 §)

Asetus valtion talousarviosta (1243/1992) sekä sen muutokset (263/2000 ja 254/2004)
- koneellisin menetelmin pidetty kirjanpito (47 §- 52 §)
- koneellisen kirjanpidon menetelmäkuvaus (47 §)
- velvoite valvoa (69 §)

Henkilötietolaki (523/1999) ja laki sen muuttamisesta (986/2000)
- tarkoituksena toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia (1 §)
- tietoturvallisuus ja tietojen säilytys (32-35 §)

Henkilökorttilaki (829/1999)
- väestötietolain muutos (527/1999) ja (202/1994)
- väestörekisterikeskuksen varmenneviranomaistoiminta

Tekijänoikeuslaki
- ohjelmistojen tekijänoikeudet

TIETOAINEISTOA JA TIETOTEKNIIKKAA KOSKEVAT:
Laki sähköisen viestinnän tietosuojasta (516/2004)
- televiestinnän turvallisuus (4 §)
- teleyrityksen tietoturvavelvoitteet (6 §)
- teleoperaattorien vaitiolovelvollisuus (7 §)
- rajoitukset suoramarkkinoinnille (21 §)

Viestintämarkkinalaki (393/2003)
- suojauksen purkujärjestelmien kielto (25 §)
- laki rikoslain muuttamisesta luvaton käyttö (28. luku 7 § – 9 §)
- vahingonteko (35. luku 1 § - 3 §)

Lait rikoslain muuttamisesta
- viestintäsalaisuuden loukkaus (38. luku 3 §)
- tietomurto (38. luku 8 §)
- virkasalaisuuden rikkominen (40. luku 5a §)
- vaaran aiheuttaminen tietojenkäsittelylle (34. luku 9a §)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- varmentamistoiminta (4 § -12§)
- sähköisen asiointipalvelujen järjestäminen, tietoturvallisuus (18 §)
- asian vireillepano sähköisellä asiakirjalla (22 §)
- päätösasiakirjan sähköinen allekirjoittaminen (28 §)

POIKKEUSOLOJEN VALMIUTTA KOSKEVAT:
Valmiuslaki (1080/1991)

Laki huoltovarmuuden turvaamisesta (1390/1992)
- valtioneuvoston päätös huoltovarmuuden tavoitteista (350/2002)

Laki Puolustustaloudellisesta suunnittelukunnasta kumottu, ja lisätty lakiin huoltovarmuuden turvaamisesta (1390/1992)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta VM 11.11.1999/0024:00/02/99/1998

Pakkokeinolaki (450/1987) 5a-luku

Henkilötietolaki (523/1999) ja laki sen muuttamisesta (986/2000)

- 5 § Huolellisuusvelvoite
- 6 § Henkilötietojen käsittelyn suunnittelu
- 7 § Käyttötarkoitussidonnaisuus
  (Viite: VAHTI 5/2004: Liite 1 tietoturvallisuus ja tietojen säilytys)
- 8 § Käsittelyn yleiset edellytykset
- 9 § Tietojen laatua koskevat periaatteet
- 10 § Rekisteriseloste
- 10. Luku 48 § Rangaistussäännökset

Väestötietolaki (507/1993, muutokset 202/1994 ja 527/1999)

Laki väestötietolain muuttamisesta (527/1999) ja (202/1994)
(Viite: VAHTI 5/2004: Liite 1)

Sähköisen viestinnän tietosuojalaki (516/2004)

Laki yksityisyyden suojasta työelämässä (759/2004) aiemmin (477/2001)

Laki viranomaisen toiminnan julkisuudesta (621/1999), muutos (636/2000)

- 1 § julkisuusperiaate
- 3 § velvoite hyvään tiedonhallintatapaan
- 10 § tiedonsaanti salassa pidettävästä asiakirjasta
- 17 § viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa
- 5 luku: viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa
- 18 § Hyvä tiedonhallintatapa
- 22 §-25 § salassapitovelvoitteet
- 22 § asiakirjasalaisuus
- 23 § vaitiolovelvollisuus ja hyväksikäyttökielto
- 24 § salassa pidettävät viranomaisen asiakirjat
- 6. luku salassapitovelvoitteet
- 7. luku salassapidosta poikkeaminen ja sen lakkaaminen
  salassapidosta poikkeaminen ja sen lakkaaminen (26 §–32 §)

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

- 1 § selvitykset hyvän tiedonhallintatavan toteuttamiseksi
- 2 § erityissuojattavan tietoaineiston luokitus
- 3 § erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvatoimenpiteet
- 4 § ohjeet, valvonta ja seuranta
- 8 § selosteet tietojärjestelmistä

Laki yhteistoiminnasta valtion virastoissa ja laitoksissa (651/1988)

Laki kunnallisesta viranhaltijasta (304/2003)

Hallintolaki (434/2003)

Valtion virkamieslaki (750/1994)
- 17 § (626/1999)
- 7 luku virkasuhteen päättäminen, purkuperusteet, kirjallinen varoitus
- 8 § selosteet tietojärjestelmistä

Asetus valtionhallinnon tietohallinnosta (155/1988, muutettu 1401/1992) kumottu säädöksellä (756/2003) ja korvattu lailla valtioneuvostosta (175/2003)
- 1 § tietojärjestelmät taloudellisia, turvattuja, toiminnallisesti yhteensopivia sekä tietosuojan vaatimukset täyttäviä
- 2 § valtionhallinnon tietojenkäsittelyn ja tietohallinnon ohjaus ja yhteensovittaminen
- 3 § velvoite pyytää merkittävästä tahi useaa virastoa tai laitosta koskevasta tietotekniikan soveltamiseen liittyvästä hankkeesta valtiovarainministeriön lausunto
- 3 § tietojenkäsittelyä ja tietohallintoa koskeva kehittämissuunnitelma

Hallintomenettelylaki (598/1982)

Valtioneuvoston ohjesääntö (1522/1995 , muutos 730/2000) kumottu säädöksellä Valtioneuvoston ohjesääntö (262/2003)
- 17§ Valtiovarainministeriön toimiala

Asetus valtion talousarviosta (1243/1992) sekä sen muutokset (263/2000 ja 254/2004)
- 26 § taloushallinnon järjestelmien tietoturvamääräykset talussäännössä
- 47§ koneellisin menetelmin pidetty kirjanpito ja sen menetelmäkuvaus
- 69 §, 69a § riskeihin nähden asianmukainen sisäinen valvonta
- 69b § taloushallinnon järjestelmien tietoturvamääräykset talussäännössä

Laki valtion talousarviosta (423/1988)
- 24 b § Sisäinen valvonta (217/2000)

Laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
- 24 § velvollisuus hoitaa sisäinen valvonta

Laki valtion talousarviolain muuttamisesta (1216/2003)

Arkistolaki (831/1994)
- 7 § käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen
- 4 luku, Asiakirjojen laatiminen, säilyttäminen ja käyttö

Laki sähköisestä asioinnista hallinnossa (1318/1999) korvattu lailla sähköisestä asioinnista viranomaistoiminnassa (13/2003)

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) ja asetus (723/1999) kumottu lailla sähköisen viestinnän tietosuojasta (516/2004)

Laki sähköisistä allekirjoituksista (14/2003)

Valmiuslaki (1080/1991)

Valtioneuvoston päätös huoltovarmuuden tavoitteista (350/2002)

Laki huoltovarmuuden turvaamisesta (1390/1992)

Työsopimuslaki (320/1970) kumottu lailla Työsopimuslaki (55/2001)

Vahingonkorvauslaki (41/1974)

Laki julkisista hankinnoista (1505/1992, uudistettavana)

Asetus valtion hankinnoista (1416/1992)

Oikeustoimilaki (228/1929)

Laki valtion talousarviosta (423/1988)

Asetus valtion talousarviosta (1243/1992)

Kauppalaki (355/1987)

Laki turvallisuusselvityksistä (177/2002)

Laki kansainvälisistä tietoturvavelvoitteista (588/2004)

Henkilökorttilaki (829/1999)

Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta (ns. Lex Makropilotti; 801/2000, kumottu asetuksella)

Laki sähköisestä asioinnissa yleisissä oikeusistuimissa (594/1993 ja 199/1998) kumottu (13/2003)

Laki työvoimahallinnon tietojärjestelmistä (1254/1993) kumottu lailla työhallinnon asiakaspalvelun tietojärjestelmästä (1058/2002)

Laki Puolustustaloudellisesta suunnittelukunnasta (238/1960, muutokset 42/1981, 1241/1987 , 444/1997 ja 623/1999) kumottu Asetuksella huoltovarmuuskeskuksista (1391/1992) ja sisältyy lakiin huoltovarmuuden turvaamisesta (1390/1992)

Tekijänoikeuslaki (404/1961, muutokset 344/2000) , tekijänoikeus suojaa tietokoneohjelmaa (1 §)

Tietokoneohjelmia ja tietokantoja koskevia erityissäännöksiä (250/1998)
- 25 j,k § (446/1995)
- 26 § Sopimuslisenssi (821/2005)

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)

Kuntalaki (365/1995)

Laki Viestintähallinnosta (625/2001), määrittelee Viestintäviraston aseman

Telemarkkinalaki (396/1997, muutos 566/1999) kumottu Viestintämarkkinalailla (393/2003)

Potilaan asemaa sosiaali- ja terveydenhuollossa koskevat säädökset (785/1992 muutoksineen; 812/2000)

Suomen ja Länsi-Euroopan unionin välisen turvallisuussopimuksen eräiden määräysten hyväksymisestä ja sen soveltamisesta (282/1998)

Rikoslaki (39/1889)

- 28.luku 7 § Luvaton käyttö (769/1990)
- 28.luku 8 § Törkeä luvaton käyttö (769/1990)
- 28.luku 9 § Lievä luvaton käyttö (769/1990)
- 34.luku 1 § Tuhotyö (578/1995)
- 34.luku 9a § Vaaran aiheuttaminen tietojenkäsittelylle (951/1999)
- 35.luku 1 § Vahingonteko(769/1990)
- 35.luku 2 § Törkeä vahingonteko(769/1990)
- 35.luku 3 § Lievä vahingonteko(769/1990)
- 38.luku 1 § Salassapitorikos (578/1995)
- 38.luku 2 § Salassapitorikkomus (578/1995)
- 38.luku 3 § Viestintäsalaisuuden loukkaus (2000/531)
- 38.luku 4 § Törkeä viestintäsalaisuuden loukkaus (578/1995)
- 38.luku 5 § Tietoliikenteen häirintä (578/1995)
- 38.luku 6 § Törkeä tietoliikenteen häirintä (578/1995)
- 38.luku 7 § Lievä tietoliikenteen häirintä (578/1995)
- 38.luku 8 § Tietomurto (578/1995)
- 38.luku 8a § Suojauksen purkujärjestelmärikos (1118/2001)
- 38.luku 9 § 1. kohta Henkilörekisteririkos (525/1999)
- 40. luku 5 § Virkasalaisuuden rikkominen (604/2002)

Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)

Liite 3. Esimerkki suojattavien resurssien luokituksesta, henkilöstöturvallisuusluokista ja niiden välisistä turvallisuussäännöistä

TIETOJÄRJESTELMIEN LUOKITUS

Tietojärjestelmiä tulee käsitellä **ensisijaisesti niiden sisältämien tietojen kannalta**. Valtiovarainministeriön VAHTI-ohjeessa 5/2004 on esitetty keskeisten järjestelmien luokitukseksi

- käytettävyys, eheys ja luottamuksellisuus (KEL) tärkeää (käytettävyys- ja salassapitotarve korkea), esimerkiksi reaaliaikaiset johtamisjärjestelmät
- käytettävyys ja eheys (KE) tärkeää (käytettävyystarve korkea), esimerkiksi sääpalvelut ja julkiset rekisterit
- luottamuksellisuus ja eheys (LE) tärkeää (salassapitotarve korkea), esimerkiksi rahoitusjärjestelmät ja varmenteiden tuotantojärjestelmät.

Näiden tekijöiden perusteella voidaan tietojärjestelmät luokitella salassapidon ja käytettävyyden perusteella viiteen luokkaan:

- julkisia ja käytettävyydeltään ei-kriittisiä tietoja sisältävät järjestelmät (luokka 5)
- käytettävyydeltään ja eheydeltään merkittäviä tietoja sisältävät järjestelmät (luokka 4)
- luottamuksellisia tai käytettävyydeltään erittäin merkittäviä tietoja sisältävät järjestelmät (luokka 3)
- salaisia käytettävyydeltään merkittäviä tietoja sisältävät järjestelmät (luokka 2)
- salaisia ja käytettävyydeltään erittäin merkittäviä tietoja sisältävät järjestelmät (luokka 1).

TILATURVALLISUUSLUOKAT

Turvattava tilat, tilaryhmät ja alueet jaetaan viiteen luokkaan

- yleiset tilat, tilaryhmät ja alueet (luokka 5, Y), esimerkiksi neuvotteluhuoneet
- valvotut työtilat, tilaryhmät ja alueet (luokka 4, V), esimerkiksi työhuoneet
- rajoitustilat ja tilaryhmät (luokka 3, R), esimerkiksi turvallisuusvalvomot
- eristystilat ja tilaryhmät(luokka 2, E), esimerkiksi poikkeusolojen johtopaikat
- erikoistilat ja tilaryhmät (luokka 1), esimerkiksi luokan 1 palvelintilat.

OMAISUUS JA MATERIAALILUOKAT

Turvattava omaisuus ja materiaali jaetaan turvallisuusominaisuuksien perusteella viiteen luokkaan

- yleismateriaali (ei erityisiä turvallisuusvaatimuksia), esimerkiksi toimistotavarat
- työvälineet (luokka D), esimerkiksi pöytäpuhelimet
- erittäin anastusherkkä omaisuus (luokka C), esimerkiksi käteinen raha
- avainmateriaali ja -järjestelmät (luokka B), esimerkiksi salauslaitteet
- erikoismateriaali ja -laitteet (luokka A), esimerkiksi laite, jossa II salassapitoluokan tietoja sisältävän tietojärjestelmän CA-salausavain.

HENKILÖSTÖTURVALLISUUSLUOKAT

Henkilöstöriskejä hallitaan rikosriskien osalta luokittelemalla henkilöstö neljään henkilöstöturvallisuusluokkaan (I – IV)

- I luokka: henkilöt, joiden toiminta voi vakavasti vahingoittaa valtion turvallisuutta tai suhteita (JulkL § 24.1 kohdat 1,2,5 ja 8-11), julkista taloutta tai yksityistä taloudellista etua, tai erittäin merkittävästi muuta tietoturvallisuutta. Luokkaan kuuluu ainoastaan hyvin rajoitettu joukko ministeriöiden ja virastojen henkilökuntaa.
- II luokka: henkilöt, joiden toiminta voi vaarantaa tai loukata merkittävästi valtion turvallisuutta tai suhteita (JulkL § 24.1 kohdat 1,2,5 ja 8-11), julkista taloutta tai yksityistä taloudellista etua, tai merkittävästi muuta tietoturvallisuutta. Luokkaan kuuluu rajoitettu joukko ministeriöiden ja virastojen henkilökuntaa tai palveluja tuottavan turvaluokitellun yrityksen henkilöstöä.
- III luokka: henkilöt, joiden toiminta voi vaarantaa ministeriön tai viraston toimintaedellytyksiä. Luokkaan kuuluu pääosa ministeriön tai viraston henkilökunnasta ja pääosa turvaluokitellun yrityksen henkilöstöstä.
- IV luokka: henkilöt, joiden toiminta voi haitata ministeriön tai viraston toimintaa, esimerkiksi pysyvän kulkuoikeuden saaneet huoltohenkilöt tai rekisteröidyt pysyväisvierailijat.

SÄÄNTÖMATRIISIN KÄYTTÖ

Luokitusjärjestelmä mahdollistaa henkilöstön ja resurssien välisten turvallisuussääntöjen käytön.

Henkilöstöturvallisuusluokka määrää periaatteen, minkä turvaluokan tilaan, tietoon hänellä on oikeus päästä tai perehtyä, sekä minkä turvaluokan laitetta, järjestelmää tai omaisuutta hänellä on oikeus käsitellä. Lisäksi on huomioitava kokonaisjärjestelyjen käytettävyyden osalta henkilön rooli kriittisten järjestelmien avainhenkilönä.

Viraston henkilökuntaan turvaluokkaan IV kuuluvalla on oikeus päästä työtehtävissään viraston valvottuihin tiloihin ja saatettuna rajoitustiloihin ja isännöidä vieraita valvotuissa tiloissa. Hänellä on myös oikeus saada tie-

toonsa ja käsitellä työtehtäviinsä liittyen rajoitetun käytön tietoja (4. luokka) sekä tapauskohtaisesti asiaryhmittäin rajoitetusti luottamuksellisia tietoja (3. luokka). Työntekijällä on oikeus käsitellä työssään tarvittavia enintään D-luokkaan kuuluvia välineitä ja omaisuutta sekä julkisia tietoja ja käytettävyydeltään ei-kriittisiä tietoja sisältäviä järjestelmiä (luokka 5).

Viraston henkilökuntaan turvaluokkaan III kuuluvalla on oikeus päästä työtehtävissään viraston valvottuihin tiloihin ja rajoitustiloihin ja isännöidä vieraita valvotuissa tiloissa. Hänellä on myös oikeus saada tietoonsa ja käsitellä työtehtäviinsä liittyen luottamuksellisia tietoja (3. luokka) sekä tapauskohtaisesti asiaryhmittäin rajoitetusti ja vähäisessä määrin salaisia tietoja (2. luokka). Työntekijällä on oikeus käsitellä työssään tarvittavia enintään C-luokkaan kuuluvia välineitä ja omaisuutta sekä käytettävyydeltään ja eheydeltään merkittäviä (luokka 4), tai luottamuksellisia tai käytettävyydeltään erittäin merkittäviä (luokka 3) tietoja sisältävät järjestelmiä.

Viraston henkilökuntaan turvaluokkaan II kuuluvalla on oikeus päästä työtehtävissään viraston rajoitustiloihin ja isännöidä vieraita sekä päästä työtehtävissään valvotusti eristys- ja erikoistiloihin. Hänellä on oikeus saada tietoonsa ja käsitellä työtehtäviinsä liittyen salaisia tietoja (2. luokka) sekä rajoitetusti ja tapauskohtaisesti erittäin salaisia tietoja (1. luokka). Työntekijällä on oikeus käsitellä erikseen nimettävissä työtehtävissä B-luokkaan tarvittavia välineitä ja omaisuutta sekä salaisia käytettävyydeltään merkittäviä (luokka 2) ja salaisia ja käytettävyydeltään erittäin merkittäviä tietoja sisältäviä järjestelmiä (luokka 1). Erikoismateriaalin ja -laitteiden (A-luokka) osalta pääsy voidaan hyväksyä tapauskohtaisesti.

Viraston henkilökuntaan turvaluokkaan I kuuluvalla on oikeus saada tietoonsa ja käsitellä työtehtäviinsä liittyen asiaryhmittäin rajaten kaikkia turvaluokiteltuja tietoja. Työntekijällä on oikeus käsitellä erikseen nimettävissä työtehtävissä A-luokkaan tarvittavia välineitä tai omaisuutta.

Turvaluokkaan IV kuuluvalla palveluntoimittajan työntekijällä (S-ryhmä) on oikeus päästä työtehtävissään viraston valvottuihin tiloihin ja isännöidä vieraita valvotuissa tiloissa. Työntekijällä on oikeus käsitellä työssään tilapäisesti tarvittavia enintään D-luokkaan kuuluvia laitteita, omaisuutta ja sopimuksen mukaan 5. luokan järjestelmiä.

Turvaluokkaan III kuuluvalla palveluntoimittajan työntekijällä (S-ryhmä) on oikeus päästä työtehtävissään viraston valvottuihin tiloihin ja saatettuna rajoitustiloihin ja isännöidä vieraita valvotuissa tiloissa. Hänellä on myös oikeus saada tietoonsa ja käsitellä työtehtäviinsä liittyen tapauskohtaisesti asiaryhmittäin rajoitetusti luottamuksellisia (3. luokka) tietoja. Työntekijällä on oikeus käsitellä työssään tilapäisesti tarvittavia enintään C-luokkaan kuuluvia laitteita, omaisuutta ja valvotusti 3. luokan järjestelmiä.

Turvaluokkaan II kuuluvalla palveluntoimittajan työntekijällä (S-ryhmä) on oikeus päästä työtehtävissään viraston valvottuihin ja rajoitustiloihin ja saatettuna palvelusopimuksen mukaisiin E-luokan tiloihin ja valvoa vieraita rajoi-

tustiloissa. Hänellä on myös oikeus saada tietoonsa ja käsitellä työtehtäviinsä liittyen asiaryhmittäin rajoitetusti luottamuksellisia (3. luokka) ja tapauskohtaisesti asiaryhmittäin rajoitetusti salaisia (2. luokka) tietoja. Työntekijällä on oikeus käsitellä työssään sopimuksen mukaisesti tarvittavia enintään B-luokkaan kuuluvia laitteita, omaisuutta sekä valvotusti 2. luokan järjestelmiä.

Muiden virastojen turvaluokkaan III kuuluvalla virkamiehellä (M-ryhmä) on lähtökohtaisesti oikeus päästä välttämättömissä virkatehtävissään viraston valvottuihin tiloihin ja saatettuna rajoitustiloihin. Muut pääsyoikeudet ja menettelyt sovitaan virastojen välisessä yhteistoimintamuistiossa.

Muiden virastojen turvaluokkaan II kuuluvalla virkamiehellä (M-ryhmä) on lähtökohtaisesti oikeus päästä välttämättömissä virkatehtävissään viraston valvottuihin tiloihin ja saatettuna E-luokan tiloihin poikkeustilanteissa. Muut pääsyoikeudet ja menettelyt sovitaan virastojen välisessä yhteistoimintamuistiossa.

Pysyvän kulkuoikeuden saaneella turvaluokkaan IV nimetyllä henkilöllä (P-ryhmä) on oikeus päästä yleisiin tiloihin ja erikseen nimettyihin valvottuihin tiloihin. Henkilöllä on oikeus käsitellä työssään enintään D-luokkaan kuuluvia laitteita, omaisuutta ja sopimuksen mukaan julkisia 5. luokan järjestelmiä, esimerkiksi internetiin kytkettyjä laitteita. Henkilöiden on akkreditoiduttava ja rekisteröidyttävä, jonka yhteydessä heille voidaan valmistaa kuvallinen tunniste.

Käyntioikeuden saaneella vierailijalla (V-ryhmä) on oikeus päästä rajoitetusti yleisiin tiloihin ja saatettuna valvottuihin tiloihin. Vierailijoiden oikeudesta käyttää internetiin kytkettyjä laitteita (5. luokka) on sovittava virastossa. Vieraalla tulee olla isäntä, jonka suosituksesta ja esittämästä tarpeesta hänet valtuutetaan.

Liite 4. Virastojen hakeutuminen turvallisuusselvitysmenettelyyn sekä paikallispoliisin tekemät turvallisuusselvitykset

VIRASTOJEN HAKEUTUMINEN SUOJELUPOLIISIN TURVALLISUUSSELVITYSMENETTELYYN

Suojelupoliisin tehtävänä on torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi. Tässä tarkoituksessa suojelupoliisi tekee **perusmuotoisia ja laajoja turvallisuusselvityksiä**.

Hakeutumismenettelyssä organisaatio selvittää ensin sisäisesti ja myöhemmin toimivaltaiselle viranomaiselle,

- millaista valtakunnallisesti merkittävää suojattavaa etua se hallinnoi
- miten tämä etu on suojattu
- missä tehtävissä sitä voidaan vakavasti vaarantaa.

Suojelupoliisi tekee turvallisuusselvityksiä vain turvallisuusselvitysmenettelyyn hakeutuneiden ja siihen hyväksyttyjen organisaatioiden hakemusten perusteella.

Hakeutuminen turvallisuusselvitysmenettelyyn suositellaan aloitettavaksi alustavalla keskustelulla suojelupoliisin lausuntotoimiston edustajien kanssa. Keskustelussa ohjataan hakeutumista harkitsevaa organisaatiota vaadittavien selvitysten tekemisessä sekä kerrotaan turvallisuusselvitysmenettelystä.

Sisäasiainministeriö on antanut asetuksen turvallisuusselvitysten hakemismenettelystä (710/2002). Asetus ohjaa organisaatioita tekemään menettelyyn pääsemiseksi tähtäävän selvityksen siten, että suojelupoliisi pystyy arvioimaan täyttyvätkö turvallisuusselvityslaista johdettavat hyväksymisen kriteerit. Asetuksen mukaan tehty selvitys toimii samalla pohjana turvallisuusselvitysmenettelyn käytännön hallinnoinnille.

Turvallisuusselvityslain (177/2002) 2§:n ja 4§:n perusteella organisaation juridisella muodolla ei käytännössä juurikaan ole merkitystä arvioitaessa sen kelpoisuutta tulla hyväksytyksi turvallisuusselvitysmenettelyyn. Tärkeintä on,

että organisaatiossa on sellaista luokiteltua tietoa, jota väärinkäyttämällä voidaan vakavasti vaarantaa Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta tai poikkeusoloihin varautumista, Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, julkista taloutta, yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua taikka edellä mainittujen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta. Suojattavan edun vahingoittumisella olisi oltava valtakunnallista vaikutusta. Suojelupoliisi edellyttää, että menettelyyn hakeutuvissa organisaatioissa lain kannalta relevantit luokitellut tiedot on riittävässä määrin suojattu. Mikäli yhteisön tietoturvallisuuden taso on heikko, ei hakemusta voida hyväksyä. Hakijan on annettava selvitys myös niistä tehtävistä, joihin turvallisuusselvitysmenettely esitetään ulotettavaksi. Muista selvitettävistä asioista on säädetty tarkemmin SM:n asetuksessa. Hakeutumismenettelyn voidaan itsessäänkin katsoa parantavan hakijan kokonaisturvallisuuden tasoa.

PAIKALLISPOLIISIN TEKEMÄT TURVALLISUUSSELVITYKSET

Suppean turvallisuusselvityksen tarkoituksena on selvittää voidaanko henkilölle työtehtävässään järjestää pääsy tiettyyn, yhteiskunnan turvallisuuden kannalta merkittävään tilaan. Merkitykselliset tilat on tyhjentävästi lueteltu turvallisuusselvityksistä annetun lain 19 §:ssä. Tällaisia tiloja ovat esimerkiksi ydinvoimalaitokset, lentoasemat ja satamat, yhdyskuntateknistä huoltoa tarjoavat merkittävät laitokset ja viranomaisen tietoverkon kannalta merkittävät toimitilat.

Toimivaltainen viranomainen on suojattavan tilan sijaintipaikkakunnan kihlakunnan poliisilaitos. Puolustusvoimien hallinnoimien tilojen osalta toimivaltainen viranomainen on kuitenkin pääesikunta.

Suppean turvallisuusselvityksen tekemisen yhteydessä on mahdollista tarkastella mm. poliisiasiain tietojärjestelmää ja tuomiolauselmajärjestelmää. Näiden rekistereiden avulla on saatavissa varsin kattava kuva henkilön taustasta kun arvioidaan voidaanko hänelle antaa pääsy yllä mainittuun tilaan.

Muilta osin suppea turvallisuusselvitys ei eroa perusmuotoisesta turvallisuusselvityksestä.

VIRASTOJEN HAKEUTUMINEN PAIKALLISPOLIISIN TURVALLISUUSSELVITYSMENETTELYYN

Suojattavan tilan haltijan on hakeuduttava paikallispoliisin suppeaan turvallisuusselvitysmenettelyyn ennen kuin yksittäisiä selvityksiä voidaan tehdä. Toimivaltainen viranomainen on kohteen sijaintipaikkakunnan poliisilaitos.

Sisäasiainministeriön asetuksessa 710/2002 on säädetty turvallisuusselvitysten hakemismenettelystä.

Asetuksen mukaisesti hakemuksessa on selvitettävä suojattavan kohteen merkitys yleiselle turvallisuudelle, terveydelle, valtion turvallisuudelle taikka julkiselle taloudelle. Lisäksi on selostettava kohteen suojauspolitiikan keskeinen sisältö sekä muutamia turvallisuusselvitysmenettelyn käyttämiseen liittyviä teknisiä seikkoja, kuten esimerkiksi miten turvallisuusselvityksiä tullaan luotettavasti käsittelemään ja säilyttämään.

Turvallisuusselvitysmenettelyyn hakeutuminen kannattaa käytännössä aloittaa yhteydenotolla toimivaltaiseen viranomaiseen.

Liite 5. Pääsyn hallinnan toteuttaminen EU:n määräyksen mukaisesti standardimallissa

Henkilöiden fyysisiin tiloihin *pääsyn valvonta* jaetaan EU:n määräyksen ”Directive on Physical Security relating to the Protection of EU Classified Information” mukaan neljään tyyppiin standardoituun vaihtoehtoon (CEN EN 50 133-1):

Pääsytaso 4:
kulunvalvonta sisäänkäynnissä tai kaikilla turvarajoilla, joissa
- turvasulku, jossa ”one entry - one transaction”-periaate
- hälyttää turvallisuusvalvomoon, jos ovi on auki kauemmin kuin 10/60 sekuntia
- tunnistusluokka 3 (tunniste sekä salasana tai biotunniste)
- kulkuluokka B: aikarajoitusryhmät käytössä, tapahtumat kirjataan

Pääsytaso 3:
kulunvalvonta sisäänkäynnissä tai turvarajoilla, joissa
- kulkuovi, jota voidaan valvoa kameroilla tai muilla valvontavälineillä
- hälyttää, jos ovi on auki kauemmin kuin 10/60 sekuntia
- tunnistusluokka 3 (tunniste sekä salasana tai biotunniste)

Pääsytaso 2:
kulunvalvonta sisäänkäynnissä tai kaikilla turvarajoilla, joissa
- henkilöllinen valvonta, joko vartija tai vastaanottovirkailija
- käytössä kuvalliset henkilökortit tai pääsy kulkukorteilla
- tunnistusluokka 2 (tunniste tai biotunniste)
- kulkuluokka B: aikarajoitusryhmät käytössä, tapahtumat kirjataan

Pääsytaso 1:
kulunvalvonta sisäänkäynnissä tai kaikilla turvarajoilla, joissa
- lukitut ovet, joista pääsy mekaanisilla avaimilla tai erillisillä sähköisillä järjestelmillä
- avaimia luovutetaan vain pääsyyn oikeutetuille.

Kulunvalvonnassa henkilö tunnistetaan, hänen pääsyoikeutensa todennetaan ja mahdollisesti kirjataan kulkutapahtuma.

KULUNVALVONTA ON HENKILÖIDEN TUNNISTAMISTA JA HEIDÄN VALTUUTENSA TODENTAMISTA

Edellä kuvattuja *pääsyn valvontatasoja*, joissa huomioidaan tunnistamisen taso, tunnistevälineiden käyttö ja kulkutapahtuman valvonta, käytetään kiinteistöjen tilojen ja tilaryhmien muodostamilla *kulkualueilla* seuraavasti:

Kiinteistön muodostamalla kuorella:
- virka-aika ja liukuman puitteissa pääsytaso 2, 3 tai 4
- virka-ajan jälkeen pääsytaso 3 tai 4.

Kiinteistön sisällä valvottujen tilojen (luokka 2) kulkualueiden turvarajalla
(keltainen alue):
- pääsytaso 2, ei vaadi henkilöllistä valvontaa
- pääsytaso 1, jos tilan isäntä paikalla (esimerkiksi henkilön pääsy omaan työhuoneeseen).

Rajoitustilojen ja tilaryhmien (luokka 3) turvarajalla
(sininen alue)
- virka-aika ja liukuman puitteissa pääsytaso 2, ei henkilöllistä valvontaa
- virka-ajan jälkeen pääsytaso 3.

Eristystilojen ja tilaryhmien (luokka 2) turvarajalla
(punainen alue)
- pääsytaso 3 tai 4.

Erikoistilat ja tilaryhmät (luokka 1) turvarajalla
(violetti alue)
- pääsytaso 4
- pääsytaso 3, jos tilan isäntä paikalla tilassa.

Liite 6. Valtiovarainministeriön voimassaolevat VAHTI-julkaisut:

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008

VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohje, VAHTI 3/2007

Äypuhelimien tietoturvallisuus – hyvät käytännöt, VAHTI 2/2007

Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Tietoturvakouluttajan opas, VAHTI 11/2006

Henkilöstön tietoturvaohje, VAHTI 10/2006

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

Muutos ja tietoturvallisuus – alueellistamisesta ulkoistamiseen – hallittu prosessi, VAHTI 7/2006

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006

Electronic Mail-handling Instructions for State Government, VAHTI 2/2006

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005

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 2004–2006, VAHTI 1/2004

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003

Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003

Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003

Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003

Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002

Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002

Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, 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

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000

Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000

Julkisuuslain mukaisen tietojärjestelmäselosteen esimerkki

Julkisuuslain mukaisen tietojärjestelmäselosteen rtf-lomakepohja

Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje

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

VAHTI
2/2008
helmikuu 2008

ISSN 1455-2566
ISBN 978-951-804-798-1 (nid.)
ISBN 978-951-804-799-8 (pdf)