Kansallinen turvallisuusauditointikriteeristö

(KATAKRI)

20.11.2009

Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2

Elinkeinoelämän keskusliitto EK
SISÄASIAINMINISTERIÖ
Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

PL 31, 00131 HELSINKI

www.defmin.fi

Taitto: Tiina Takala/puolustusministeriö

ISBN: 978-951-25-2077-0 (nid.)
ISBN: 978-951-25-2078-7 (pdf)

Johdanto

Tämän kansallisen turvallisuusauditointikriteeristön ensimmäisenä päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen, auditoinnin. Viranomainen voi tarpeen mukaan täydentää auditointia turvallisuusarvioinnilla, joissakin tapauksissa myös konsultoinnilla. Nämä toimet eivät kuitenkaan kuulu itse auditoinnin piiriin. Tässä turvallisuusauditointikriteeristön ensimmäisessä versiossa keskitytään ainoastaan ns. security-turvallisuuteen.

Turvallisuusauditointikriteeristön toinen päätavoite on auttaa yrityksiä ja muita yhteisöjä sekä myös viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset lähtötason suositukset, joista toivotaan voitavan poimia kulloinkin käyttökelpoisia turvallisuuskäytänteitä ja edetä tätä kautta tarvittaessa viranomaisvaatimusten tasolle.

Turvallisuusauditointikriteeristö jakautuu neljään pääosioon: hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, eli niitä ei ole rakennettu itsenäisiksi kokonaisuuksikseen. Jokaiselle osiolle on laadittu kolmiportainen vaatimusluokittelu, joka vastaa paraikaa laajamittaisesti käyttöön otettavia turvallisuustasokäsitteitä – perustaso, korotettu taso ja korkea taso. Näitä täydentävät edellä mainitut lähtötason suositukset. Kriteeristö on rakennettu ehdottomien vaatimusten näkökulmasta, eikä se sisällä joissakin kriteeristöissä käytettävää pisteytysmenettelyä. Tällä on pyritty siihen, ettei auditoinnin lopputulokseen jäisi mahdollisesti tunnistamattomia, mutta kriittisiä riskejä. Valittu menettely asettaa erityisiä vaatimuksia turvallisuusauditointeja toteuttavalle henkilöstölle, mihin pyritään vastaamaan riittävillä koulutustasovaatimuksilla.

Valtionhallinnolla on käytössään ja valmisteilla useita yhteiskunnan elintärkeiden toimintojen turvaamisen alaan liittyviä vaatimusmäärittelyjä, jotka omalta osaltaan täydentävät nyt käyttöön otettavaa turvallisuusauditointikriteeristöä. Kyseiset näkemykset on pyritty huomioimaan kriteeristötyössä. Merkittävänä rinnakkaisaineistona voidaan pitää erityisesti valtiovarainministeriön johdolla valmisteltuja tietoturvallisuuden ja varautumisen kokonaisuuksia linjaavia ohjeistoja. Turvallisuusauditointikriteeristön nyt julkaistavassa ensimmäisessä versiossa on huomioitu mahdollisimman pitkälle myös samanaikaisesti valmistelussa olleiden valtionhallinnon tietoturvallisuusasetuksen ja Euroopan Unionin uuden turvallisuusregulaation linjaukset. Kriteeristö täydentää lisäksi omalta osaltaan sekä kansainvälisiä tietoturvallisuusvelvoitteita, että turvallisuusselvityksiä säätäviin lakeihin sisältyviä menettelyjä.

Toimenpiteen johtoryhmä

Sisällys

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

SAATE 1 (1)

1325/50.01.00/2009
FI.PLM.2009-4910

20.11.2009

Sisäasiainministeriö

SISÄISEN TURVALLISUUDEN OHJELMA II, TOIMENPIDE 6.4. tp 2, KANSALLINEN TURVALLISUUSAUDITOINTIKRITEERISTÖ

Hallitus vahvisti 8.5.2008 sisäisen turvallisuuden ohjelman toisen vaiheen (STO II). Kyseisen ohjelman toimenpide-ehdotuksen 6.4 toinen toimenpide oli osoitettu puolustusministeriön johtovastuulle. Toimenpiteelle perustettiin johtoryhmä 12.9.2008 ja se organisoitui kokonaisuudessaan 5.12.2008 pidetyssä aloitusseminaarissa. Työn oli määrä olla valmis vuoden 2009 loppuun mennessä. Työ on luovutusvalmis tällä päivämäärällä.

Toimenpiteen tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi ja omavalvonnan sekä auditoinnin parantamiseksi. Toimenpiteen vastuualueen kattamiseksi johtoryhmä päätti perustaa neljä työryhmää sekä lisäksi erillisen seurantaryhmän palautteen saamiseksi työn eri vaiheissa.

Puolustushallinto, etunenässä puolustusvoimat, on pitkään huolehtinut niistä turvallisuusviranomaisen viranomaisvelvoitteista, joihin on ollut välttämätöntä vastata kansainvälisten sopimusten ja muiden käytänteiden vuoksi yritysten turvallisuustason varmentamiseksi. Sisäasiainhallinto on vuonna 2009 ottanut osaltaan vastuun näistä velvoitteista. Kansallinen turvallisuusauditointikriteeristö valmisteltiin laajalla otannalla maamme viranomais-, järjestö- ja yrityskentästä. Toimenpiteeseen osallistui yli sata henkilöä. Mittava työmäärä on jalostunut kriteeristöksi, jossa on huomioitu työn kuluessa välillä kovaakin ristivetoa aiheuttaneet kansalliset ja kansainväliset sidonnaisuudet. Täydellinen nyt valmistunut kriteeristö ei varmastikaan ole, joten työtä on syytä jatkaa, mihin toimenpiteen johtoryhmä liitteenä olevissa suosituksissaan ottaakin kantaa.

Esitän sisäasiainministeriölle, että tämä kansallinen turvallisuusauditointikriteeristö otetaan käyttöön viranomaisten yrityksiin kohdistaman turvallisuusauditoinnin perustana.

Kansliapäällikkö

Kari Rimpi

LIITTEET Toimenpiteen johtoryhmän suositukset (liite 1)
Luettelo toimenpiteeseen osallistuneista (liite 2)
Kansallinen turvallisuusauditointikriteeristö (liite 3

Postiosoite Puolustusministeriö PL 31 FI-00131 Helsinki Finland
Käyntiosoite Etelärinne Makasiinikatu 8 A 00130 Helsinki Finland
Puhelin (09) 16001 Internat. +358 9 16001
Faksi (09) 160 88278 Internat. +358 9 160 88278
s-post, internet puolustusministerio@defmin.fi www.defmin.fi

20.11.2009

TOIMENPITEEN 6.4.2 JOHTORYHMÄN SUOSITUKSET

Johtoryhmä luovuttaa kaikkien liitteessä 2 mainittujen työhön osallistuneiden puolesta kansallisen turvallisuusauditointikriteeristön puolustusministeriön välityksellä viranomaisten ja elinkeinoelämän käyttöön ja haluaa samalla antaa kaksi lopputuotteeseen liittyvää suositusta:

1. Sisäisen turvallisuuden ohjelman ohjausryhmän toivotaan pohtivan kansallisen turvallisuusauditointikriteeristön ylläpitovastuita ja -aikataulua. Toimenpiteen johtoryhmä suosittaa, että ylläpidon koordinaatio- ja ohjausvastuu olisi sisäisen turvallisuuden ohjelman sihteeristöllä. Samalla johtoryhmä toivoo, että nyt luovutettavan kriteeristötyön viranomaisosapuolet voisivat jatkossakin yhdessä elinkeinoelämän edustuksen kanssa toimia kriteeristön ylläpitäjinä vuosittaiseen tarkasteluun pohjautuen.

2. Toimenpiteen johtoryhmä esittää, että opetusministeriö pohtisi kansalliseen turvallisuusauditointikriteeristöön pohjautuvan koulutuksen aloittamista ja siihen liittyviä edellytyksiä. Johtoryhmä suosittaa koulutuksen jalkauttamista turvallisuusauditoinnin kokonaishallintaa koskevaksi ammattikorkeakoulutasoiseksi opetukseksi, ja toisaalta itse auditointitehtävään keskittyväksi ammatilliseksi tai täydennyskoulutustyyppiseksi opetukseksi. Toimenpiteen kuluessa johtoryhmän puoleen on käännytty usean oppilaitoksen taholta ja tiedusteltu mahdollisuutta aloittaa kyseinen koulutus pikaisestikin. Johtoryhmä haluaa kuitenkin tähdentää, että koulutuksen lopputuloksen valvonta on erityisen oleellista siitä syystä, että viranomaisen on voitava luottaa sen työn laatuun, jota oppikokonaisuuden läpäisseet mahdollisesti viranomaisen toimeksiannosta tekevät.

Johtoryhmä
Kalevi Tiihonen, Elinkeinoelämän keskusliitto
Arto Heiska, suojelupoliisi
Tommi Reen, sisäasiainministeriö
Matti Kesäläinen, puolustusministeriö

TOIMENPITEESEEN OSALLISTUNEET HENKILÖT JA ORGANISAATIOT

1. Johtoryhmä

Kalevi Tiihonen, Elinkeinoelämän Keskusliitto
Arto Heiska, suojelupoliisi
Tommi Reen, sisäministeriö
Matti Kesäläinen, puolustusministeriö

2. Työryhmät

HALLINNOLLINEN TURVALLISUUS
pj. Heljo Laukkala, Metso
Martti Herman Pisto, Outokumpu
Kari Harju, suojelupoliisi
Reijo Kaariste, puolustusvoimat
Tarmo Vuorinen, Patria
(Harri Uusitalo, Suomen Lähikauppa, seurantaryhmän edustajana)

HENKILÖSTÖTURVALLISUUS
pj. Ilkka Hanski, suojelupoliisi
Terhi Vira, puolustusvoimat
Rauno Hammarberg, Nokia
Reijo Lähde, OP-Keskus
Seppo Sundberg, Valtiokonttori
Elisa Kumpula, tietosuojavaltuutetun toimisto
(Mats Fagerström, Helsingin Energia, seurantaryhmän edustajana)

FYYSINEN TURVALLISUUS
pj. Mikko Viitasaari, UPM Kymmene
varapj. Juha Elomaa, suojelupoliisi
Aku Pänkäläinen, Finanssialan keskusliitto
Juha Åberg, puolustusvoimat
Juha Kreus, Laurea
(Jouni Viitanen, suojelupoliisi, seurantaryhmän edustajana)

TIETOTURVALLISUUS
pj. Timo Lehtimäki, Viestintävirasto
varapj. Matti Viirret, suojelupoliisi
Sami Hohenthal, suojelupoliisi
Mikko Valkonen, Teollisuuden Voima
Mikko Hakuli, puolustusvoimat
Ari Takanen, Codenomicon
Paavo Laakso, Itella
Erkki Mustonen, F-Secure
(Kalevi Halonen, Tietoturva r.y., seurantaryhmän edustajana)

3. Seurantaryhmä

Timo Härkönen, Heikki Hovi, valtioneuvoston kanslia
Erkki Väätäinen, Markku Meriluoto, ulkoministeriö
Mikael Kiviniemi, valtiovarainministeriö
Rauli Parmes, liikenne- ja viestintäministeriö
Kari Mäkinen, työ- ja elinkeinoministeriö
Jukka Savolainen, rajavartiolaitos
Saija Hyttinen, Marko Hasari, suojelupoliisi
Kimmo Markkula, Markku Ranta-aho, keskusrikospoliisi
Erkki Hämäläinen, Helsingin poliisilaitos
Sauli Savisalo, Huoltovarmuuskeskus
Tom Ferm, Jussi Leppälä, Tullihallitus
Matti Räisänen, Petri Käyhkö, Suomen kaupan liitto
Mats Fagerström, Helsingin Energia
Harri Koskenranta, Laurea-ammattikorkeakoulu
Jarkko Paananen, Kaarlo Haario, AEL
Päivi Rosenqvist, Aulis Koistinen, Tero Koivisto, Innova
Jari Pirhonen, Pete Nieminen, Kalevi Halonen, Tietoturva r.y.
Jouko Laitinen, FinnSecurity r.y.
Esa Valtonen, Harri Uusitalo, Veli-Matti Lumiala, Secman r.y.
Catharina Candolin, Juha Putkonen, Tero Lampen, puolustusvoimat
Juha Pekkola, puolustusministeriö

Sisäasiainministeriön sisäisen turvallisuuden sihteeristön pöytäkirja 4/2009/ 26.11.2009

SISÄISEN TURVALLISUUDEN MINISTERIRYHMÄN PÄÄTÖS 26.11.2009

Sisäisen turvallisuuden ministeriryhmän kokouksessa 26.11.2009 tehtiin viitteenä olevan pöytäkirjan mukaisesti kansallista turvallisuusauditointikriteeristöä (KATAKRI) koskeva alla oleva päätös.

Kokouksessa olivat läsnä seuraavat henkilöt:

Sisäasiainministeri Anne Holmlund, puheenjohtaja
Oikeusministeri Tuija Brax
Puolustusministeri Jyri Häkämies
Valtiosihteeri Heljä Misukka, OPM
Erityisavustaja Anna Anttinen, LVM
Erityisavustaja Kristiina Kokko, SM
Erityisavustaja Mikko Ollikainen, OPM
Erityisavustaja Corinna Tammenmaa, SM
Alivaltiosihteeri Heikki Aaltonen, VNK
Ylijohtaja Jarmo Littunen, OM
Johtaja Kari Paaso, STM
Neuvotteleva virkamies Merja Söderholm, STM
Päällikkö Tarja Mankkinen, SM, sihteeri

Turvallisuusjohtaja Juha Pekkola PLM, asiantuntija

Päätös:

Sisäisen turvallisuuden ministerityhmä päätti esityksen mukaisesti, että sisäisen turvallisuuden ohjelmaan sisältyvä toimenpide 6.4 tp 2 on valmistunut.

Ministeriryhmä suosittaa kansallisen turvallisuusauditointikriteeristön (KATAKRI) käyttöönottoa.

Sisäisen turvallisuuden ministeriryhmä päätti, että sisäisen turvallisuuden ohjelman ohjausryhmän tulee valmistella päätökset koskien turvallisuusauditointikriteeristön toimeenpanon, ylläpidon ja jatkovalmistelun organisointia ottaen huomioon toimenpiteen valmistelusta vastanneen johtoryhmän suositukset.

OSA-ALUE

HALLINNOLLINEN TURVALLISUUS JA TURVALLISUUSJOHTAMINEN

Johdanto

Hallinnollisen turvallisuuden ja turvallisuusjohtamisen kysymyssarja turvallisuusauditointia varten.

Kriteeristön osa-aluetta on lähestytty tarkastelemalla hallinnollista turvallisuustyötä turvallisuuden johtamisena. Kokonaisuuden perusteena käsitellään turvallisuuden johtamisjärjestelmää ja sen osa-alueiden auditoinnissa vaadittavaa vähimmäistasoa suojaustasoissa II (korkea taso), III (korotettu taso) ja IV (perustaso). Lisäksi kriteeristö sisältää elinkeinoelämän omaehtoista turvallisuustyötä silmällä pitäen lähtötason suositukset turvallisuusjohtamisen alalla.

Ohjeistoa sovelletaan alihankintaketjuun siten, kuin organisaatiolla on mahdollisuus toimeksiantonsa perusteella siirtää työtä alihankintaan. Organisaatio vastaa samojen periaatteiden auditoinnista alihankintayrityksissä.

Sisällys

Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 101.0 **Onko organisaation johto määrittänyt ja hyväksynyt turvallisuuspolitiikan. Onko politiikka tarkistettu määräajoin?** *Kysymyksellä arvioidaan: Organisaation turvallisuusjohtamisen kypsyystasoa*	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina tai osana yleisten tavoitteita	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina tai osana yleisten tavoitteita	Organisaatiolla on kirjattuna ylimmän johdon hyväksymä turvallisuuspolitiikka tai vastaava turvallisuustoimintaa ohjaava hyväksytty määrittely.	Organisaatiolla on voimassa oleva, julkaistu ja koulutettu turvallisuuspolitiikan nimellä dokumentoitu turvallisuustoiminnan ylätason asiakirja, joka on ylimmän johdon hyväksymä. Turvallisuuspolitiikka tarkistetaan vähintään vuosittain ja tarkistukset dokumentoidaan sekä hyväksytetään ylimmällä johdolla. Organisaation turvallisuuspolitiikka ohjaa seuraavia kokonaisuuksia: turvallisuuden vuotuinen toimintaohjelma, turvallisuustyön tavoitteet, riskien tunnistamisen arviointi ja kontrollit, turvallisuusorganisaatio ja vastuut, onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennaltaehkäisevät toimenpiteet, turvallisuusdokumentaatio ja sen hallinta, koulutuksen ja tietoisuuden lisääminen sekä osaamisen, raportoinnin ja johdon katselmukset.		
A 102.0 **Mitä turvallisuuden osatekijöitä turvallisuuspolitiikka ja/tai turvallisuuden johtaminen organisaatiossa kattaa?** *Kysymyksellä arvioidaan: Turvallisuustyön kokonaisvaltaisuutta ja järjestelmällisyyttä.*	Turvallisuusdokumentaatio sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet.	Turvallisuusdokumentaatio sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet.	Turvallisuusdokumentaatio sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet sekä turvallisuuspolitiikassa todetun turvallisuusjohtamisen selkeän organisoinnin.	Turvallisuusdokumentaatio sisältää perustan laajalle ja kokonaisvaltaiselle lähestymistavalle. Esimerkiksi turvallisuuskäsite kattaa: turvallisuusjohtamisen, tuotannon ja toiminnan turvallisuuden, työturvallisuuden, ympäristöturvallisuuden, pelastustoiminnan, poikkeustilanteiden hallinnan, tietoturvallisuuden, henkilöstöturvallisuuden, tilaturvallisuuden, ulkomaantoimintojen turvallisuuden ja rikosturvallisuuden.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 103.0 **Vastaako organisaation turvallisuusdokumentaatio toiminnan ja tuotteiden laajuutta ja toimintatapaa sekä niihin liittyviä turvallisuusriskejä?** *Kysymyksellä arvioidaan: Turvallisuuspolitiikan tasoa.*	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä projektidokumenttina tai osana yleisten tavoitteita.	Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä projektidokumenttina tai osana yleisten tavoitteita.	Turvallisuusdokumentaatio käsittelee organisaatiota yksilöllisesti ja ottaa huomioon muutokset organisaation toiminnassa	Organisaation turvallisuusdokumentaatio sisältää ja kattaa kaikki organisaation toimintaan kuuluvat menettelyt. Riskien käsittely on suhteessa organisaation toimintaan.		
A 104.0 **Toimivatko organisaation kaikki tasot turvallisuuspolitiikan mukaisesti?** *Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisältämien asioiden viemistä organisaation kaikille tasoille.*	Organisaatio pystyy osoittamaan turvallisuustyössään turvallisuuspolitiikan tai projektidokumentin velvoitteiden valvonnan toteutumisen osana muuta valvontaa tai erillisenä turvallisuusauditointina.	Ei vaatimusta.	Organisaatiolla on selvä ohjelma valvoa turvallisuuspolitiikan perusteiden mukaista toimintaa. Valvonnan tulokset ovat esitettävissä.	Organisaatio pystyy sisäisten ja ulkoisten auditointien tuloksilla osoittamaan, että se kaikilla tasoilla sitoutuu turvallisuustyön vaatimuksiin ja niiden toteuttamiseen.		
A 105.0 **Huomioiko turvallisuuspolitiikka yleisen lainsäädännön ja paikallisten turvallisuusmääräysten sisältämät velvoitteet?** *Kysymyksellä arvioidaan: Organisaatiota koskevan turvallisuuslainsäädännön tuntemusta ja lainsäädännön soveltamisen valvontaa.*	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa.	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa.	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa. Turvallisuuslainsäädännön seuraaminen on määritetty organisaation tehtävänkuvauksessa henkilön tai toiminnon tehtäväksi.	Organisaatiota koskevan turvallisuuslainsäädännön seuranta on vastuutettu tietylle henkilölle tai toiminnolle. Lainsäädännön soveltaminen ja sen seuranta turvallisuusohjeissa on myös määritetty tehtäväkuvauksissa.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 106.0 **Pääkysymys:** **Onko turvallisuuspolitiikan sisältö tiedotettu kaikille työntekijöille, jotta heillä on selvä kuva omista turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan?** *Lisäkysymys:* *Onko turvallisuuspolitiikka-dokumentaatio jatkuvasti kaikkien saatavilla?* *Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön viemistä organisaation kaikille tasoille ja politiikan vaatimusten mukaisen toiminnan varmistamista jokapäiväisessä työssä.*	Turvallisuuspolitiikka tai vastaava turvallisuusohjeistus on koulutettu koko henkilöstölle ja se on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuuspolitiikka tai vastaava turvallisuusohjeistus on koulutettu koko henkilöstölle ja se on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuuspolitiikka on koulutettu koko henkilöstölle. Koulutus on dokumentoitu. Koulutus kerrataan esimerkiksi osana muuta koulutusta. Politiikka on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla. Organisaation turvallisuuspolitiikka on koulutettu tarvittaville sidosryhmien edustajille.	Organisaation turvallisuuspolitiikka on koulutettu koko henkilöstölle ja se on osa perehdyttämiskoulutusta. Politiikan tunteminen on varmistettu sisällyttämällä sen kertaus osaksi muuta koulutusta. Politiikka on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla. Turvallisuuspolitiikan koulutuksen kattavuus on dokumentoitu osallistujien ja sisällön osalta. Turvallisuuspolitiikka on koulutettu myös tarvittaville sidosryhmien edustajille.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 107.0 **Sisältääkö organisaation turvallisuuspolitiikka vaatimuksen kaikkien työntekijöiden sitoutumisesta jatkuvaan turvallisuustilanteen parantamiseen?** *Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön kattavuutta.*	Turvallisuuspolitiikka ja/tai -ohjeisto sisältää henkilökohtaisen sitoutumisen merkityksen.	Ei vaatimuksia.	Turvallisuuspolitiikka sisältää henkilökohtaisen sitoutumisen merkityksen.	Turvallisuuspolitiikassa kuvataan johdon ja yksittäisten henkilöiden sitoutumisen tarve turvallisuuspolitiikkaan ja korostetaan, että se on jokaista henkilöä koskeva asia, joka toisaalta velvoittaa yksilöä ja toisaalta myös takaa häiriöttömän toiminnan ja työn jatkumisen. Turvallisuus tunnistetaan organisaation laatu- ja kilpailutekijänä.		
A 108.0 **Onko turvallisuuspolitiikassa määritetty organisaation keskeiset turvallisuustavoitteet?** *Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön kattavuutta.*	Keskeiset tavoitteet on kuvattu turvallisuuspolitiikassa tai -ohjeistossa.	Keskeiset tavoitteet on kuvattu turvallisuuspolitiikassa tai -ohjeistossa.	Keskeiset turvallisustavoitteet on kuvattu turvallisuuspolitiikassa.	Organisaation turvallisuuspolitiikassa on kuvattu keskeiset turvallisuuden tavoitteet koskien niitä seikkoja, jotka takaavat organisaation laatu- ja kilpailutekijät.		

Turvallisuuden vuotuinen toimintaohjelma, osa-alue A200

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 201.0 **Onko organisaatiolla kirjoitettu ja dokumentoitu toimintaohjelma turvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?** *Kysymyksellä arvioidaan: Organisaation kykyä tunnistaa turvallisuuden kokonaisuus, oman toiminnan vahvuudet ja sellaiset alueet, joissa tarvitaan parantamista.*	Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Ei vaatimuksia.	Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Organisaatiolla on kaikkia turvallisuuden osa-alueita koskeva toimintaohjelma, joka kattaa toimenpiteet, vastuut, aikataulut ja mitattavat tulokset. Toimintaohjelma käsittelee myös turvallisuuden johtamisen kehitystyön samaan periaatteeseen perustuen.		
A 202.0 **Onko toimintaohjelmassa eritelty menetelmät, vastuut ja aikataulut tavoitteiden saavuttamiseksi?** *Kysymyksellä arvioidaan: Ohjelman yksityiskohtaisuutta.*	Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Ei vaatimuksia.	Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Turvallisuuden vuotuinen toimintaohjelma sisältää organisaation työnkuvauksiin perustuvan suunnitelman turvallisuuden hallinnoitavien osa-alueiden jatkuvaksi parantamiseksi. Vuotuinen suunnitelma sisältää tavoitteet, vastuut ja mitattavat tavoitteet.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 203.0 **Tarkistetaanko toiminta-ohjelma säännöllisesti?** *Kysymyksellä arvioidaan: Ottaako organisaatio huomioon mahdollisesti muuttuvat tilanteet ja päivitetäänkö vuotuinen toimintaohjelma tarvittaessa muutosten mukaisesti.*	Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.	Ei vaatimuksia.	Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.	Organisaatiolla on säännöllinen prosessi (esimerkiksi johtoryhmän tai turvallisuuden johtoryhmän kokouskäytäntö), jossa yhtenä asiakohtana on vastuullisen tahon esittelemä katsaus turvallisuuden toiminta-ohjelman etenemisestä ja mahdollisista tarpeista kehittää ohjelmaa tavoitteiden, vastuiden tai aikataulun suhteen.		

Turvallisuustyön tavoitteiden määrittely, osa-alue A300

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 301.0 **Onko organisaation liiketoiminta ja sitä tukeva turvallisuuspolitiikka ja -ohjelma perusteena turvallisuustyön tavoitteita asetettaessa?** *Kysymyksellä arvioidaan: Muodostavatko politiikka, ohjelma ja tavoitteiden asettaminen kokonaisuuden.*	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.	Toimintaohjelman tavoitteissa on kattavasti huomioitu turvallisuuspolitiikan kattamat alueet.		
A 302.0 **Onko organisaatio asettanut turvallisuustavoitteet organisaation eri hierarkiatasoille ja/tai toiminnoille?** *Kysymyksellä arvioidaan: Tavoitteiden konkreettista asettamista ja eri osatavoitteiden merkityksellisyyden ymmärtämistä organisaation eri osien ja hierarkiatasojen osalta. Tavoitteiden dokumentoinnilla varmistetaan se, että vaatimustasoa voidaan kehittää jatkuvan parantamisen periaatteella.*	Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltynä organisaation toiminnassa tarvittavat osat ja tasot.	Ei vaatimuksia.	Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltynä organisaation tarvittavat osat ja tasot.	Organisaatio on määrittänyt selkeästi mitattavat tavoitteet organisaation kokonaisuudelle ja osille sekä tasoille toiminnan vaatimusten mukaisesti. Tavoitteet on dokumentoitu ja ne ovat osa organisaation johtamisjärjestelmää.		
A 303.0 **Onko tavoitteet asetettu siten, että niiden saavuttaminen on mitattavissa?** *Kysymyksellä arvioidaan: Tavoitteiden konkreettista ja realistista asettamista sekä laadullisten mittareiden sisällyttämistä tavoitteisiin.*	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.	Turvallisuustyön tavoitteet on asetettu siten, että eri osille ja organisaation hierarkiatasoille on niitä koskevat mitattavat tavoitteet. Mitattavuus on esimerkiksi kuvattu annettavan koulutuksen kattavuutena, turvallisuuspoikkeamien määrän vähenemisenä tai vastaavana selkeänä tavoitteena.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A304.0 **Onko tavoitteiden saavuttamiselle asetettu aikataulu?** *Kysymyksellä arvioidaan: Tavoitteiden konkreettista ja realistista asettamista.*	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteille on kaikilta osin asetettu aikataulu.		
A 305.0 **Onko seuraavat tekijät otettu huomioon tavoitteiden asettamisen yhteydessä:** a. tunnistetut riskit b. organisaation oman toiminnan ja/tai liiketoiminnan vaatimukset c. tekniset vaatimukset ja mahdollisuudet d. taloudelliset vaatimukset e. muiden intressiryhmien vaatimukset (esim. asiakkaat, viranomaiset) f. lainsäädännön ja/tai muiden ohjeistojen sekä sopimusten vaatimukset *Kysymyksellä arvioidaan: Onko tavoitteita asetettaessa tunnistettu mm. edellä kuvatut vaatimukset, mahdollisuudet ja rajoittavat tekijät.*	Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), d), e), f).	Ei vaatimuksia.	Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), e), f).	Tavoitteiden asettamisen yhteydessä on huomioitu tekijät a), b), c), e), f).		

Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 401.0 **Onko organisaatiolla menetelmät tunnistaa ja arvioida turvallisuusriskit?** *Kysymyksellä arvioidaan: Priorisoiko organisaatio turvalisuustyönsä arvioimalla riskit.*	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.	Riskienarviointi on jatkuva prosessi, joka sisältää riskin tunnistamisen, todennäköisyyden ja vaikuttavuuden arvioinnin, tarvittavat toimenpiteet, vastuut ja aikataulut. Riskienarvioinnit toteuttavat organisaation parhaat asiantuntijat. Riskienarviointi on perustana turvallisuustyön priorisoinnille.		
A 402.0 **Kattavatko nämä menetelmät normaalin toiminnan, erityistilanteet, onnettomuudet ja hätätapaukset?** **Otetaanko aliurakoitsijat ja palveluntarjoajat huomioon?** *Kysymyksellä arvioidaan: Riskienarvioinnin kattavuutta.*	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu myös normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.	Arvioitavat riskit sisältävät laaja-alaisesti koko organisaation toimintakentän ja mahdolliset erityistilanteet. Asiat on huomioitu normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.		
A 403.0 **Dokumentoidaanko riskienarviointien tulokset ja päivitetäänkö ne säännöllisesti?** *Kysymyksellä arvioidaan: Onko organisaatiossa todennettava järjestelmä riskien arvioinneista tallenteineen.*	Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskien arvioinnit dokumentoidaan siten, että ne ovat todennettavissa.	Ei vaatimuksia.	Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskien arvioinnit dokumentoidaan siten, että ne ovat todennettavissa.	Turvallisuusriskien arviointi on määritetty osaksi organisaation johtamisprosessia ja se taltioidaan osana organisaation dokumentointijärjestelmää.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 404.0 **Otetaanko riskienarviointien havainnot huomioon turvallisuustoiminnan tavoitteita asetettaessa?** *Kysymyksellä arvioidaan: Onko riskienarviointi osa laadukasta turvallisuustoimintaa, joka tähtää jatkuvaan toiminnan tason parantamiseen.*	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.	Riskienarviointityökalu sisältää toimenpiteet, joita riskien hallitseminen edellyttää sekä vastuut ja aikataulut. Näitä hyödynnetään, kun organisaation turvallisuustoiminnan tavoitteita asetetaan. Riskienarviointiprosessi on kuvattu.		
A 405.0 **Voidaanko riskienarvioinnin tulosten perusteella priorisoida riskit?** *Kysymyksellä arvioidaan: Saadaanko tuloksena perusteet riskienhallinnan toimenpiteiden valinnalle, tärkeysjärjestykselle ja kiireellisyydelle.*	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.	Riskienarviointi perustuu riskin todennäköisyyden ja vaikuttavuuden arviointiin siten, että tuloksena on riskiluokitus, jota voidaan käyttää määritettäessä tarve poistaa riski, parantaa riskin hallitsemista tai pienentää tunnistetun riskin vaikutusta.		
A 406.0 **Antavatko riskienarvioinnit perusteet turvallisuuskoulutuksen vaatimuksille?** *Kysymyksellä arvioidaan: Onko riskienarviointi myös työkalu, joka tukee koulutuksen suunnittelua yhtenä keinona pienentää riskin vaikutusta.*	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 407.0 **Onko organisaatiolla menetelmät valvoa turvallisuuden riskienarviointien perusteella tehtyjen toimenpiteiden toteuttamista ja tehokkuutta?** *Kysymyksellä arvioidaan: Toteutuuko riskienarvioinnin perusteella valittujen toimenpiteiden haluttu vaikutus.*	Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.	Ei vaatimuksia.	Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.	Turvallisuusjohtamisen syklissä käsitellään riskienarvioinnin perusteella laadittujen toimenpiteiden oikea laatu ja laajuus sekä vaikuttavuus verrattuna haluttuun tulokseen.		

Turvallisuusorganisaatio ja vastuut, osa-alue A500

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 501.0 **Onko turvallisuustyön vastuut määritetty? Kattavatko määrittelyt organisaation eri tasot?** *Kysymyksellä arvioidaan: Onko turvallisuustyön vastuut asetettu siten, että kaikki toiminnot ja organisaation tasot on katettu.*	Turvallisuusorganisaatio kattaa ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty.	Turvallisuusorganisaatio kattaa ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty.	Turvallisuusorganisaatio kattaa turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.	Turvallisuustyön vastuut on määritetty turvallisuusjohtamisen ja turvallisuuspolitiikan mukaisten osa-alueiden sekä organisaation toimintojen ja tasojen suhteen. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.		
A 502.0 **Onko roolit, vastuut ja toimeenpanovalta tiedotettu organisaatiossa ja niille ulkopuolisille tahoille, joiden on tunnettava turvallisuusorganisaation rakenne?** *Kysymyksellä arvioidaan: Tietääkö organisaatio ne henkilöt, jotka vastaavat eri turvallisuuden osa-alueista ja jotka samalla pystyvät tukemaan eri ongelmatilanteissa.*	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuusorganisaation rakenne ja vastuut on koulutettu ja tiedot on jatkuvasti saatavissa päivitettyinä koko organisaatiossa mukaan lukien tarvittavat sidosryhmät.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 503.0 **Onko turvallisuustyölle suunnattu riittävästi resursseja työn toteuttamiseksi, kontrolloimiseksi sekä parantamiseksi?** **Resurssien tulisi kattaa:** **– henkilöstö** **– erityisosaaminen** **– teknologiset resurssit** **– taloudelliset resurssit** *Kysymyksellä arvioidaan: Onko turvallisuustyöllä realistiset onnistumisen mahdollisuudet.*	Turvallisuusjohtaminen kattaa mm. henkilöstön, teknologian ja taloudellisten resurssien riittävyyden arvioinnin.	Ei vaatimuksia.	Turvallisuustyöstä vastaa koulutettu ja kokenut henkilöstö, jonka osaamistasoa ylläpidetään suunnitellusti ja jatkuvasti. Turvallisuusjohtaminen kattaa mm. henkilöstön, teknologian ja taloudellisten resurssien riittävyyden arvioinnin. Osatekijät on sisällytetty osaksi turvallisuustyön jatkuvaa parantamista.	Turvallisuustyöstä vastaa koulutettu ja kokenut henkilöstö, jonka osaamistasoa ylläpidetään suunnitellusti ja jatkuvasti. Osaamisen jatkuvuus on turvattu hyvällä henkilöstösuunnittelulla. Laadukasta turvallisuusteknologiaa käytetään osana turvallisuuden hallintaa ja se on integroitu tarkoituksenmukaisesti.		
A 504.0 **Onko organisaation ylin johto määrittänyt henkilön, joka on vastuussa turvallisuustoiminnan kehittämisestä ja johtamisesta sekä siitä, että turvallisuustyö kattaa kaikkien organisaation tasojen tarpeet?** *Kysymyksellä arvioidaan: Onko turvallisuudesta vastaavalla henkilöllä johdon tuki ja aseman tuoma valtuus ja onko asetettu tehtävä riittävän laaja-alainen kokonaisuuden hallitsemiseksi. Tehtävä voi olla osa henkilön muuta toimenkuvaa.*	Organisaatiolla on turvallisuudesta vastaava henkilö, jolla on riittävät mahdollisuudet johtaa turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Tehtäväkenttä voi olla myös jaettu, mikäli se on organisaation toiminnan kannalta tarkoituksenmukaista.	Organisaatiolla on turvallisuudesta vastaava henkilö, jolla on riittävät mahdollisuudet johtaa turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Tehtäväkenttä voi olla myös jaettu, mikäli se on organisaation toiminnan kannalta tarkoituksenmukaista.	Organisaatiolla on turvallisuudesta keskitetysti vastaava henkilö, jolla on riittävät mahdollisuudet johtaa ja koordinoida turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet.	Organisaatiossa on nimetty turvallisuusvastaava, jolla on kokonaisvaltainen vastuu turvallisuuden kehittämisestä ja johtamisesta osana organisaation johtamista. Tehtävä kattaa turvallisuuden osa-alueet, organisaation osat ja tasot.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 505.0 **Onko nimetyllä turvallisuustyöstä vastaavalla henkilöllä vastuu ja valtuus sen varmistamiseksi, että turvallisuuden johtamisjärjestelmä on muodostettu niiden vaatimusten mukaisesti, joita tavoitteissa on asetettu?** *Kysymyksellä arvioidaan: Onko turvallisuustoimitaa johtavalla henkilöllä mahdollisuus vaikuttaa johtamisjärjestelmään siten, että turvallisuustavoitteiden saavuttaminen on mahdollista.*	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisessa asemassa, että hänellä on mahdollisuus vaikuttaa turvallisuuden toteuttamiseen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisessa asemassa, että hänellä on mahdollisuus vaikuttaa turvallisuuden toteuttamiseen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisella tasolla, että hänellä on mahdollisuus vaikuttaa turvallisuuden johtamisjärjestelmän kokonaisuuteen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisella tasolla, että hänellä on mahdollisuus vaikuttaa turvallisuuden johtamisjärjestelmään osana organisaation normaalia johtamista. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.		
A 506.0 **Onko organisaation johto sitoutunut turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen?** *Kysymyksellä arvioidaan: Toteutuuko turvallisuustyöhön sitoutuminen organisaation kaikilla tasoilla. Organisaation johdon esimerkin vaikutus on ratkaiseva tekijä.*	Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa.	Ei vaatimuksia.	Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa. Malli on yksilöitävä organisaation prosessikuvauksessa.	Organisaation johto osoittaa sitoutumistaan konkreettisesti turvallisuusvaatimuksia noudattamalla ja kehitystyöhön osallistumalla. Johto tuo esille turvallisuuden tavoitteita, menetelmiä ja saavutuksia osana muuta johtamistoimintaa.		

Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, osa-alue A600

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 601.0 **Onko organisaatiolla jatkuvuudenhallintamenettely?** *Kysymyksellä arvioidaan: Onko organisaatio tunnistanut toimintaa uhkaavat häiriöt ja varautunut niistä sellaisiin, jotka voivat hidastaa tai estää päätavoitteiden saavuttamista.*	Organisaatio on tunnistanut jatkuvuuttaan uhkaavat tärkeimmät seikat ja varautunut niihin suojaus-, varmennus-, kahdennus- yms. menettelyin. Organisaatiolla on lakisääteinen vakuutusturva.	Ei vaatimuksia.	Organisaation toiminnan johtamisessa on otettu huomioon varautuminen liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin ja laadittu niitä koskevat valmius- ja toipumissuunnitelmat organisaation keskeisimpiin toimintoihin. Resurssitarve on määritetty ja niiden saatavuus suunniteltu. Jatkuvuuden hallinnan toteutumista seurataan ja arvioidaan.	Organisaation toiminnan johtamisessa on otettu huomioon varautuminen liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin ja laadittu niitä koskevat valmius- ja toipumissuunnitelmat. Resurssit on määritetty ja varattu, menetelmät on koulutettu ja testattu. Jatkuvuuden hallinnan toteutumista seurataan ja arvioidaan. Jatkuvuudenhallinta on viety läpi koko organisaation kattaen kaikki organisaation prosessit. Menettelytapa on dokumentoitu. Keskeytysriskit on suunnitellusti vakuutettu.		
A 602.0 **Onko organisaatiossa määritetty onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt?** *Kysymyksellä arvioidaan: Onko organisaatio ottanut huomioon turvallisuuspoikkeamat ja onko niiden hallinta määritetty ja organisoitu. Onko yhteistoiminta viranomaisten suuntaan suunniteltu.*	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia.	Ei vaatimuksia.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Vastuut on kuvattu henkilöiden tehtäväkuvauksissa. Vastaavat henkilöt ovat hyvin selvillä organisaation ja viranomaisen välisestä toimivalta- ja vastuujaosta.	Onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt on määritetty ottaen huomioon organisaation toiminnan laajuus, organisaation osat ja tasot. Henkilöt ovat hyvin selvillä organisaation ja viranomaisen välisestä toimivalta- ja vastuujaosta.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 603.0 **Onko vastuut kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi määritetty?** *Kysymyksellä arvioidaan: Onko organisaatio ottanut ennakolta huomioon poikkeavien tilanteiden ilmenemisen ja onko riskien pienentäminen määritetty ja organisoitu.*	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.	Ei vaatimuksia.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa. Kuvaus sisältää riskien pienentämisen vastuun.		
A 604.0 **Onko organisaatiolla menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien sekä korjaavien toimenpiteiden tekemiseksi?** *Kysymyksellä arvioidaan: Onko organisaatiolla menetelmät valvoa turvallisuustilannetta ja menetelmät sekä valmius suojaavien ja korjaavien toimenpiteiden tekemiseksi.*	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat.	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.	Organisaatiolla on dokumentoitu järjestelmä, jolla se seuraa ja raportoi turvallisuuspoikkeamat kaikkien turvallisuuden osa-alueiden osalta. Poikkeamien seurantajärjestelmä on jatkuva. Organisaatiolle on määritetty vastuut ja valta toteuttaa suojaavat sekä korjaavat toimenpiteet.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 605.0 **Onko organisaatiolla menetelmät sen varmistamiseksi, että tehdyt suojaavat ja korjaavat turvallisuustoimenpiteet ovat tehokkaita ja oikein kohdistettuja?** *Kysymyksellä arvioidaan: Tehdäänkö turvallisuuden saavuttamiseksi oikeita asioita.*	Turvallisuustoimenpiteiden vaikutus arvioidaan ja organisaatiolla on käsitys panos-tuotos -suhteesta.	Ei vaatimuksia.	Turvallisuustoimenpiteiden toivottua ja saavutettua vaikutusta verrataan. Organisaatiolla on käsitys panos-tuotos -suhteesta.	Turvallisuustoimenpiteiden toivottua ja saavutettua vaikutusta verrataan säännöllisesti. Organisaatiolla on käsitys panos-tuotos -suhteesta.		
A 606.0 **Onko organisaatiolla menetelmät arvioida riskit, joita suunnitellut korjaavat toimenpiteet aiheuttavat?** *Kysymyksellä arvioidaan: Varmistaako organisaatio turvallisuusjärjestelmiä muutettaessa, ettei samalla aiheuteta uusia uhkia tai vaaratilanteita.*	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.	Ei vaatimuksia.	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.		
A 607.0 **Onko organisaatiolla menetelmät turvallisuustoimenpiteiden vaikutusten analysointia varten?** *Kysymyksellä arvioidaan: Dokumentoiko ja analysoiko organisaatio turvallisuustoimenpiteet sekä niiden vaikutukset.*	Organisaatio seuraa turvallisuustoimenpiteiden vaikutuksia.	Organisaatio seuraa turvallisuustoimenpiteiden vaikutuksia.	Organisaatio analysoi turvallisuustoimenpiteiden vaikutukset vähintään vuosittain. Esimerkiksi tilastoja seuraamalla tarkastellaan tietyn vaaratilanteen tapahtumataajuuden muutosta.	Organisaatiolla on prosessi, joka dokumentoinnin lisäksi säännöllisesti analysoi tehdyt turvallisuustoimenpiteet ja niiden vaikutukset organisaation turvallisuustasoon ja toimintaan vähintään vuosittain. Analyysit käytetään hyödyksi turvallisuustoimintaa kehitettäessä.		

Turvallisuusdokumentaatio ja sen hallinta, osa-alue A700

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 701.0 **Onko organisaatiolla toimintamallit, jotka koskevat:** **a. turvallisuustiedostoja / turvallisuusrekistereitä tai dokumentointimenetelmiä?** **b. turvallisuusdokumentaation tietojen yksilöintiä ja jäljittämistä?** **c. turvallisuusdokumentaation säilyttämisaikoja, säilytyspaikkaa ja säilytyksen vastuita?** *Kysymyksellä arvioidaan: Onko organisaatiolla järjestelmä, jonka avulla hallitaan edellä mainitut osatekijät.*	Organisaatiolla on järjestelmä, joka sisältää omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat.	Organisaatiolla on järjestelmä, joka sisältää omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat.	Organisaatiolla on järjestelmä, joka sisältää turvallisuusrekisterit, omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat. Järjestelmä täyttää lainsäädännön asettamat vaatimukset (mm. rekisteriseloste).	Organisaatiolla on helposti käytettävä ja sisällöltään kattava tietojenhallintajärjestelmä, joka on ulotettu organisaation kaikille tasoille. Järjestelmä sisältää turvallisuusrekisterit (esimerkiksi luvat) ja muut dokumentit (kuten ohjeet). Tietojen tallentaminen tapahtuu siten, että järjestelmän avulla tapahtumat voidaan yksilöidä ja jäljittää. Järjestelmä täyttää lainsäädännön asettamat vaatimukset esimerkiksi tiedon luottamuksellisuuden ja säilytysaikavaatimusten osalta.		
A 702.0 **Sisältävätkö rekisterit myös tiedot turvallisuustavoitteiden saavuttamisen tasosta?** *Kysymyksellä arvioidaan: Onko mitattavat tavoitteet asetettu selkeästi ja onko tavoitteiden toteutuminen helposti todettavissa järjestelmän avulla.*	Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.	Ei vaatimuksia.	Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.	Organisaatiolla on tietojenhallintajärjestelmä, josta ajantasaiset tiedot ovat saatavissa. Raportit ovat yksilöitävissä ja vertailtavissa ajan, paikan ja aiheen mukaisesti.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 703.0 **Sisältävätkö turvallisuusrekisterit tiedot annetuista turvallisuuskoulutuksista?** *Kysymyksellä arvioidaan: Rekisteröidäänkö turvallisuuskoulutukset siten, että niiden riittävyys ja voimassaolo voidaan todeta. Onko asetetut vaatimukset täytetty.*	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö.	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö.	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus, sen sisältö ja voimassaolo.	Organisaatiolla on turvallisuuden eri osa-alueisiin liittyvä koulutusrekisteri erillisenä tai osana organisaation muuta koulutusrekisteriä. Tietojen avulla voidaan seurata sitä, että kaikkiin koulutusta vaativiin tehtäviin koulutus on annettu ja koulutusten vanhentuminen on havaittavissa siten, että kertauskoulutus ja täydennyskoulutus voidaan antaa velvoitteiden täyttämiseksi.		
A 704.0 **Voidaanko dokumentaation perusteella osoittaa, että turvallisuuskoulutuksen taso on riittävän korkea?** *Kysymyksellä arvioidaan: Onko turvallisuuskoulutukselle asetettu määrälliset ja laadulliset tavoitteet ja rekisteröidäänkö näiden täyttyminen.*	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.	Ei vaatimuksia.	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.		

Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 801.0 **Ovatko organisaation kaikki henkilöt tietoisia turvallisuusvaatimusten noudattamisen tärkeydestä ja oikeista toimintatavoista?** *Kysymyksellä arvioidaan: Organisaation turvallisuuskulttuurin kypsyystasoa ja johdon sitoutumista turvallisuuden jatkuvaan parantamiseen kouluttamisen avulla.*	Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Erillisiin projekteihin osallistuva henkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Erillisiin projekteihin osallistuva henkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Projektihenkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Organisaation koko henkilöstö on koulutettu turvallisuuden tavoitteiden osalta. Projektihenkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.		
A 802.0 **Onko varmistuttu siitä, että henkilöstö tuntee omaan työhönsä liittyvät turvallisuusriskit?** *Kysymyksellä arvioidaan: Onko turvallisuusasioiden riskienarviointi toteutettu siten, että henkilöstö on itse mukana arvioinnissa ja tuntee työhönsä liittyvät turvallisuusriskit.*	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.	Riskienarvioinnin yhteydessä käsitellään turvallisuuden kaikkia osa-alueita koskevat seikat ja henkilöstö osallistuu johdettuun riskienarviointiin.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 803.0 **Onko varmistuttu siitä, että henkilöstö osaa toimia oikein tilanteissa, joissa turvallisuus on vaarantunut?** *Kysymyksellä arvioidaan: Poikkeustilanteiden turvallisuusriskien hallintaa, esimerkiksi tilaturvallisuuden osalta tulipalotilanteet, tietoturvallisuuden osalta tietojen palauttamisen periaatteet.*	Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan.	Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan.	Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan säännöllisesti.	Organisaatiolla on riskienarviointiin perustuva dokumentoitu ja koulutettu toimintasuunnitelma tärkeimpien turvallisuusriskien varalle. Poikkeustilanteiden hallinta koulutetaan ja koulutettu toimintamalli harjoitellaan.		
A 804.0 **Onko organisaatiolla menetelmä varmistua siitä, minkä tasoista turvallisuuskoulutusta henkilöstö tarvitsee tehtävissään?** *Kysymyksellä arvioidaan: Onko organisaatiolla prosessi, jossa arvioidaan annettavan koulutuksen tarve huomioiden lakien vaatimukset, riskienarviointien perusteella annettavat keskeiset turvallisuusasiat ja yleiset turvallisuustietoisuuden vaatimukset.*	Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.	Ei vaatimuksia.	Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.	Organisaatiolla on toiminto, joka arvioi koulutuksen kohderyhmiä, annettavan koulutuksen sisältöä ja laatua.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 805.0 **Onko organisaatiolla menetelmä varmistaa, että työntekijöillä on tehtävien edellyttämä sopivuus, turvallisuuskoulutus, tehtävään perehtyminen ja kokemus?** *Kysymyksellä arvioidaan: Turvallisuuskoulutustason selvittämisen mahdollisuutta.*	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.	Turvallisuuskoulutusrekisteristä saadaan tieto, onko kyseiselle henkilölle annettu vaadittu koulutus.	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.		

Raportointi ja johdon katselmukset, osa-alue A900

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 901.0 **Raportoiko turvallisuudesta vastaava henkilö suoraan organisaation ylimmälle johdolle turvallisuuteen liittyvissä asioissa?** *Kysymyksellä arvioidaan: Johdon sitoutumista turvallisuustyöhön. Onko turvallisuusjohdolla suora nopea ja tehokas yhteyskanava organisaation johtoon.*	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.	Turvallisuudesta vastaava henkilö raportoi toimitusjohtajalle, varatoimitusjohtajalle, johtoryhmälle tai johtoryhmän jäsenelle.		
A 902.0 **Tarkastaako organisaation ylin johto säännöllisesti (vähintään kerran vuodessa) turvallisuusjärjestelmän toimivuuden?** *Kysymyksellä arvioidaan: Organisaation johdon sitoutumista turvallisuustyön jatkuvaan parantamiseen ja laadukkaaseen johtamiseen.*	Vähintään vuosittainen turvallisuusasioiden raportointi on järjestetty osaksi muuta johtamisprosessia.	Turvallisuusasioiden raportointi on järjestetty osaksi muuta johtamisprosessia.	Turvallisuusasiat esitetään osana organisaation johtamisprosessia laaja-alaisesti ainakin kerran vuodessa johtoryhmälle. Johtoryhmästä on nimetty henkilö, joka seuraa turvallisuuteen liittyviä asioita osana toimenkuvaansa.	Turvallisuusasiat esitetään osana organisaation johtamisprosessia laaja-alaisesti ainakin kerran vuodessa johtoryhmälle esimerkiksi johdon katselmuksessa. Johtoryhmästä on nimetty henkilö, joka seuraa turvallisuuteen liittyviä asioita osana toimenkuvaansa.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
A 903.0 **Arvioidaanko ylimmän johdon tekemissä tarkastuksissa turvallisuusjärjestelmän soveltuvuus, resurssien riittävyys ja toiminnan tehokkuus?** *Kysymyksellä arvioidaan: Raportoinnin laatu ja laaja-alaisuus.*	Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.	Ei vaatimuksia.	Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.	Organisaation turvallisuustyön tavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.		
A904.0 **Dokumentoidaanko tehdyt seurantatarkastukset?** *Kysymyksellä arvioidaan: Organisaation johdon systemaattista toimintaa ja mahdollisuutta tarkastella seurannan perusteella tehtyjen ratkaisujen vaikutusta ja tehokkuutta.*	Seurantatarkastukset dokumentoidaan.	Ei vaatimuksia.	Seurantatarkastukset dokumentoidaan.	Seurantatarkastukset dokumentoidaan turvallisuuden tietojenhallintajärjestelmään.		
A 905.0 **Toimivatko nämä seurantatarkastukset jatkuvan parannuksen perustekijöinä, eli vaikuttavatko ne politiikan ja tavoitteiden sisältöön?** *Kysymyksellä arvioidaan: Muodostaako turvallisuusjohtaminen laadukkaan toiminnan, jossa politiikka ja tavoitteet sekä turvallisuuden toimintamallit ovat jatkuvan parantamisen kohteina.*	Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon palautetta käytetään turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.	Ei vaatimuksia.	Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon katselmuksen palautetta käytetään turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.	Organisaation turvallisuustyön prosessi sisältää toiminnon, jossa johdon katselmuksessa esitetyt tulokset sekä niistä tehdyt johtopäätökset käytetään hyödyksi turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.		

OSA-ALUE

HENKILÖSTÖTURVALLISUUS

Johdanto

Soveltamisala

Osassa työnantajan tehtäviä henkilöstö joutuu käsittelemään viranomaisen salassa pidettäviä tietoja taikka työnantajan sellaista sensitiivistä tietoa (yritys- tai liike- ja ammattisalaisuuksia), joiden turvallisuusmääräysten vastainen käyttö saattaisi aiheuttaa vakavaa vahinkoa työnantajalle. Oheisen kriteeristön tarkoituksena on osaltaan parantaa mahdollisuuksia valita näihin tehtäviin parhaiten sopivat henkilöt. Kriteeristöä voidaan käyttää yritysten keskinäisissä ja viranomaisen kanssa tehtävissä turvallisuussopimuksissa.

Henkilöstöturvallisuuskriteeristö alkaa teknisellä osiolla, joka on sama kaikissa suojaustasoissa. Sen tarkoituksena on sensitiiviseen tai salassa pidettävään tietoon pääsevän henkilöstön hallinnointi.

Kriteeristö jatkuu suositus- ja vaatimustasoittain (IV-II) jaoteltuna vaatimusluettelona, jossa käsitellään tehtävään rekrytoitaessa taikka valittaessa huomioitavia seikkoja. Vaatimusluetteloa voidaan soveltaa uusrekrytointia tehtäessä, mutta myös soveltuvin osin valittaessa jo olemassa olevasta henkilöstöstä sopivia ammattilaisia turvallisuusluokiteltuun projektiin. Käytettäessä ulkopuolisia alihankkijoita, on sopimusneuvotteluvaiheessa hyvä tuoda esille, että sopimuskumppanin projektiin osallistuva henkilöstö tullaan mahdollisesta alistamaan turvallisuusselvitysmenettelyyn.

Yksityisyyden suoja

Liiteohjeistoa sovellettaessa on huomioitava laki yksityisyyden suojasta työelämässä. Erityisesti on muistettava, että työantaja saa käsitellä vain välittömästi työsuhteen kannalta merkittäviä tietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työsuhteen erityisluonteesta. Tällaisena työsuhteen erityisluonteena voidaan pitää mm. työsuhteen edellyttämää poikkeuksellisen luotettavuuden vaatimusta.

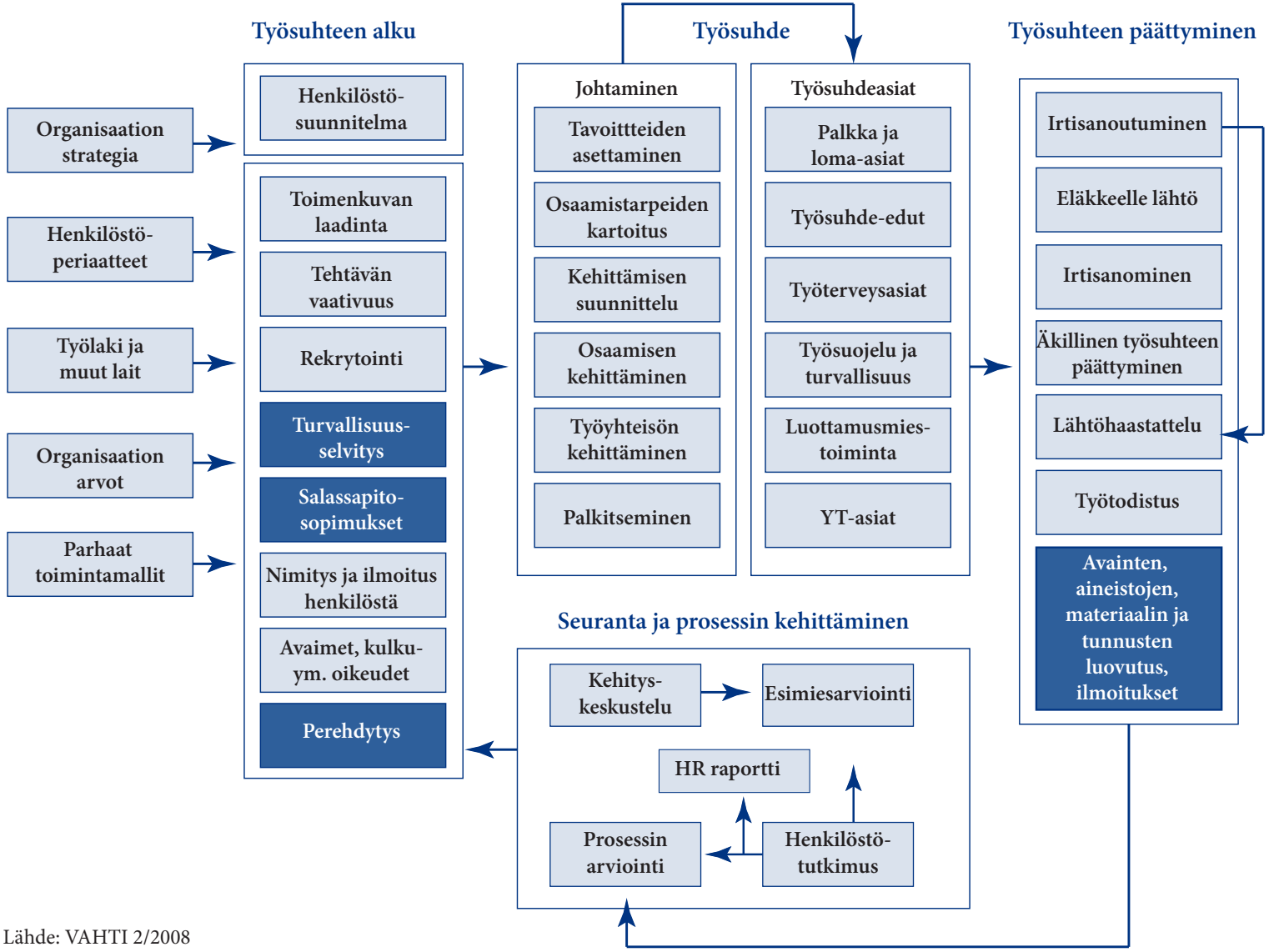
Työantajan on myös pääsääntöisesti kerättävä työntekijää koskevat henkilötiedot työntekijältä itseltään. Muussa tapauksessa työntekijältä on hankittava suostumus tietojen keräämiseen. Henkilöluottotietoja kerättäessä henkilön luotettavuuden selvittämiseksi ei tarvita suostumusta, mutta tällöinkin työntekijää on informoitava etukäteen tietojen hankkimisesta sekä käytettävistä tietolähteistä. Muualta kuin henkilöltä itseltään kerättävien tietojen käytöstä on informoitava työntekijää ennen päätösten tekemistä. Tältä osin työsuhteen pelisäännöt on syytä käsitellä yhteistoimintamenettelyssä.

Ohjeita ja neuvoja

Muilta osin hyvään ja turvalliseen henkilöstöprosessiin liittyen on saatavissa hyviä ohjeita ja neuvoja mm. valtionhallinnon tietoturvallisuuden johtoryhmän julkaisusta VAHTI 2/2008: ”Tärkein tekijä on ihminen–henkilöstöturvallisuus osana tietoturvallisuutta”. Ohessa em. julkaisun henkilöstöprosessikaavio.

Sisällys

Henkilöstöprosessi



Lähde: VAHTI 2/2008

Tekninen kriteeristö, osa-alue P100

Osa-alue on luonteeltaan tekninen kriteeristö. Sen tarkoituksena on sensitiiviseen tai salassa pidettävään tietoon pääsevän henkilöstön hallinnointi.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 101.0 **Onko hankkeeseen osallistuvista henkilöistä tehty luettelo?**	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.	Kuten perustasolla.	Kuten perustasolla.		
P 102.0 **Onko menettelytapaohje luotu ja pitävätkö yhteyshenkilön tiedot paikkansa?** *Lisäkysymys: Säilytetäänkö henkilöstöasiakirjat asianmukaisesti?*	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.	Kuten perustasolla.	Kuten perustasolla.		
P 103.0 **Onko koulutusdokumentaatio olemassa (merkinnät saadusta koulutuksesta)?**	Hankkeeseen osallistuvalle henkilöstölle on koulutettava hankkeen turvallisuuteen liittyvät asiat.	Hankkeeseen osallistuvalle henkilöstölle on koulutettava hankkeen turvallisuuteen liittyvät asiat.	Kuten perustasolla.	Kuten perustasolla.		

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 104.0 **Onko vierailijaluettelo olemassa ja pidetäänkö sitä yllä asianmukaisesti?** *Lisäkysymys: Ymmärtääkö isäntähenkilöstö vieraiden käsittelysäännöt?*	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.	Kuten perustasolla.	Kuten perustasolla.		
P 105.0 **Noudatetaanko vaatimuksia suojaustasojen tai turvallisuusluokituksen mukaisesti?**	Rekrytointimenettely-ohjeistusta sovelletaan.	Rekrytointimenettely-ohjeistusta sovelletaan.	Kuten perustasolla.	Kuten perustasolla.		

Riittävän osaamisen varmistaminen, osa-alue P200

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 201.0 **Onko työnhakijalta vaadittu keskeiset dokumentit jo olemassa olevan osaamisen varmistamiseksi?**	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Kuten perustasolla.	Kuten perustasolla.	Laki yksityisyyden suojasta työelämässä 4§	
P 202.0 **Miten työhaastattelussa saatujen tietojen oikeellisuus tarkastetaan?** *Perustelu: Harhaanjohtavien referenssien ja todistusten antaminen ei ole harvinaista.*	Tarkistetaan saatujen tietojen oikeellisuus.	Tarkistetaan saatujen tietojen oikeellisuus.	Kuten perustasolla.	Kuten perustasolla.		Auditoinnin jälkeen ohjataan tarvittaessa, miten toteutetaan käytännössä.
P 203.0 **Varmennetaanko haastattelutilanteessa työnhakijan osaamista asiantuntevilla kysymyksillä?**	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen	Kuten perustasolla.	Kuten perustasolla.		

Henkilön muu soveltuvuus tehtävään, osa-alue P300

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 301.0 **Varmennetaanko haastattelutilanteessa, että henkilö pystyy työssään toimimaan yrityksen arvojen mukaisesti?**	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Kuten perustasolla.	Kuten perustasolla.	Laki yksityisyyden suojasta työelämässä 3 §	Myös uuteen projektiin valittaessa. Voidaan kysyä esim. ymmärrystä kilpailunrajoitus- ja salassapitosopimuksista.
P 302.0 **Onko huumausainetestaus käytettävissä mikäli siihen katsotaan olevan tarvetta?**	Huumausainetestaus edellytetään tarvittaessa.	Huumausainetestaus edellytetään tarvittaessa.	Kuten perustasolla.	Kuten perustasolla.	Laki yksityisyyden suojasta työelämässä 6 §, 7 §, 8 §, 9 §, 14 § *Laki yhteistoiminnasta yrityksissä (334/2007) 19 § 2 kohta*	
P 303.0 **Varmennetaanko ammattilaisten tekemillä testeillä henkilön kykenevyys erityistä luotettavuutta vaativaan työhön?**	Henkilö- ja soveltuvuusarviointitesti.	Henkilö- ja soveltuvuusarviointitesti.	Kuten perustasolla.	Kuten perustasolla.	Laki yksityisyyden suojasta työelämässä 13 §	

Rekrytointipäätöksen jälkeiset toimet, osa-alue P400

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 401.0 **Käytetäänkö tähän tehtävään otettaessa salassapito- ja vaitiolositoumuksia ja jos, niin mikä niiden tarkka sisältö on?**	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Kuten perustasolla.	Kuten perustasolla.		Myös uuteen projektiin valittaessa.
P 402.0 **Käytetäänkö rekrytoitaessa koeaikaa ja jos, niin kuinka pitkää koeaikaa käytetään?**	Koeaikamenettely on käytössä.	Koeaikamenettely on käytössä.	Kuten perustasolla.	Kuten perustasolla.	TyösopimusL 1 luku 4 § 2 luku 4 §	
P 403.0 **Minkä tehtävien osalta katsotaan, että vastuuhenkilötiedot ja yrityskytkennät on syytä selvittää?** *Lisäkysymys:* *Miten tiedot selvitetään?*	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Kuten perustasolla.	Kuten perustasolla.	Henkilötietolaki 8 § 1 mom. 8 kohta	Henkilöltä itseltään ja käytettävissä olevista muista rekistereistä
P 404.0 **Haetaanko henkilöstä suppea turvallisuusselvitys, mikäli tämä on mahdollista?**	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Kuten perustasolla.	Kuten perustasolla.	Turvallisuusselvityslaki 19§	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 405.0 **Onko perusmuotoisen turvallisuusselvityksen hakumahdollisuus selvitetty tämän projektin tai tehtävän osalta?**	-	Ei vaatimuksia.	Haetaan perusmuotoinen turvallisuusselvitys tietojen suojaamiseksi mahdollisuuksien mukaan.	Haetaan perusmuotoinen turvallisuusselvitys tietojen suojaamiseksi mahdollisuuksien mukaan.		Myös uuteen projektiin valittaessa. Hakijana joko rekrytoija taikka turvallisuussopimuksen mukainen suojattavan edun omistaja.
P 406.0 **Haetaanko projektiin tai tehtävään valittavista henkilöistä luottotiedot?**			Hankitaan henkilöluottotiedot.	Hankitaan henkilöluottotiedot.	Laki yksityisyyden suojasta työelämässä *5 a §*	

Toimenpiteet työsuhteen solmimisen yhteydessä, osa-alue P500

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 501.0 **Miten varmistetaan, että työnhakija ja työnantaja ovat samaa mieltä työntekijän tehtävistä, vastuista, oikeuksista sekä velvollisuuksista etenkin tietojen suojaamisen osalta?**	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Kuten perustasolla.	Kuten perustasolla.		Myös uuteen projektiin valittaessa.
P 502.0 **Miten uusi työntekijä perehdytetään yhtiön turvallisuusmääräyksiin?** *Perustelu:* *Henkilökohtainen keskustelu turvallisuusasiantuntijan tms. kanssa yhtiön turvallisuusmääräyksistä ja niiden merkityksestä parantaa huomattavasti määräysten noudattamista.*	Turvallisuusperehdytys.	Turvallisuusperehdytys.	Kuten perustasolla.	Kuten perustasolla.		Myös uuteen projektiin valittaessa.
P 503.0 **Miten uusi työntekijä perehdytetään tehtäviinsä ja yrityksen toimintaan?**	Perehdytys toimintaan ja tehtäviin.	Perehdytys toimintaan ja tehtäviin.	Kuten perustasolla.	Kuten perustasolla.		Myös uuteen projektiin valittaessa.
P 504.0 **Miten tietoturvakoulutus on yrityksessä järjestetty?** *Lisäkysymys:* *Kuinka usein ja miten osaamista päivitetään?*	Koulutus tietoturva-asioihin, päivitys määräajoin.	Koulutus tietoturva-asioihin, päivitys määräajoin.	Kuten perustasolla.	Kuten perustasolla.		Myös uuteen projektiin alittaessa.
P 505.0 **Miten prosessikuvaukset on toteutettu valtuuttamisesta ja pääsyoikeuksien antamisesta tietoon ja tiloihin?**	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	Kuten perustasolla.	Kuten perustasolla.	VAHTI 2/2008	Myös uuteen projektiin valittaessa.

Toimenpiteet työsuhteen aikana, osa-alue P600

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 601.0 **Miten sijaisuusjärjestelyihin ja avainhenkilöihin liittyvät ohjeistukset (VAP-varaukset) on järjestetty?**	Ohjeisto on olemassa.	Ohjeisto on olemassa.	Ohjeisto on olemassa ja sitä ylläpidetään.	Ohjeisto on olemassa ja sitä ylläpidetään.		Pyydetään nähdä ko. ohjeistukset.
602.0 **Miten yrityksessä on huolehdittu työtyytyväisyyden ja työmotivaation ylläpitämisestä?** *Lisäkysymys: Kannustetaanko täydennyskoulutukseen osallistumista ja osaamisen kehittämistä?*	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta voidaan näyttää toteen dokumenttipohjaisesti.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta voidaan näyttää toteen dokumenttipohjaisesti.		Perustelu: Alhainen työtyytyväisyys ja työmotivaatio ovat merkittävä tehokkuutta huonontava tekijä sekä turvallisuusriski
P 603.0 **Miten työssä jaksamisen ja työkyvyn seuranta on järjestetty?**	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Mm. työterveyshuoltolaki 13 §	Perustelu: Työkyvyn seuranta on merkittävä turvallisuuskysymys luotettavuutta vaativissa tehtävissä.
P 604.0 **Miten toimitaan kun työntekijän toiminta muuttuu ilman havaittavaa syytä huolestuttavasti? Kenellä on toimintavastuu?**	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Kuten perustasolla.	Kuten perustasolla.		Perustelu: Alentunut työkyky esimerkiksi alkoholismista johtuen taikka väärinkäytöksiin syyllistyminen näkyvät monesti poikkeavana käyttäytymisenä.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
P 605.0 **Löytyykö organisaatiosta menettelyohje työsuhteen päättämisestä?**	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Kuten perustasolla.	Kuten perustasolla.		Perustelu: Oikean toimintatavan noudattaminen jouduttaessa päättämään työsuhde on tärkeä turvallisuuskysymys.
P 606.0 **Miten vierailukäytäntö on järjestetty?**	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Kuten perustasolla.	Kuten perustasolla.		Pyydetään nähdä vierailuja koskevat ohjeet.

OSA-ALUE

FYYSINEN TURVALLISUUS

Johdanto

Fyysisen turvallisuuden auditointikriteeristö keskittyy toimitilaturvallisuuteen, mutta huomioi tarvittavissa määrin myös muita fyysisen turvallisuuden elementtejä. Kriteeristöosion perusajatus on suojata sensitiivisen tai salassa pidettävän tiedon salassa pysyminen kuoriajatteluun pohjautuen siten, että pääsy edellä mainittuihin tietoihin estetään mahdollisimman varhaisessa vaiheessa ja tiukennetaan suojaamisvaatimuksia sitä mukaa, mitä lähemmäs fyysisesti tietoon päästään (ns. turvallisuusvyöhykemalli). Tärkeimpiä suojattavia kohteita ovat usein tietojärjestelmien kriittisiä osia sisältävät laitetilat. Näiden osalta on esitetty joitakin erityisvaatimuksia myös tämän kriteeristön tietoturvallisuusosiossa

Sisällys

Alueen turvallisuus, osa-alue F100

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 101.0 **Onko pysäköinnissä tarpeellista huomioida suojautuminen lähialueelta toteutettavalta elektroniselta tiedustelulta?**	Tiestölle ja pysäköinnille ei vaatimuksia.	Tiestölle ja pysäköinnille ei vaatimuksia.	Tiestölle ja pysäköinnille ei vaatimuksia.	Pysäköintialueen tulee sijaita riittävän kaukana tai se on suojattu siten, että sieltä ei voi suorittaa hajasäteilyyn perustuvaa tiedustelua. Pysäköintialueen tulee olla valvottu siten, että sinne ei voi viedä elektronisia tiedustelulaitteita. Pysäköintialue voi olla myös katveessa, jolloin suora elektroninen tiedustelu ei ole mahdollista.		Jos tilaa tai laitetta ei ole suojattu, tulee huolehtia siitä että pysäköintialueelta ei voida suorittaa ko. tiedustelua.
F 102.0 **Onko lastaus- ja purkualueella tarpeellista huomioida suojautuminen lähialueelta toteutettavalta elektroniselta tiedustelulta?**	Lastaus- ja purkualueille ei vaatimuksia.	Lastaus- ja purkualueille ei vaatimuksia.	Lastaus- ja purkualueille ei vaatimuksia.	Lastaus ja purkualue tulee sijaita riittävän kaukana tai se on suojattu siten, että sieltä ei voi suorittaa hajasäteilyyn perustuvaa tiedustelua. Lastaus ja purkualueen tulee olla valvottu siten, että sinne ei voi viedä elektronisia tiedustelulaitteita. Lastaus ja purkualue voi olla myös katveessa, jolloin suora elektroninen tiedustelu ei ole mahdollista.		Jos tilaa tai laitetta ei ole suojattu, tulee huolehtia siitä että lastaus- ja purkualueelta ei voida suorittaa ko. tiedustelua.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 103.0 **Onko tarpeellista rajoittaa kiinteistön alueella liikkumista aidoilla, porteilla ja ajoesteillä?**	Aidoille, porteille ja ajoesteille ei rakenteellisia vaatimuksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, tulee aidan täyttää seuraavat vähimmäisvaatimukset: -uusi aita: sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m, aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm), koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m, metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.	Aidoille, porteille ja ajoesteille ei rakenteellisia vaatimuksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, tulee aidan täyttää seuraavat vähimmäisvaatimukset: -uusi aita: sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m, aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm), koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m, metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.	Kuten perustaso.	Kuten perustaso.		Kaikki kiinteistön alueelle tulevat henkilöt ja ajoneuvot ovat kontrolloitu.
F 104.0 **Pystytäänkö videovalvonnalla seuraamaan alueella liikkumista?**	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityisvaatimuksia.	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityisvaatimuksia.	Kuten perustaso.	Kuten perustaso.		Videovalvonnalla on voitava yksilöidä riittävän tarkasti ajoneuvot ja henkilöt.

Rakenteellinen turvallisuus, osa-alue F200

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 201.0 **Mitä materiaalia tilan seinät, katto ja lattia ovat?**	Kuoren rakenne normaalia toimistorakennetta.	Kuoren rakenne normaalia toimistorakennetta.	Tilan seinät, katto ja lattia on oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet on vahvennettava. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta.			Rakenteiden tulee olla yhtä vahvat kuin ikkunat ja ovet.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 202.0 **Onko tilassa (tiloissa) alle 4 metrin korkeudessa ikkunoita?** **Korkean tason (II) kysymys: Onko tilassa (tiloissa) yli 4 metrin korkeudessa ikkunoita?**	Ikkunoiden on oltava suojattuja siten, että niitä ei saa rikkomatta ulkopuolelta auki.	Maatason (alle 4 m) ikkunat on suojattava turvakalvolla P1A (SFS - EN 356) tai sitä turvallisemmalla järjestelyllä. Ikkunat on varustettu näköestesuojalla, peitetty tai muuten estetty suora näkyvyys ko. turva-alueen ulkopuolelta.	Maatason (alle 4 m) ikkunat on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne.	Maatasossa (alle 4m) sijaitsevassa tilassa ei saa olla ikkunoita. Maatason yläpuolella (yli 4 m) ikkunat on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä, joka on murronkestävä, eikä välitä äänivärähtelyjä uloimpaa lasiin. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne. Jos tietoteknisiä laitteita ei ole Tempest-suojattu, voidaan tilan rakenteita muuttamalla saavuttaa vastaa suojaus. (Jos alue ei ole kulunvalvottu väh. 300metrin etäisyydeltä kohteesta tulee ikkunoiden ja tilan olla Tempest-suojattu)		Heikoista ikkuna-aukoista on helpompi murtautua kuin ovesta.
F 203.0 **Onko tilassa (tiloissa) kattoikkunoita?**	Kattoikkunat/luukut oltava lukitut ja ne on suojattava turvakalvolla P1A (SFS-EN 356) tai sitä turvallisemmalla järjestelyllä.	Kattoikkunat/luukut oltava lukitut ja ne on suojattava turvakalvolla P1A (SFS-EN 356) tai sitä turvallisemmalla järjestelyllä.	Kattoikkunat (tai kattotasanteiden tasolla olevat ikkunat) on suojattava turvalasilla (SFS-EN 356 / P6B),tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne.	Kattoikkunoita (tai kattotasanteita) ei saa olla II – tason tiloissa.		Heikoista ikkuna-aukoista on helpompi murtautua kuin ovesta.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 204.0 **Onko tilan kuoressa muita aukkoja, joita voitaisiin käyttää tunkeutumiseen?**	Tilan kuoressa ei saa olla muita kuin lukittuja aukkoja.		Tilan kuoressa ei saa olla muita aukkoja, kuin tunkeutumisen ilmaisujärjestelmillä valvottuja ovia, ikkunoita tai savunpoisto- ja ilmanottoaukkoja. Aukot voidaan sulkea kalteroinnilla tai vahvoilla terässäleiköillä.	Tilan kuoressa ei saa olla muita aukkoja, kuin tunkeutumisen ilmaisujärjestelmillä valvottuja ovia, ikkunoita tai savunpoisto- ja ilmanottoaukkoja. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä.		IV- ja kaapelikanavia, savunpoisto- ja ilmanottoaukkoja voidaan käyttää tunkeutumiseen.
F 205.0 **Minkälaiset ovat tilaan johtavat ovet?**	Normaalit ovet (ei vaatimuksia)	Ei vaatimuksia.	Ovien on täytettävä SFS EN 1627-luokka 3:n murronkestoluokan vaatimukset. Ovien rakenteita tarkastettaessa on lisäksi kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Karmirakenteen on estettävä kiinnitys ruuvien sahaamisen ulkoapäin. Välys oven ja karmin välillä max 2 mm. Oven läpinäkeminen suojattavaan tilaan tulee estää.	Ovien on täytettävä SFS EN 1627-luokka 3:n murronkestoluokan vaatimukset. Ovien rakenteita tarkastettaessa on lisäksi kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Karmirakenteen on estettävä kiinnitys ruuvien sahaamisen ulkoapäin. Välys oven ja karmin välillä max 2 mm. Oven läpinäkeminen suojattavaan tilaan tulee estää.		Ovien rungon, karmirakenteen ja karmien kiinnitykset seiniin tulee korkeammilla turvallisuustasoilla olla vahvat.
F 206.0 **Onko tilassa suuria, esim. halliovia?**	-	Ei vaatimuksia.	Mikäli ovia ei voida rakentaa em. periaatteella esimerkiksi niiden suuren koon takia, on kyseisen aukon teknilliseen suojaamiseen kiinnitettävä erityistä huomiota. Teräspuomien on estettävä ajoneuvon läpiajoa. Hyväksytyt rullakalterit toimivat murtosuojana.	Mikäli ovia ei voida rakentaa em. periaatteella esimerkiksi niiden suuren koon takia, on kyseisen aukon teknilliseen suojaamiseen kiinnitettävä erityistä huomiota. Teräspuomien on estettävä ajoneuvon läpiajoa. Hyväksytyt rullakalterit toimivat murtosuojana.		Nostettavat halliovet ovat usein murtosuojauksellisesti heikkoja.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 207.0 **Miten hyvin ääni liikkuu naapuritiloihin?**	-	Ei vaatimuksia.	Tilan äänieristyksen tulee olla sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta. Kaapelikouruihin äänieristemateriaalin lisääminen, ilmastointikanaviin ääniloukut.			Suojattavasta tilasta ei saa välittyä puhetta suojaamattomiin naapuritiloihin.
F 208.0 **Onko tilassa tiedon säilyttämistä varten kassakaappi tai holvi?**	Tilassa kassakaappi (vähintään Euro I SFS-EN 1143-1) tai jos luokiteltua tietoaineistoa säilytetään lukitussa kaapissa, tulee tila olla valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava.	Tilassa kassakaappi, tai jos suojaustason IV tietoaineistoa säilytetään lukitussa kaapissa, tulee tila olla valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava.	Tilassa kassakaappi (vähintään Euro II SFS-EN 1143-1) tai holvi (vähintään Euro IV).	Tilassa kassakaappi (vähintään Euro II SFS-EN 1143-1) tai holvi (vähintään Euro IV).		Tietoa tulee säilyttää lukitussa kaapissa tai holvissa pidemmän vasteajan mahdollistamiseksi.
F 209.0 **Miten pääsyoikeudet on hallinnoitu?**	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Kuten perustasolla.	Kuten perustasolla.		Tiloihin liittyvien pääsyoikeuksien tulee olla prosessissa yksiselitteisesti vastuutettu.
F 210.0 **Minkälainen tilan lukitus on?**	Suojatun tilan lukituksen on oltava kunnossa. Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3.	Suojatun tilan lukituksen on oltava kunnossa. Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3.	Suojatun tilan lukituksen on oltava kunnossa. Tila on lukittava aina. Käyttölukko vyöhykkeen rajalla FK:n varmuus-luokka 3. Tämän lisäksi vyöhykkeen rajalla varmuuslukko, varmuusluokka 4. Vyöhykkeen sisällä käyttölukko, FK:n varmuusluokka 3.	Suojatun tilan lukituksen on oltava kunnossa. Tila on lukittava aina. Käyttölukko vyöhykkeen rajalla FK:n varmuus-luokka 3. Tämän lisäksi vyöhykkeen rajalla varmuuslukko, varmuusluokka 4. Vyöhykkeen sisällä käyttölukko, FK:n varmuusluokka 3.		Lukot on luokiteltu eri tasoihin murtosuojan perusteella.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 211.0 **Miten (mekaanisten) avainten hallinta on järjestetty?**	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Kuten perustasolla.	Kuten perustasolla.		Tilan hallinnan vuoksi on tarkastettava myös ylimääräisten avainten säilytys, sekä lisä-avainten hallittu teettäminen.
F 212.0 **Kenellä suojattavaan tilaan on avaimia?**	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Kuten perustasolla.	Kuten perustasolla.		Tilan hallinnan vuoksi on aina tiedettävä kenellä avaimia suojattavaan tilaan on.
F 213.0 **Mihin tiloihin yleisavaimella pääsee?**	-	Ei vaatimuksia.	Suojaustason III tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. III – tason yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos sidosryhmän tiloista on kielletty.	Suojaustason II tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. II – tason yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos sidosryhmän tiloista on kielletty.		Yleisavaimella ei pääse suojattuun tilaan.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 214.0 **Onko vartiointi- ja kiinteistönhoitohenkilöstölle jaettu avaimia suojattuun tilaan?**	-	Ei vaatimuksia.	Vartiointi- ja kiinteistönhoitohenkilöstölle jaettavat avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten.	Vartiointi- ja kiinteistönhoitohenkilöstölle jaettavat avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten. Hälytystilanteissa II –tason tilaan edellytetään saapuvan kaksi henkilöä samanaikaisesti.		Vartiointi- ja kiinteistönhoitohenkilöstöllä ei saa olla hallitsematonta pääsyä suojattavaan tilaan.
F 215.0 **Miten tilan huoltotoimenpiteet on ohjeistettu tapahtuvaksi?**	-	Ei vaatimuksia.	Ei vaatimuksia.	Tilaan liittyvät huoltotoimenpiteet on toteutettava hankkeeseen hyväksytyn henkilön valvonnassa. II -tasoon kuuluvan tietoaineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.		Vaikka tieto on suojattu, voi ulkopuolinen henkilöstö saada tietoonsa tilaan liittyviä suojaamistoimenpiteitä, sekä tuoda tilaan kuulumattomia laitteita.

Turvallisuustekniset järjestelmät, osa-alue F300

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 301.0 **Onko tilassa rikosilmoitinjärjestelmä?**	Tila on valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava. Tarvitaan, jos suojaustason IV luokiteltua aineistoa säilytetään lukitussa kaapissa.	Tila on valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava. Tarvitaan, jos suojaustason IV luokiteltua aineistoa säilytetään lukitussa kaapissa.	Tilassa rikosilmoitinjärjestelmä (vähintään 3-luokka). Ovet, aukot, ikkunat ja tilat valvottava.	Tilassa rikosilmoitinjärjestelmä (vähintään 3-luokka). Ovet, aukot, ikkunat, tilat ja kuori valvottava. Vahvistettuun seinärakenteeseen lisätään joko runkoääni- tai inertia-ilmaisimet.		Rikosilmoitinjärjestelmä antaa ilmaisun ja käynnistää vastatoimenpiteet.
F 302.0 **Onko tilassa kulunvalvontajärjestelmää?**		Ei vaatimuksia.	Tila on valvottava kulunvalvonnalla siten, että vain ne henkilöt, jotka ovat hyväksyttyjä hankkeeseen, ovat oikeutettuja pääsemään tilaan, ja että tilaan kulku voidaan myöhemmin todentaa.	Tila on valvottava kulunvalvonnalla siten, että vain ne henkilöt, jotka ovat hyväksyttyjä hankkeeseen, ovat oikeutettuja pääsemään tilaan, ja että tilaan kulku voidaan myöhemmin todentaa jokaisen henkilön osalta. Kulunvalvonnassa on käytettävä sisään mentäessä kaksoistunnistusta. Poistuttaessa tilasta tulee käyttää kulunvalvontatunnistetta.		Suojattuun tilaan kulku voidaan myöhemmin todentaa. Lisäkommentti tasolla II: Kaksois-tunnistuksella estetään toisen henkilön tunnisteen luvaton käyttö.
F 303.0 **Onko tilassa kameravalvontajärjestelmä?**		Ei vaatimuksia.	Ei vaatimusta kameravalvonnasta. Voidaan käyttää kehävalvonnassa heikkojen halli-ovien täydentäjänä.	II –tason tila on varustettava kameravalvonnalla. Kamerat on sijoitettava siten, että II –tason tietoa ei siirry kameran välityksellä. Kameravalvontatieto on tallennettava ja liitettävä rikosilmaisinjärjestelmään.		Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan. Tämä perustelu vain tasolla II, ilman edellistä: Rikosilmoitinjärjestelmän antamasta hälytyksestä saadaan liipaisu tallentimelle jolloin saadaan tunkeutujasta myös tunnistuskuvaa.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
F 304.0 **Onko palvelintilassa kameravalvontajärjestelmä?**		Ei vaatimuksia.	Ei vaatimuksia.	Laite- ja palvelintilat on varustettava jatkuvalla kameravalvonnalla.		Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan.
F 305.0 **Onko rikosilmoitinjärjestelmä toimintakunnossa?**		Ei vaatimuksia.	Rikosilmoitinjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä ja vasteajan testaus tulee tehdä kerran vuodessa. Testaukset tulee dokumentoida.	Rikosilmoitinjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä ja vasteajan testaus tulee tehdä kerran vuodessa. Testaukset tulee dokumentoida.		Toimimattomasta rikosilmoitinjärjestelmästä ei ole hyötyä. Vastaako vartioinnin vasteaika ja vartijan toiminta sopimusta? Liian pitkä vaste-aika tai vartijan virheellinen toiminta poistaa rakenteellisella suojauksella saavutettua turvaa.
F 306.0 **Miten kulunvalvontajärjestelmän hallinnointi on järjestetty?**		Ei vaatimuksia.	Ei vaatimuksia.	Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu. Normaalin käyttäjän työasemalta tapahtuva oven avaus turvatilaan pitää olla estetty.		Kulunvalvontajärjestelmän hallinnoija voi luoda tai poistaa turvatilan kulkutunnisteita sekä ohjata ovia etäkäyttöisesti.
F 307. **Miten rikosilmoitinjärjestelmän hallinnointi on järjestetty?**		Ei vaatimuksia.	Ei vaatimuksia.	Rikosilmoitinjärjestelmän hallinta tulee olla yrityksen omassa hallinnassa.		Rikosilmoitinjärjestelmän hallinnoija voi luoda tai poistaa turvatilan ohjaustunnisteita sekä etäkäyttöisesti ilmaisimia.
F 308.0 **Miten LVI-automaation hallinta on järjestetty?**		Ei vaatimuksia.	Ei vaatimuksia.	Jos turvatilassa on palvelimia tai muita olosuhteelle herkkiä laitteita ei tilan LVI-järjestelmää saa ohjata etäkäyttöisesti.		LVI-automaation etähallinnan avulla voidaan tilan olosuhdemuutoksilla vahingoittaa laitteita ja tietoa.

OSA-ALUE

TIETOTURVALLISUUS

Johdanto

Kansallisen turvallisuusauditointikriteeristön tietoturvaosio kuvaa tietoturvallisuuden vähimmäisvaatimukset sellaisille tiedoille, joiden luottamuksellisuutta, eheyttä ja käytettävyyttä tulee suojata. Tällaisia tietoja ovat esimerkiksi yrityksen sensitiiviset tiedot (esim. tuotekehitykseen liittyvät yrityssalaisuudet) sekä viranomaisten suojattavat tai turvaluokitellut tiedot. Tietoturvakriteeristö on luotu osana Sisäisen turvallisuuden ohjelman turvallisuusauditoitikriteeristötyötä siten, että tietoturvakriteeristöön on sisällytetty eräitä tietoturvallisuudelle välttämättömiä vaatimuksia tämän kokonaiskriteeristön muista osioista. Silti esimerkiksi fyysisen turvallisuuden kriteeristö on looginen osa tietoturvakriteeristöä, jossa viitataankin fyysisen turvallisuuden kriteeristöön monissa tiedon fyysiseen suojaamiseen liittyvissä vaatimuksissa. Tietoturvakriteeristötyössä on otettu mahdollisimman tarkasti huomioon samanaikaisesti tekeillä olleen valtionhallinnon tietoturvallisuusasetuksen ja tätä täydentävien ohjeiden yksityiskohtaiset linjaukset. Samoin on pyritty yhteismitallisuuteen valtiovarainministeriön johdolla toteutetun tietoturvallisuutta ja varautumista ohjeistavan aineiston suhteen.
Tietoturvakriteeristö on jaettu seitsemään sisällysluettelossa esiintyvään osa-alueeseen. Osa-alueet on jaettu neljään tasoon. Tasoja ovat lähtötason suositukset, perustason vaatimukset (IV), korotetun tason vaatimukset (III) ja korkean tason vaatimukset (II). Alin taso, lähtötason suositukset, koskee koko organisaation kohteiden turvaamista sekä tietoturvallisuuden kokonaishallintaa. Suositustason pohjalta on hyvä edetä vaatimusten täyttämiseen. Tasojen IV-II vaatimukset koskevat vain suojattavaa kohdetta. Suojattavalla kohteella tarkoitetaan suojattavaa tietoa sekä sen käsittely-ympäristöä. Suojattava kohde voi olla esimerkiksi yksittäinen tietojärjestelmä, verkon osa tai vaikka yksittäinen työhuone. Vaatimukset periytyvät ylemmille tasoille siten, että esimerkiksi II-tasolla edellytetään omien erillisvaatimusten lisäksi tasojen IV-III vaatimusten täyttyminen.
Viranomaisten suojattavien tai turvaluokiteltujen tietojen käsittely edellyttää organisaatiolta vastaavan vaatimustason täyttämistä. Täyttämällä vaatimustason organisaatiolla tai sen osalla on tietoturvallisuuden osalta valmiudet suojaustasoa vastaavien tietojen tietotekniseen käsittelyyn edellyttäen, että tämän auditointikriteeristön muiden osioiden asettamat vaatimukset täyttyvät. Tietoturvakriteeristön vaatimustasoja määritettäessä on pyritty huomioimaan kansainvälisiä vaatimuksia kuitenkin siten, että suomalainen säädöspohja on viime kädessä määräävä tekijä.

Sisällys

Hallinnollinen tietoturvallisuus, osa-alue I100

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 101.0 **Onko organisaation tietoturvallisuudella johdon tuki?**	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu tarvittavat resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu tarvittavat resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu tarvittavat resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu tarvittavat resurssit.	ISO/IEC 27002 5.1.1, ISO/IEC 27002 5.1.2, ISO/IEC 27002 6.1.1, ISO/IEC 27002 6.1.3, ISO/IEC 27002 7.1, ISO/IEC 27002 8.2.1, PCI DSS 12.1, PCI DSS 12.3.1, PCI DSS 12.4, PCI DSS 12.5	Suositellaan, että järjestelmille on määritetty ylläpitovastuun lisäksi myös omistajat. Suositellaan, että tekninen ylläpito ei ole sama kuin omistaja.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 102.0 **Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?**	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	Kuten perustasolla.	Kuten perustasolla.	PCI DSS 12.2	Todennetaan tarkistamalla suunnitelman ja ohjeiden olemassaolo.
I 103.0 **Pääkysymys:** **Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät) tunnistettu?** *Lisäkysymykset:* *Mitä uhkia niihin kohdistuu?* *Onko suojattaville kohteille määritetty vastuuhenkilöt?*	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. I 104.0).	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. I 104.0).	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 7.1, VAHTI 8/2006, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf	1) Suojattavien kohteiden tunnistaminen voidaan todentaa esimerkiksi siten, että täytetään liitteen 1 lomake. 2) Vastaavasti uhat esimerkiksi siten, että pyydetään listaamaan tunnistetut uhat per suojattava kohde. 3) Voidaan todentaa pyytämällä listaus suojattavista kohteista ja niiden vastuuhenkilöistä. 4) Erityisesti on varmistettava, että organisaatiolle kriittisten järjestelmien suojaukset ovat riittäviä.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 104.0 **Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?**	1) Suojattaviin kohteisiin (vrt. I 103.0) kohdistuvia riskejä arvioidaan jollain järjestelmällisellä menetelmällä. 2) Arviointi tapahtuu vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 3) Valitut suojausmenetelmät on asianmukaisesti suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin. 4) Johto on hyväksynyt valitut suojausmenetelmät ja jäännösriskit	1) Salassa pidettäviin tietoihin kohdistuvia riskejä hallitaan prosessina. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvallisuusriskien hallinta on erottamaton osa viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa	1) Salassa pidettäviin tietoihin kohdistuvia riskejä hallitaan prosessina. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan säännöllisesti. 4) Turvallisuusriskien hallinta on erottamaton osa viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa.	1) Salassa pidettäviin tietoihin kohdistuvia riskejä hallitaan prosessina. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan säännöllisesti. 4) Turvallisuusriskien hallinta on erottamaton osa viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa.	ISO/IEC 27001 luku 4, ISO/IEC 27002 7.1, VAHTI 8/2006, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf,http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/03_TTT-kaesikirja-Liite1-org-kypsyys-20081030.pdf, 2009/xxx/EC:n 5. artiklan kohta 1	Suositustaso: 1 & 2) Voidaan todentaa esimerkiksi kuvailemalla käytetty menetelmä ja näyttämällä menetelmän tuottamat päivätyt ”tulosraportit”. Esimerkkejä: http://www.pk-rh.fi/. 3 & 4) Erityisesti varmistettava, että organisaatiolle kriittisten järjestelmien suojaukset ovat riittäviä.
I 105.0 **Pääkysymys:** **Miten organisaation tietoturvallisuutta arvioidaan?** *Lisäkysymys:* *Kehitetäänkö toimintaa havaintojen perusteella?*	Tietoturvallisuuden tasoa seurataan säännöllisesti.	1) Tietoturvallisuuden tasoa arvioidaan ja kehitetään jatkuvasti.	1) Tietoturvallisuuden tasoa arvioidaan ja kehitetään jatkuvasti. 2) Organisaatiolla on käytössään järjestelmällinen menetelmä tietoturvallisuuden arviointiin ja mittaamiseen. 3) Organisaation tietoturvallisuuden toimintamallille ja sen toteuttamiselle suoritetaan riippumaton katselmus suunnitelluin väliajoin, tai kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.	1) Tietoturvallisuuden tasoa arvioidaan ja kehitetään jatkuvasti. 2) Organisaatiolla on käytössään järjestelmällinen menetelmä tietoturvallisuuden arviointiin ja mittaamiseen. 3) Organisaation tietoturvallisuuden toimintamallille ja sen toteuttamiselle suoritetaan riippumaton katselmus suunnitelluin väliajoin, tai kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.	ISO/IEC 27002 6.1.8, VAHTI 8/2006	III-tasolla: 1) Voidaan todentaa pyytämällä esimerkkejä siitä, miten tietoturvallisuutta on arvioitu ja kehitetty. 2) Voidaan todentaa pyytämällä kuvaamaan käytetty järjestelmällinen menetelmä ja näyttämään sen antamia tuloksia. 3) Voidaan pyytää nähtäväksi ulkopuolisen auditoijan tuottama raportti.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 106.0 **Onko tietoturvallisuudesta huolehdittu alihankinta-, palveluhankinta- ja muissa vastaavissa yhteistyökuvioissa?**	Tarjouspyyntöihin on liitetty tietoturvavaatimukset.	1) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 2) Palveluihin on määritelty palvelun laatutaso (SLA). 3) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovittu menettelytavat tietoturvapoikkeamien varalle. 4) Turvaluokiteltua aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.	1) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 2) Organisaation sensitiivistä tietoa käsitteleviin palveluihin on varattu oikeus tietoturvatarkastuksiin. 3) Tunnistetuista turvallisuusvaatimuksista huolehditaan ennen kuin asiakkaille annetaan pääsy organisaation tietoon tai suojattaviin kohteisiin. 4) Palveluihin on määritelty palvelun laatutaso (SLA). 5) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovittu menettelytavat tietoturvapoikkeamien varalle. 6) Turvaluokiteltua aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.	1) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 2) Organisaation sensitiivistä tietoa käsitteleviin palveluihin on varattu oikeus tietoturvatarkastuksiin. 3) Tunnistetuista turvallisuusvaatimuksista huolehditaan ennen kuin asiakkaille annetaan pääsy organisaation tietoon tai suojattaviin kohteisiin. 4) Palveluihin on määritelty palvelun laatutaso (SLA). 5) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovittu menettelytavat tietoturvapoikkeamien varalle. 6) Turvaluokiteltua aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.	ISO/IEC 27002 6.2.1, ISO/IEC 27002 6.2.2, ISO/IEC 27002 10.6.1, ISO/IEC 27002 12.1.1, VAHTI 8/2006, 2009/xxx/EC:n 11. artikla, 2009/xxx/EC:n liitteen V kohta 22	Huolehdittava myös salassapitositoumukset /vaitiolovakuutukset (I 204.0). Alihankkijoilta ja vastaavilta voidaan tapauskohtaisesti vaatia myös säännölliset raportit tietoturvallisuuden nykytilasta (esim. kuukauden havainnot, hyökkäysyritykset, poikkeukset, jne.).

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 107.0 **Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?**	Tietoturvapoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu/koulutettu, ja erityisesti 3) viestintäkäytännöt ja -vastuut on sovittu.	Tietoturvapoikkeamien hallinta on edellisen lisäksi dokumentoitu.	Tietoturvapoikkeamien hallinta on edellisten lisäksi harjoiteltu. Tapahtuneesta tai epäillystä tietoturvapoikkeamasta ilmoitetaan välittömästi turvallisuusviranomaiselle (tai CERT-FI). Tietoturvapoikkeamat tutkitaan viranomaistoimenpitein.	Tietoturvapoikkeamien hallinta on edellisten lisäksi harjoiteltu. Tapahtuneesta tai epäillystä tietoturvapoikkeamasta ilmoitetaan välittömästi turvallisuusviranomaiselle (tai CERT-FI). Tietoturvapoikkeamat tutkitaan viranomaistoimenpitein.	ISO/IEC 27002 13.2.1, PCI DSS 12.9, 2009/xxx/EC:n 13. artiklan kohta 3	Vrt. I 409.0.
I 108.0 **Pääkysymys:** **Onko toiminnan lakisääteiset vaatimukset huomioitu?** *Lisäkysymys:* *Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?*	Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty.	1) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 2) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 15.1, VAHTI 8/2006, http://www.finlex.fi/fi/laki/ajantasa/1999/19990523, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/pdf/ Tietoturvakartoituskysymyslista.pdf, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/Tietoaineistojen Turvallinen-Kasittely_v14.pdf, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/03_TTT-kaesikirja-Liite1-org-kypsyys-20081030.pdf, http://www.tietosuoja.fi/tulostus/5940.htm	Käytännössä kaikkia organisaatioita koskee ainakin henkilötietolain (523/1999) 6 § ja sen asettamat vaatimukset henkilötietojen käsittelyn tarkoituksesta, henkilörekistereistä ja tietojen suojaamista koko tiedon elinkaaren ajalta sen kaikissa olomuodoissa.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 109.0 **Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?**	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely	Ei auditointivaatimuksia.	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.	ISO/IEC 27002 Luku 12 ja 10.1.2, PCI DSS 6.4	Vaatimuksen voi toteuttaa esimerkiksi siten, että merkittävimpien muutosten prosessiin kuuluu muutosten tunnistaminen ja kirjaaminen, muutosten suunnittelu ja testaus, muutosten mahdollisten vaikutusten arviointi mukaan lukien turvallisuusvaikutukset ja ehdotettujen muutosten virallinen hyväksymisprosessi. Todentaminen esimerkiksi vertaamalla organisaation tietoturvaperiaatteita, -politiikkoja ja -ohjeita käytännön toteutukseen.

Henkilöstöturvallisuus osana tietoturvallisuutta, osa-alue I200

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 201.0 **Hallitaanko kaikkien käyttäjien pääsy- ja käyttöoikeuksia hyvän tiedonhallintatavan mukaisesti?**	1) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 2) On olemassa selkeä ja toimiva tapa muutosten ilmoittamiseen ja tarvittavien muutosten tekemisiin. 3) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen (kulunvalvonta jne) että loogiseen pääsyyn ja käyttöön. 4) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 5) Käyttöoikeuksien käsittely ja myöntäminen ohjeistettu. 6) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen). 2) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 3) Järjestelmän käyttäjätyypit on dokumentoitu. 4) Järjestelmän käyttäjistä on olemassa lista. 5) On olemassa menettelyohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi asiaankuuluville tahoille. 6) Yhteistyökumppaneiden/muiden ulkopuolisten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä.	Perustason vaatimusten lisäksi seuraavat vaatimukset: 1) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin. 2) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 3) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen (kulunvalvonta jne) että loogiseen pääsyyn ja käyttöön.	Perustason vaatimusten lisäksi seuraavat vaatimukset: 1) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin. 2) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 3) Muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön.	ISO/IEC 27002 11.1, ISO/IEC 27002 11.1.1, ISO/IEC 27002 11.2.4, ISO/IEC 27002 11.4.1, ISO/IEC 27002 11.6.1, ISO/IEC 27002 8.3.3, VAHTI 4/2002, VAHTI 8/2006	Voidaan käytännössä toteuttaa esimerkiksi siten, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työnkierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä sopivina. Tämä voi tarkoittaa käytännössä esimerkiksi sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 202.0 **Onko salassapito- tai vaitiolositoumukset laadittu ja otettu käyttöön siten, että ne vastaavat organisaation tietojen suojaamistarpeita?**	Salassapito- tai vaitiolositoumukset vastaavat organisaation tietojen suojaamistarpeita.	Kaikki työntekijät, toimittajat, kumppanit, alihankkijat ja ulkopuoliset käyttäjät allekirjoittavat salassapito- tai vaitiolositoumuksen ennen pääsyoikeuden saamista luottamukselliseen tietoon.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 6.1.5, ISO/IEC 27002 8.1.3	Koko salassapitoketju tulee olla tuettu salassapitosopimuksin. Ts. kun organisaatio tekee sopimuksen salassapidosta alihankkija-/kumppaniyrityksen kanssa ja alihankkija/kumppani oman työntekijänsä kanssa, tavoitteena on henkilökohtainen vastuu (työntekijä) ja korvausvelvollisuus (alihankkija/kumppani).
I 203.0 **Pääkysymys:** **Onko avainhenkilöt sekä organisaation riippuvuus heistä tunnistettu?** *Lisäkysymys:* *Onko heidän varalleen suunniteltu varahenkilöt tai -menettelyt?*	Organisaation avainhenkilöt on tunnistettu ja varahenkilöjärjestelmä on perustettu.	1) Avaintehtävät on tunnistettu ja niihin on nimetty varahenkilö tai –henkilöt 2) Kriittisissä tehtävissä vastuulliset avainhenkilöt on koulutettu toimimaan häiriötilanteissa (TTT:3.2.4, JHTT: 3D).	Edellisen lisäksi: 1) Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön varajärjestelyt. 2) Avainhenkilöstö harjoittelee säännöllisesti ylläpitämään kriittisiä toimintoja erityistilanteissa.	Edellisten lisäksi: Kriittisten tehtävien toteuttamisen edellyttämät varajärjestelyt poikkeusoloissa on testattu ja harjoiteltu.	TTT: 3.2.2, 3.2.4. JHTT: 3D VAHTI 5/2004 VAHTI 3/2007 ISO/IEC 27002	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 204.0 **Onko organisaatiossa huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?**	Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. Henkilöstö on saanut perehdytyksen yhteydessä ohjeet, kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Salassa pidettäviä tietoja käsitteleviin järjestelmiin on laadittu turvallisen käytön ohjeistus. 2) Tiedon merkitsemistä (luokittelua), käsittelyä (sis. salaus) ja tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön. 3) Henkilöstö on perehdytetty henkilötietojen käsittelyyn ja siihen liittyviin vastuisiin (mm. salassapito- ja vaitiolovelvollisuuteen) (vrt. I 108.0). 4) Henkilöstö on ohjeistettu ja velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja -uhista. 5) Tulevista työasemien tietoturva-aukkojen päivityksistä tiedotetaan vähintään sillä tarkkuudella, että käyttäjät ovat tietoisia siitä, mitä toimia heiltä vaaditaan. Käyttäjille tiedotetaan merkittävimmistä ajankohtaisista uhista, jotka kohdistuvat organisaation käyttäjiin (esim. kohdistetuista hyökkäyksistä)	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 10.7.3, ISO/IEC 27002 13.1.1, ISO/IEC 27002 7.2.2, ISO/IEC 27002 8.2.2, PCI DSS 12.6, VAHTI 8/2006, 2009/xxx/EC:n liitteen I kohta 31	Voidaan todentaa esim. siten, että kysytään auditoitaessa satunnaisesti valituilta käyttäjiltä, miten heidät on ohjeistettu toimimaan.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 205.0 **Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle?**	1) Hyväksyttävän käytön säännöt on määritetty. 2) Dokumentoidut säännöt ovat henkilöstölle helposti saatavilla.	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty ja dokumentoitu. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 7.1.3, PCI DSS 12.3, VAHTI 8/2006	Voidaan todentaa tarkistamalla AUP:n (acceptable use policy) olemassaolo ja sisältö, lisäksi se, onko AUP helposti saatavilla henkilöstölle. Selvitetään lisäksi miten AUP:sta tiedotettu henkilöstölle.
I 206.0 **Valvotaanko organisaatiossa tietoturvaohjeiden noudattamista ja onko tietoturvarikkomusten käsittely ja seuraukset määritelty?**	Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan.	1) Tietoturvarikkomusten käsittely ja seuraukset määritelty. 2) Käsittely ja seuraukset samat koko henkilöstölle.	1) Tietoturvarikkomusten käsittely ja seuraukset määritelty. 2) Käsittely ja seuraukset samat koko henkilöstölle. 3) Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.	1) Tietoturvarikkomusten käsittely ja seuraukset määritelty. 2) Käsittely ja seuraukset samat koko henkilöstölle. 3) Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.	ISO/IEC 27002 8.2.3, VAHTI 8/2006, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf	Voidaan todentaa selvittämällä a. miten valvonta käytännössä toteutetaan, b. millaisia rikkeitä on tullut viime vuosina esille, ja c. miten rikkeisiin on puututtu.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 207.0 **Pääkysymys:** **Millaisia menettelytapoja organisaatiolla on tunnistaa ulkopuoliset työntekijät sekä vierailijat?** *Lisäkysymys:* *Onko henkilöstö ohjeistettu vieraiden isännöintiä varten?*	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Vieraat eivät koskaan jää valvomatta tiloihin ilman isäntää tai hänen edustajaansa. 2) Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. 3) Kaikki urakoitsijat, ulkopuoliset käyttäjät, huoltohenkilökunta sekä vierailijat käyttävät jonkinlaista näkyvää tunnistetta (esim. henkilökortti/vierailijakortti). 4) Henkilökunta on ohjeistettu reagoimaan ilman henkilökorttia (tai vastaavaa muuta näkyvää tunnistetta) liikkuviin henkilöihin.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 9.1.2, PCI DSS 9.2, PCI DSS 9.3, VAHTI 8/2006	Näkyvät tunnisteet eivät tarpeen jos organisaatiossa työskentelee vain muutama henkilö, jotka varmasti tuntevat toisensa ja toistensa työsuhteiden keston. Vieraat voivat jäädä valvomatta julkisiin tiloihin.

Fyysinen turvallisuus osana tietoturvallisuutta, osa-alue I300

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 301.0 **Pääkysymys:** **Miten suojattavaa tietoa sisältävän tilan fyysisestä turvallisuudesta on huolehdittu?** *Lisäkysymys:* *Miten kulunvalvonta on järjestetty?*	Toimistojen, tilojen ja laitteistojen fyysinen turvallisuus on suunniteltu ja toteutettu riskiarvion mukaisilla menetelmillä. Suojattavat tiedot, niitä käsittelevät laitteistot, oheislaitteet ja tietovälineet on sijoitettu ja suojattu niin, että niihin ei ole pääsyä ulkopuolisilla.	Ks. fyysisen turvallisuuden auditointikriteeristö.	Ks. fyysisen turvallisuuden auditointikriteeristö.	Ks. fyysisen turvallisuuden auditointikriteeristö.	ISO/IEC 27002 9.1.2, ISO/IEC 27002 9.1.3, ISO/IEC 27002 9.2.1, VAHTI 8/2006	
I 302.0 **Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuina?**	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat riskienarvioinnin mukaisesti. Riskienarvioinnissa voidaan päätyä hyväksymään toimet esim. vain oman henkilöstön valvomana, sähköisellä tallentavalla kulunvalvonnalla (esim. sähköinen kulkuavain ja koodi) järjestettynä, ja/tai sopimuksin suojattuna.	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain turvatasolle hyväksytyn henkilön valvonnassa.	Perustason vaatimusten lisäksi seuraavat vaatimukset: Suojaustasoon III kuuluvan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Perustason vaatimusten lisäksi seuraavat vaatimukset: Suojaustasoon II kuuluvan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	VAHTI 8/2006	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I303.0 **Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?**	Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan salassa pidettävistä asioista. Henkilöstölle on muistutettava, että taukopaikoilla (tupakkakopit jne.) ei saa keskustella salassa pidettävistä asioista.	Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan luokitelluista asioista. Huoneen ovet ja ikkunat on pidettävä kiinni keskusteltaessa em. asioista.	1) Tilassa ei käytetä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet jne.) joiden käyttö on erikseen kielletty. 2) Tapauskohtaisesti arvioidaan tarve järjestelmien suojaamiseksi lähtevältä hajasäteilyltä (TEMPEST). 3) Tilan äänieristys on sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta.	1) Tilaan ei saa viedä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet jne.) jotka eivät ole tilaan erikseen hyväksyttyjä. 2) Tapauskohtaisesti arvioidaan tarve viranomaisen tekemälle tarkastukselle salakuunte-lulaitteiden (ja vastaavien) varalta. 3) Tapauskohtaisesti arvioidaan tarve TEMPEST- tai EMP/HMP-suojaukselle.	VAHTI 8/2006, 2009/xxx/EC:n 10. artiklan kohta 5	Elektronisten laitteiden tilaanvientikielto voidaan joissain tilanteissa erikseen sallia esim. irrottamalla akut. Lähtevältä hajasäteilyltä suojautuminen on hoidettava toimitilan fyysisen sijainnin valinnalla, vuorauksella tai käyttämällä suojattuja laitteistoja ja kaapelointeja (TEMPEST). Vrt. fyysisen turvallisuuden kriteeristön vaatimukset.
I 304.0 **Pääkysymys:** **Onko LVIS-järjestelyt varmistettu niin, että ne vastaavat organisaation toiminta-vaatimuksia?** *Lisäkysymys:* *vatko organisaation kriittiset laitteistot häiriöttömän sähkönsyötön (UPS) piirissä?*	1) Kriittiset laitteistot ovat tunnistetut ja tarvittaviin toimenpiteisiin on ryhdytty.	1) Kriittiset laitteistot ovat tunnistetut ja tarvittaviin toimenpiteisiin on ryhdytty.	1) Kriittiset laitteistot ovat tunnistetut ja häiriöttömän sähkönsyötön (UPS) piirissä. 2) Häiriöttömän sähkönsyötön toimintavarmuus varmistetaan säännöllisesti testaamalla. 3) LVIS-järjestelyt varmistettu toimintavaatimusten mukaisesti. Tärkeät laitteet ja laitetilat on suojattu ympäristötekijöitä vastaan (mm. murto, palo, lämpö, kaasut, vesi).	1) Kriittiset laitteistot ovat tunnistetut ja häiriöttömän sähkönsyötön (UPS) piirissä. 2) Häiriöttömän sähkönsyötön toimintavarmuus varmistetaan säännöllisesti testaamalla. 3) LVIS-järjestelyt varmistettu toimintavaatimusten mukaisesti. Tärkeät laitteet ja laitetilat on suojattu ympäristötekijöitä vastaan (mm. murto, palo, lämpö, kaasut, vesi).	ISO/IEC 27002 9.1.4, VAHTI 8/2006	
I 305.0 **Ovatko näyttöpäätteet asetetut siten, ettei salassa pidettävää tietoa paljastu ohikulkijoille tai muille asiattomille?**	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille.	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille. Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuodatin.	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille. Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuodatin.	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille. Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuodatin.	VAHTI 8/2006	

Tietoliikenneturvallisuus, osa-alue I400

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 401.0 **Onko tietoliikenneverkon rakenne turvallinen?**	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internet-verkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja. (Vrt. I 403.0)	1) Tietoliikenneverkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri tietoturvatason järjestelmät on sijoitettu erillisille verkko-alueille. 2) Vyöhykkeisiinjakoperusteet on kuvattu. 3) Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain luvallinen liikenne sallitaan. 4) Valvonnan ja rajoitusten periaatteet on kuvattu. 5) Työasemilla, kannettavilla tietokoneilla ja vastaavilla on käytössä (host-based) palomuuriratkaisu, myös organisaatioverkon sisällä. 6) Fyysinen verkko on jaettu turvavyöhykkeisiin. Käytännössä vaaditaan, että verkko salataan, kun se menee hallitun fyysisen tilan ulkopuolelle (vrt. I 605.0).	1) Tietojenkäsittelyympäristö on fyysisesti erotettu verkko. (Ei liittymää esim. Internetiin; ei liittymää muuhun osaan yrityksen sisäverkkoa; ei liittymää muihin, kuin erikseen hyväksyttyihin järjestelmiin.) 2) Mikäli työtehtävät edellyttävät pääsyä Internetiin, se on järjestetty erillisellä tietokoneella, jota ei kytketä korotetun tason (III) verkkoon. Tällöinkin pääsy on pyrittävä rajaamaan erikseen määritellyille sivustoille ja protokollille (whitelisting).	Tietojenkäsittelyympäristö on fyysisesti erotettu ja valvottu verkko, josta ei ole liittymää muihin järjestelmiin.	ISO/IEC 27002 11.4.5, ISO/IEC 27002 11.4.6, ISO/IEC 27002 11.6.1, PCI DSS 1.1.5, PCI DSS 1.4, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 402.0 **Pääkysymys:** **Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia?** *Lisäkysymys:* *Onko varauduttu yleisimpiin nykyisiin verkkohyökkäyksiin?*	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Yleisiin verkkohyökkäyksiin on varauduttu konfiguroimalla palomuuri estämään verkkohyökkäykset.	1) Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Yleisiin verkkohyökkäyksiin on varauduttu vähintään seuraavilla oletuskonfiguraatioilla: a. Osoitteiden väärentäminen (spooffing) estetty. b. Lähdereititys (source routing) oletuksena estetty kaikissa verkkolaitteissa. c. Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. d. Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. e. SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. f. On määritetty mitä ICMP-liikennettä sallitaan. g. Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. h. Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. i. Palvelunestohyökkäysten (DoS, DDoS) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin.	Kuten perustasolla.	Kuten perustasolla.	Soveltaen VAHTI 2/2003, PCI DSS 1.1.5, VAHTI 8/2006	Perustason palomuurausvaatimus on työasemilla ja kannettavilla tietokoneilla usein helpointa toteuttaa sovelluspalomuurilla, johon on määritetty sallitut ohjelmistot ja estetty muiden liikennöinti.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 403.0 **Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?**	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu (vrt. I 401.0).	Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan tarkastuksilla.	Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisesti turva-auditoinnilla.	Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisesti turva-auditoinnilla.	PCI DSS 1.1.6, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/04_TTT-kaesikirja-Liite2-IT-kyp-syys-20081030.pdf	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 404.0 **Onko hallintayhteydet suojattu asianmukaisesti?**	Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 11.1, PCI DSS 2.3, VAHTI 8/2006	Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Mikäli verkkolaitteita hallitaan muuten kuin laitteeseen fyysisesti kytkeytymällä, ja mikäli hallintayhteys ei ole fyysisesti eriytetty, hallintaliikenteen tulee olla salattua. Vaatimus voidaan toteuttaa usein helpoiten siten, että estetään verkkolaitteiden hallinta telnetiä käyttäen ja käytetään hallinnassa SSH-yhteyttä. Vastaavasti vältettävä muitakin salaamattomia hallintatoteutuksia (käytettävä esim. HTTPS:ää HTTP:n sijaan web-selaimella hallittavissa järjestelmissä).

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 405.0 **Ovatko verkon aktiivilaitteet kovennettuja (konfiguroituja organisaation omilla parametreilla tehdasparametrien sijasta)?**	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan ainakin, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan ainakin, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.			ISO/IEC 27002 11.1, PCI DSS 2.1, PCI DSS 2.2, PCI DSS 6.1, PCI DSS 6.2, VAHTI 8/2006, ISO/IEC 11.2.3	Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Vrt. I 502.0, erityisesti lähteet.
I 406.0 **Ovatko langattomien verkkojen perussuojaukset käytössä?**	1) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 2) Liikenne salataan luotettavasti. 3) ”Vierasverkoille”, joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista.	1) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 2) Liikenne salataan riittävällä tasolla.	Langattoman ratkaisun tulee täyttää korotetun tietoturvatason vaatimukset.	Langattoman ratkaisun tulee täyttää korotetun tietoturvatason vaatimukset.	ISF-SOGP NW2.4	
I 407.0 **Onko sisäverkon rakenteen näkyminen Internetiin estetty?**	Ei erityissuosituksia.	Tietoliikenne ei saa paljastaa organisaation sisäverkon rakennetta.	Kuten perustasolla.	Kuten perustasolla.	PCI DSS 1.3.8, ISO/IEC 27002 12.5.4	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 408.0 **Pääkysymys:** **Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan?** *Lisäkysymys:* *Onko resurssit mitoitettu toimintavaatimusten mukaisiksi?*	Ei erityissuosituksia.	Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa.	Perustason lisäksi: 1) Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti. 2) Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. I 107.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a. merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b. normaalitilaan nähden poikkeavat protokollat, c. luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).	Perustason lisäksi: 1) Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti. 2) Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. I 107.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a. merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b. normaalitilaan nähden poikkeavat protokollat, c. luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.3.1, PCI DSS 11.4, VAHTI 8/2006	

Tietojärjestelmäturvallisuus, osa-alue I500

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 501.0 **Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?**	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin.	Vaaditaan ainakin, että 1) käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet, 2) kaikki käyttäjät tunnistetaan ja todennetaan, 3) pääsyä käyttöjärjestelmään valvotaan turvallisen sisäänkirjausmenettelyn avulla, 4) todennus tehdään vähintään salasanaa käyttäen 5) järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä /sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille. 6) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.	Perustason vaatimusten lisäksi käyttäjän tunnistamiseen käytetään vahvaa käyttäjäntunnistusta, mikäli samalla tietojärjestelmällä hallinnoidaan useampia kuin yhtä ko. turvatason projektia.	Perustason vaatimusten lisäksi käytetään aina vahvaa käyttäjäntunnistusta.	ISO/IEC 27002 11.4, ISO/IEC 27002 11.5.1, ISO/IEC 27002 11.5.2, PCI DSS 8.1, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/04_TTT-kaesikirja-Liite2-IT-kyp-syys-20081030.pdf	Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuskredentiaalit ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force –hyökkäyksiä vastaan. B- ja A-tason vaatimus vahvasta käyttäjätunnistuksesta voidaan joissain tapauksissa järjestää siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisestä tilasta, jonka pääsynvalvonnassa käytetään vahvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 502.0 **Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?**	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Työasemilta ja kannettavilta tietokoneilta vaaditaan, että 1) alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja; 2) tarjottavat (erityisesti verkko-)palvelut minimoitu ja rajattu vain välttämättömiin; 3) käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset; 4) järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. ”administrator” ja ”guest”) on oikeudet rajattu minimiin tai poistettu käytöstä; 5) oletussalasanat on vaihdettu (lisätietoa: I 510.0);	Menettely kattaa sen, että työasemien ja kannettavien tietokoneiden: 1) Verkkojaot poistettu käytöstä tai minimoitu. Verkkojaot poistettu aina käytöstä, kun laite kytkeytyy ei-luotettuun verkkoon. 2) Ohjelmistot, erityisesti webselaimet ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja. Sähköpostiohjelmistolta vaaditaan: a. Ajettava koodi oletuksena estetty. b. HTML-muotoisen sähköpostin lähettäminen estetty ja sen vastaanottamisessa viestit muunnetaan tekstimuotoon. c. Sähköpostin automaattinen esikatselu poistettu käytöstä.	Perustason vaatimusten lisäksi: Menettely kattaa sen, että palvelimien, työasemien ja kannettavien tietokoneiden BIOS-asetukset on asetettu turvallisuutta tehostaviksi ja asetusten muuttaminen on estetty valtuuttamattomilta käyttäjiltä. Käytännössä vaaditaan, että 1) BIOS-asetuksiin pääsy on suojattu salasanalla, 2) on sallittu vain ensisijaiselta kovalevyltä käynnistys; 3) tarpeettomat palvelut ja portit on poistettu käytöstä.	Korotetun tason vaatimusten lisäksi: Menettely kattaa sen, että on käytössä mekanismi, menetelmä tai menettelytapa, jolla tietojärjestelmään tehtävät muutokset tallentuvat ja tehdyt muutokset voidaan jälkikäteen havaita.	PCI DSS 2.1, PCI DSS 2.2, VAHTI 8/2006, ISO/IEC 11.2.3, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf Lähteitä järjestelmien / laitteiden kovennukseen ja turvalliseen konfiguraatioon: http://www.nsa.gov/ia/guidance/index.shtml, http://nvd.nist.gov/fdcc/index.cfm, http://iase.disa.mil/stigs/stig/index.html, http://iase.disa.mil/stigs/checklist/index.html,	II-tason vaatimus voidaan toteuttaa esimerkiksi tiedostojärjestelmän eheyttä tarkkailevalla ohjelmistolla. Lisätietoa löytyy esimerkiksi osoitteesta http://nsrc.org/security/#integrity.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
	6) työasemat lukittuvat automaattisesti, jos niitä ei käytetä vähään aikaan (minimivaatimus: salasanasuojattu näytönsäästäjä aktivoituu 10 minuutin käyttämättömyyden jälkeen); 7) käyttöoikeudet asetettu I 203.0:n mukaisesti; 8) lokimenettelyt asetettu (lisätietoa: I 504.0). Palvelimilta vaaditaan LISÄKSI, että a. alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti; b. palvelimet konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti. Verkkolaitteiden vaatimukset: I 405.0. Verkkotulostimet, puhelinjärjestelmät ja vastaavat: Soveltaen vastaavat vaatimukset kuin työasemilla ja palvelimilla: (verkko-)palvelut karsittava tarvittaviin, oletushallintatunnukset vaihdettava, tarpeelliset turvapäivitykset asennettava.	d. Liitetiedostoja ei avata automaattisesti. e. Sähköpostin liitteinä sallitaan vain erikseen määritellyt tiedostotyypit. Muiden käyttö on teknisesti estetty esimerkiksi ne pois suodattamalla ja asiaankuuluvasti aiheesta viestiin merkitsemällä. f. Roskapostiksi tulkittava liikenne suodatetaan pois tai merkitään vähintään varoitus esim. viestin otsikkokenttään.			http://www.cert.org/tech_tips/usc20.html, http://technet.microsoft.com/en-us/library/cc163140.aspx, http://technet.microsoft.com/en-us/library/cc757698.aspx, http://httpd.apache.org/docs/1.3/misc/security_tips.html, http://csrc.nist.gov/publications/PubsSPs.html, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml, http://www.hp.com/rnd/pdfs/Hardening_ProCurve_Switches_White_Paper.pdf	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 503.0 **Miten on pienennetty haittaohjelmien aiheuttamia riskejä?**	Haittaohjelmien havaitsemis- ja estotoimet sekä niistä toipumismekanismit ja asiaankuuluvat käyttäjien valppautta lisäävät ohjeet otettu käyttöön. Käytännössä vaaditaan, että ainakin 1) haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet); 2) torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä; 3) torjuntaohjelmistot tuottavat havainnoistaan lokitietoja; 4) haittaohjelmatunnisteet päivittyvät säännöllisesti; 5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta (vrt. I 206.0).	Edellisen tason suositusten lisäksi seuraava vaatimus: Haittaohjelmahavaintoja seurataan (vrt. I 105.0).	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 10.4.1, PCI DSS 5.1, PCI DSS 5.2, http://www.sans.org/cag/control/12.php	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 504.0 **Pääkysymys:** **Miten organisaation lokimenettelyt on toteutettu?** *Lisäkysymys:* *Kerätäänkö verkoista, laitteista ja järjestelmistä keskeiset lokitiedot ja käsitelläänkö niitä asianmukaisesti?*	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 2) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 3) Luottamukselliset lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 2) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 3) Luottamukselliset lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).	Perustason vaatimusten lisäksi: 1) On käytössä menettely hyökkäyksen/väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan. Erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan. (Vrt. I 409.0 ja I 107.0) 2) Samassa organisaatiossa tai turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun tarkan ajanlähteen kanssa. 3) Lokitiedot ja niiden kirjauspalvelut ovat suojattuja väärentämiseltä ja luvattomalta pääsyltä. On käytössä jokin menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen. 4) Keskeiset lokitiedot varmuuskopioidaan säännöllisesti. 5) Kriittisten tietojen käsittelystä muodostuu lokimerkintä. 6) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkintä. 7) Kriittisistä ylläpitotoimista tallennetaan kirjausketju (audit trail).	Perustason vaatimusten lisäksi: 1) Kriittisten tietojen käsittelystä muodostuu lokimerkintä. 2) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkintä. 3) Kriittisistä ylläpitotoimista tallennetaan kirjausketju (audit trail).	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.10.3, ISO/IEC 27002 10.10.6, PCI DSS 10.1, PCI DSS 10.2, PCI DSS 10.3, PCI DSS 10.4, PCI DSS 10.5, VAHTI 4/2002, VAHTI 8/2006	Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien peruslokitus on päällä. Tapahtumalokeja olisi hyvä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista. Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipalvelimelle, jonka tiedot sitten varmuuskopioidaan säännöllisesti. Se, mitä lasketaan säilytysvaatimuksen ”keskeisiin tallenteisiin” vaihtelee käyttöympäristöstä riippuen. Tähän kuuluvat aina keskeisten verkkolaitteiden ja palvelinten lokitiedot. Käyttöympäristöstä ja turvatasosta riippuen myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein. Toteutus työasemissa vaatii usein oletusarvojen muuttamista säilytysajan/-tilan suhteen.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 505.0 **Miten salassa pidettävät tiedot säilytetään tietojärjestelmissä?**	Tietojärjestelmissä sensitiivisten tietojen jakelu hoidetaan käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.	Edellisen tason suositusten lisäksi seuraava vaatimus: Tietojärjestelmien käytön yhteydessä syntyvät salassa pidettävää tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti (ks. I 603.0).	Perustason vaatimusten lisäksi: 1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason III tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 511.0). 2) Mikäli samalla tiedostopalvelimella/palvelimilla säilytetään useamman kuin yhden ko. turvatason hankkeen/projektin/toiminnon tietoja, palvelimella olevat tiedot säilytetään luotettavasti salakirjoitettuna käyttöoikeusrajoitteisissa hakemistoissa tai alueilla. 3) Suojaustason III tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	Korotetun tason vaatimusten lisäksi: 1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason II tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 511.0). 2) Mikäli samalla tiedostopalvelimella/palvelimilla säilytetään useamman kuin yhden ko. turvatason hankkeen/projektin/toiminnon tietoja, palvelimella olevat tiedot säilytetään luotettavasti salakirjoitettuna käyttöoikeusrajoitteisissa hakemistoissa tai alueilla. 3) Suojaustason II tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	VAHTI 8/2006, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf	Toteutussuositus väliaikaistietojen hävitykseen: logon- tai logoff-skriptein tuhotaan ylikirjoittaen tiedostot yleisimmistä käytetyistä dokumenttiformaateista yleisimmistä hakemistoista, jonne tilapäistiedostoja syntyy. Käytännössä esim. %HOMEPATH%/Local Settings/Temp alihakemistoineen, joista ylikirjoitetaan .doc*, .dot*, .xls*, .ppt*, .pdf, .rtf, .txt, acc*, .htm*, .mht, .xml, .jpg, .jpeg, .png, .tif*, .gif, .bmp, .zip, .gz, .tgz, .rar, .part.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 506.0 **Kuinka varmistutaan siitä, että luottamuksellista tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?**	1) Sensitiivistä tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. 2) Sensitiivistä tietoa sisältävät älypuhelimet suojataan riskiarvion mukaisesti.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: Turvaluokiteltua tietoa sisältävät älypuhelimet: 1) Pääsy puhelimen ja muistikortin tietoihin suojataan salasanalla. 2) Käytössä puhelimen/SIM-kortin/muistikortin automaattinen lukittuminen. 3) Etätyhjennysmahdollisuus käytössä. 4) Verkko- ja haittaohjelmauhat huomioidaan riskienarvioinnin mukaisesti.	Älypuhelimilla suojaustason III tiedon käsittely sallitaan vain viranomaisen erikseen hyväksymällä menettelyllä salattuna tai muutoin suojattuna.	Älypuhelimilla suojaustason II tiedon käsittely sallitaan vain viranomaisen erikseen hyväksymällä menettelyllä vahvasti salattuna tai muutoin vahvasti suojattuna.	ISO/IEC 27002 10.8.3, ISO/IEC 27002 9.2.5, VAHTI 8/2006, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/Tietoaineistojen-TurvallinenKasittely_v14.pdf, 2009/xxx/EC:n 9. artiklan kohta 4	Useimmat nykyiset käyttöjärjestelmät tarjoavat jo asennuksen yhteydessä mahdollisuuden kiintolevyn salaamiseen. Vaihtoehtoisesti voidaan käyttää erillistä ohjelmistoratkaisua. USB-muistien ja muiden tallennusmedioitten salaamiseen on olemassa sekä ohjelmisto- että laitetason ratkaisuja. Vrt. I 511.0. Salassa pidettävän aineiston käsittelyä tai säilyttämistä älypuhelimissa ei suositella. Mikäli näin kuitenkin on pakko tehdä, suojausten on vastattava kyseisen tason vaatimuksia.
I 507.0 **Kuinka varmistutaan siitä, etteivät salassa pidettävät tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?**	1) Kaikki sensitiivistä tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, sensitiivistä tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan, jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä. 3) Suositellaan turvallisuussopimuksen tekemistä huoltoyhtiön kanssa.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: Kaikki salassa pidettävää tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, salassa pidettävää tietoa sisältävä osa on tuhottava mekaanisesti.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.6, VAHTI 8/2006, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/Tietoaineistojen-TurvallinenKasittely_v14.pdf	Luotettavalla tyhjennyksellä tarkoitetaan tässä yhteydessä tiedon ylikirjoittamista. Vaatimus kattaa kaikki laitteistot, joihin on joskus tallennettu luottamuksellista tietoa, esim. kannettavat, työasemat, palvelimet, puhelimet, tulostimet, verkkolaitteet, jne. Vrt. I 603.0. Mikäli luotettava tyhjennys ei ole mahdollista, laitteisto tai sen osa on tuhottava mekaanisesti.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 508.0 **Pääkysymys:** **Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä?** *Lisäkysymykset:* *Miten tiedetään mitä (tietojärjestelmiin liittyviä) laitteita organisaatiossa on käytössä? Miten hallitaan tietoa käytetyistä ohjelmistoista ja niiden versioja lisenssitilanteesta? Havaitaanko, jos laite viedään luvatta pois organisaation tiloista? Havaitaanko, jos järjestelmiin on asennettu luvattomia ohjelmistoja?* *Tarkistetaanko kaikki tilat, joista on mahdollista päästä organisaation verkkoon, säännöllisesti luvattomien laitteistojen ja ohjelmistojen havaitsemiseksi?*	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Organisaation verkot tarkistetaan säännöllisesti luvattomien tietojärjestelmien (ohjelmistot, verkkopalvelut, jne.) löytämiseksi. 2) Konesalit, kytkentäkaapit ja vastaavat tilat tarkistetaan ajoittain luvattomien laitteistojen (pakettikaappaimet, key-loggerit, luvattomat langattomat tukiasemat, jne.) löytämiseksi.	Perustason vaatimusten lisäksi: 1) Kaikki tilat, joista on mahdollista päästä suojattuun verkkoon, tarkistetaan säännöllisesti luvattomien laitteistojen löytämiseksi. 2) Verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet, jotka eivät ole käytössä, on kytketty fyysisesti kytkentäpisteistä irti. 3) Kytkimien käyttämättömät portit on poistettu käytöstä. 4) Tuntemattomien laitteiden kytkeminen verkkoon estetään verkkoteknisin keinoin	Korotetun tason vaatimusten lisäksi: 1) Laitteistot on suojattu luvattomien laitteiden (key-loggerit ja vastaavat) liittämistä vastaan. Mikäli käytetään sinetöintiä, sinettien eheys tarkistetaan aina ennen laitteiston käyttöä. 2) Sähkökaapelointi sekä tietoja siirtävä tai tietotekniikkapalveluja tukeva tietoliikennekaapelointi on suojattu salakuuntelulta ja vaurioilta.	ISO/IEC 27002 9.2.1, ISO/IEC 27002 9.2.3, ISO/IEC 27002 11.4.1, ISO/IEC 27002 15.1.2, VAHTI 8/2006, http://www.sans.org/cag/control/1.php, http://www.sans.org/cag/control/2.php	II-tason vaatimusten toteutus voi edellyttää esim. a. laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan, b. peukalointia vastaan suojattujen laitteiden käyttämistä, tai c. jotain vastaavaa menettelyä (esim. laitteiden sinetöintiä).
I 509.0 **Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?**	Käytetään tunnettuja ja yleisesti luotettavina pidettyjä salausratkaisuja, tai ratkaisun luotettavuudesta on varmistuttu jollain muulla luotettavalla menetelmällä.	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on hyväksytty a. kansallisen tietoturvaviranomaisen toimesta, b. kansainvälisen tietoturvaviranomaisen toimesta, c. erillisessä ratkaisulle suoritetussa tarkastuksessa.	Kuten perustasolla.	Kuten perustasolla.	2009/xxx/EC:n 10. artiklan kohta 6, http://nato-cat.softbox.co.uk/	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 510.0 **Salausavainten hallinta.** **Pääkysymys:** **Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä?** *Lisäkysymys:* *Ovatko salausavaintenhallinnan prosessit ja käytännöt dokumentoituja ja asianmukaisesti toteutettuja?*	Vaaditaan, että salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Vaaditaan vähintään, että prosessit edellyttävät 1) kryptografisesti vahvoja avaimia; 2) turvallista avaintenjakelua; 3) turvallista avainten säilytystä; 4) säännöllisiä avaintenvaihtoja; 5) vanhojen tai paljastuneiden avainten vaihdon; 6) valtuuttamattomien avaintenvaihtojen estämisen.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 12.3.2, PCI DSS 3.6, VAHTI 8/2006	Kattaa myös SSL-avaimet. Vrt. I 511.0. Avaintenvaihdon aikavälin vaatimus arvioidaan tapauskohtaisesti käyttöympäristöstä ja -tarkoituksesta riippuen.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 511.0 **Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?**	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Vaatimukset samat kuin lähtötason suositukset.	Vaatimukset samat kuin lähtötason suositukset.	Vaatimukset samat kuin lähtötason suositukset.	ISO/IEC 27002 11.5, VAHTI 3/2001	
I 512.0 **Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?**	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Vaatimukset samat kuin lähtötason suositukset.	Vaatimukset samat kuin lähtötason suositukset.	Vaatimukset samat kuin lähtötason suositukset.	PCI DSS 3.2, PCI DSS 8.4, ISO/IEC 27002 11.5.3	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 513.0 **Miten on varmistuttu ajettavan koodin turvallisuudesta?**	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	1) Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus). 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaatteiden, esim. Open Web Application Security Project Guide, toteuttamista. Toimittajilta vaaditaan selvitys miten tietoturvallisuus on otettu huomioon tuotekehityksessa.	ko. toimintaympäristöön hyväksymiä järjestelmiä/ohjelmistoja. 2) Kaikki koodi on avoimesti tarkastettavissa (esim. takaportit, turvattomat toteutukset, jne.) tai sopimuksessa on varattu oikeus lähdekoodin tarkastukseen. Vaihtoehdossa 2 on näytettävä todiste koodin luotettavaksi toteamisesta (esim. kuvaukset toimittajan prosesseista ja ulkopuolisen tekemä katselmointiraportti).	ISO/IEC 27002 12.2.1, ISO/IEC 27002 12.4.1, ISO/IEC 27002 15.1.2, PCI DSS 6.5, VAHTI 8/2006, http://www.bsimm.com/, http://www.opensamm.org/, http://www.owasp.org/index.php/Category:OWASP_Guide_Project, http://www.owasp.org/index.php/Top_10_2007	Ohjelmistotoimittajalta voidaan vaatia esim. seuraavia: 1) Ohjelmistokehittäjien riittävä tietoturvatietous on varmistettu. 2) Ohjelmistokehityksen aikana on suoritettu tietoturvauhka-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty. 3) Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä. 4) Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan (esim. Microsoftilla on listat kielletyistä funktioista). 5) Arkkitehtuuri ja lähdekoodi on katselmoitu. 6) Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä. 7) Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu. 8) Hankittavista ohjelmistoista on saatava myös dokumentaatio, josta selviää lisäksi ainakin sovelluksen käyttämät verkkoportit. Suotavaa on myös edellyttää, että a. sovellukset käyttävät pientä määrää määriteltyjä portteja, b. dynaamisia portteja käyttävät sovellukset käyttävät vain pientä porttiavaruutta, ja c. ohjelmistot eivät vaadi laajoja käyttöoikeuksia toimiakseen (ts. ”peruskäyttäjän” oikeudet)

Tietoaineistoturvallisuus, osa-alue I600

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 601.0 **Millainen tiedon luokittelumenettely organisaatiolla on?**	Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella.	1) Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	Kuten perustaso.	Kuten perustaso.	ISO/IEC 27002 7.2.1, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/ 20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf, 2009/xxx/EC:n 2. artikla	Vrt. käsittelysääntövaatimukset I 505.0, I 602.0, I 506.0, I 603.0, I 604.0, I 605.0, I 606.0, I 607.0.
I 602.0 **Onko huolehdittu siitä, että salassa pidettäviä tietoa sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti?**	Salassa pidettävälle aineistolle on työtiloissa lukitut kaapit, kassakaapit tai vastaavat.	1) Työskentelyn jälkeen selväkielisessä muodossa oleva, mutta salassa pidettävä aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään kassakaappiin, lukittuun kaappiin tai vastaavaan säilytystilaan. 2) Työskentelyn jälkeen työskentelytila tarkistetaan tai tila lukitaan ulkopuolisilta.	Työskentelyn jälkeen suojaustason III aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään EURO II -tason kassakaappiin tai vastaavaan säilytystilaan, kuten holviin (EURO IV).	Työskentelyn jälkeen suojaustason II aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään EURO II -tason kassakaappiin tai vastaavaan säilytystilaan, kuten holviin (EURO IV).	VAHTI 8/2006, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf, 2009/xxx/EC:n liite II	Vrt. aineistot tietojärjestelmissä: I 505.0, I 506.0, I 507.0, I 508.0. Kassakaapeille ja vastaaville säilytystiloille on aina tarkistettava tarkentavat vaatimukset (esim. tarkka luokka, kiinnitys, lisävaatimukset rikosilmoitusjärjestelmälle, jne.) fyysisen turvallisuuden kriteeristöosuudesta.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 603.0 **Hävitetäänkö luottamuksellisia tietoja sisältävät aineistot luotettavasti?**	1) Luottamuksellisten sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen). 2) Ei-sähköisten luottamuksellisten aineistojen tuhoaminen on järjestetty luotettavasti.	1) Organisaatiossa on paperinrepijä tai muu luotettava menettely (esim. polttaminen) suojaustason IV aineiston hävittämiseksi. 2) Tietojärjestelmien käytön yhteydessä syntyvät salassa pidettävää tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti. Vrt. I 505.0.	Organisaatiossa on hyväksytty paperinrepijä suojaustason III aineiston hävittämiseksi. Silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4).	Suojaustason II aineiston hävittäminen hoidetaan toisen henkilön valvonnassa viranomaisen hyväksymällä tavalla, kuten paperinrepijällä jonka silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4). Hävittäminen dokumentoidaan.	VAHTI 8/2006, 2009/ xxx/EC:n liitteen III jakso VI	Toteutussuositus väliaikaistietojen hävitykseen: logon- tai logoff-skriptein tuhotaan ylikirjoittaen tiedostot yleisimmistä käytetyistä dokumenttiformaateista yleisimmistä hakemistoista, jonne tilapäistiedostoja syntyy. Käytännössä esim. %HOMEPATH%/Local Settings/Temp alihakemistoineen, joista ylikirjoitetaan .doc*, .dot*, .xls*, .ppt*, .pdf, .rtf, .txt, acc*, .htm*, .mht, .xml, .jpg, .jpeg, .png, .tif*, .gif, .bmp, .zip, .gz, .tgz, .rar, .part. Muistettava myös käytöstä poiston yhteydessä: I 507.0.
I 604.0 **Onko salassa pidettävän aineiston kopiointi ja tulostus järjestetty turvallisesti?**	Sensitiivisen aineiston kopiointi ja tulostus on järjestetty riskienarvioinnissa riittävän turvalliseksi katsotulla menettelyllä.	1) Kopioita käsitellään kuten alkuperäistä asiakirjaa. 2) Alkuperäiset luokittelumerkinnät säilyvät kopioinnissa ja tulostuksessa (tai vastaavat merkinnät lisätään välittömästi kopioinnin/ tulostuksen jälkeen).	Perustason vaatimusten lisäksi: 1) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus aineistoon ja tarve tietosisältöön. 2) Kopion/tulosteen voi ottaa vain turvatasolle hyväksytyn laitteen kautta. 3) Kopiokoneiden ja tulostimien on oltava hyväksytyssä tilassa, eikä niistä saa olla ulkoisia tiedonsiirto- tai huoltoyhteyksiä.	Perustason vaatimusten lisäksi: 1) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus aineistoon ja tarve tietosisältöön. 2) Kopiointi merkitään sekä alkuperäisen aineiston etusivulle, että diaariin/ rekisteriin jokaisen kopion ehdottoman jäljitettävyyden mahdollistamiseksi. 3) Kopion/tulosteen voi ottaa vain hankkeeseen hyväksytyn laitteen kautta. 4) Kopiokoneiden ja tulostimien on oltava hyväksytyssä tilassa, eikä niistä saa olla ulkoisia tiedonsiirto- tai huoltoyhteyksiä.	http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/ VAHTI-ohje ”Tietoaineistojen turvallinen käsittely”	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 605.0 **Pääkysymys:** **Onko salassa pidettävän aineiston sähköinen välitys järjestetty turvallisesti?** *Lisäkysymys:* *Onko tietoliikenne (ml. sähköinen viestintä) suojattu riskeihin nähden riittävillä mekanismeilla?*	1) Organisaatiossa pystytään tunnistamaan sensitiiviset / salassa pidettävät tiedot ja huolehtimaan siitä, että ne välitetään asianmukaisesti suojaten. 2) Yhteys sähköpostipalvelimen ja -asiakasohjelman välillä on suojattu. 3) Mikäli sähköpostissa, pikaviestimissä, VoIP-puheluissa ja vastaavissa käsitellään sensitiivistä tietoa, on liikenne (tai viesti) suojattava riskienarvioinnin mukaisesti siten, että sensitiivistä tietoa ei pääse vuotamaan ulkopuolisille.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Sähköpostia/ telekopiolaitetta käytettäessä varmistetaan vastaanottajan osoite/ numero. 2) Aina, kun liikenne kulkee julkisen verkon (Internet, puhelinverkko, GSM-verkko tai muu verkko, mikä ei ole ko. turvatason vaatimusten mukainen) kautta, on liikenne (tai aineisto) salattava luotettavasti. 3) Yhteyden on oltava luotettavasti suojattu päästä päähän. Tapauskohtaisesti voidaan hyväksyä toteutukset, joissa a. liikenne kulkee salaamattomana vain organisaation luotetun verkon tai verkon osan sisällä, b. liikenne salataan palvelimelta palvelimelle tai organisaatioiden välillä rajalta rajalle. 4) Puhelinkeskustelut salataan riittävällä menetelmällä. 5) Kun turvaluokiteltu tieto siirretään tietojärjestelmästä toiseen, se suojataan siirron aikana ja vastaanottavassa järjestelmässä tiedon alkuperäisen turvaluokituksen edellyttämällä tavalla.	Perustason vaatimusten lisäksi: 1) Telekopiona suojaustason III aineistoa lähetetään vain, jos telekopiokone on varustettu viranomaisen hyväksymällä salaamislaitteella ja mikäli telekopiolaite on sijoitettu tilaan, johon pääsy on asiattomilta estetty. 2) Puhelimessa suojaustason III tiedosta voidaan keskustella vain viranomaisen erikseen hyväksymän salausmenetelmän välityksellä.	Korotetun tason vaatimusten lisäksi: 1) Suojaustason II aineisto voidaan lähettää julkisen verkon yli salattuna viranomaisen hyväksymällä vahvalla päästä päähän salaustuotteella. 2) Suojaustason II tietoa ei tallenneta, eikä siirretä missään muodossa sellaisessa verkossa tai tietolaitteessa, joka ei ole viranomaisen erikseen tähän tarkoitukseen hyväksymä. Tietoa tulee tallentaa vain määritetyn laitteen kautta. 3) Suojaustason II aineistoista ei keskustella puhelimessa muuten kuin viranomaisen erillisesti hyväksymään salausjärjestelyyn perustuen.	ISO/IEC 27002 10.8, soveltaen PCI DSS 4.1, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf, 2009/xxx/EC:n liite IV	Kattaa puhelimen, telefaksin, sähköpostin, pikaviestimet ja vastaavat tiedonsiirtomenetelmät. Suositus 2: Toteutus on usein helpointa käyttämällä liikenteen salaavia protokollia salaamattoman vaihtoehdon sijaan, esim. IMAPS-protokolla IMAP:n sijaan. Vrt. myös I 513.0. Suositus 3: Toteutus on usein helpointa käyttämällä päästä päähän -salausta sovellustasolla, tai kirjaamalla sensitiiviset tiedot liitetiedostoon, joka salataan luotettavasti (vrt. I 511.0). Joskus on suositeltavaa käyttää yritystason pikaviestin- tai/ja VoIP-ratkaisuja, joissa palvelin, asiakasohjelmat ja niiden välinen liikenne pysyy luotetun organisaatioverkon tai sen osan sisällä, ja liikenne on salattua. Suojaustason IV vaatimus 2: Vrt. I 401.0. Suojaustason IV vaatimus 3: Vrt. suosituksen 3 huomiot.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 606.0 **Onko salassa pidettävän aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?**	Välitys on hoidettu riskienarvioinnin perusteella riittävän turvalliseksi katsotulla menettelyllä.	1) Lähetykset osoitetaan henkilön nimellä. 2) Pakkaus ei saa ulkoisesti paljastaa sen sisältävän turvaluokiteltua materiaalia. Huom: kirjekuoren tai vastaavan on oltava läpinäkymätön. 3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.	1) Aineistot lähetetään kirjattuna postina suljetussa, kaksinkertaisessa kirjekuoressa, josta ainakin sisäkuoren on oltava läpinäkymätön. Suositellaan, että sisempi kuori sinetöidään ja että vastaanottajaa vaaditaan tarkistamaan sinetöinnin eheys. 2) Organisaation sisäiseen postin käsittelyketjuun saa kuulua vain hyväksyttyä henkilöstöä, jonka perehtymisoikeus ko. tiedon suojaustasoon on hyväksytty ja kirjattu. Henkilöllä on oltava esimiehensä määrittämä, työtehtäviinsä perustuva tarve perehtyä ko. aineistoon. 3) Lähetettäessä aineistoa kuriirin välityksellä pakkauksen päällä tulee selkeästi ilmoittaa, että pakkauksen saa toimittaa vain kuriirin välityksellä. Kuriiri on koulutettava ja varustettava sekä kuriiritodistuksella, että kuriiripostikirjalla, johon vastaanottaja kuittaa vastaanottamansa lähetyksen.	1) Suojaustason II aineistoa ei lähetetä postitse, vaan lähetys toimitetaan perille joko henkilökohtaisesti tai viranomaisten hyväksymän kuriirimenettelyn välityksellä. 2) Kuriirimenettelyllä toimitettuna aineistojen on oltava kaksinkertaisessa kuoressa, joista sisäkuoren on oltava sinetöity. Vastaanottajan on tarkistettava sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään. 3) Organisaation sisäiseen suojaustason II postin käsittelyketjuun saa kuulua vain sellaista henkilöstöä, jonka perehtymisoikeus ko. tiedon turvallisuusluokkaan on hyväksytty ja kirjattu. Henkilöllä on oltava työtehtävään perustuva, esimiehen määrittämä tarve perehtyä ko. aineistoon. Jokainen asiakirjaan perehtynyt henkilö kirjaa koko nimensä ja perehtymispäivämäärän aineiston etusivulle tai erilliseen kuittauskirjaan.	ISO/IEC 27002 10.8.3, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 607.0 **Pääkysymys:** **Pystytäänkö seuraamaan minne ja mistä salassa pidettävät aineistot on välitetty?** *Lisäkysymys:* *Kirjataanko turvaluokitellut aineistot?*	Ei erityistä suositusta.	Ei auditointivaatimuksia.	Suojaustason III tieto, riippumatta sen muodosta, rekisteröidään diaariin tai rekisteriin ennen välitystä ja vastaanotettaessa. Jos kyseessä on viestintä- ja tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa sen omien prosessien avulla.	Korotetun tason vaatimusten lisäksi: 1) suojaustason II tieto rekisteröidään omaan rekisteriinsä tai diaariin. 2) Diaaria/rekisteriä säilytetään, kuten suojaustason II asiakirjaa. 3) Diaarista/rekisteristä tulee käydä ilmi kunkin asiakirjan sen hetkinen haltija tiedon elinkaaren loppuun asti.		

Käyttöturvallisuus, osa-alue I700

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 701.0 **Pääkysymys:** **Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat?** *Lisäkysymykset:* *Testataanko toipumisvalmiutta säännöllisesti?* *Suojataanko salassa pidettävät tiedot myös hätätilanteissa?*	On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan (liike)toimintavaatimuksiin nähden riittävässä ajassa. Käytännössä tämä vaatii usein 1) jatkuvuus-/toipumissuunnitelmaa, ja 2) suunnitelman säännöllistä testaamista. Vähintään tulee määritellä järjestelmien käytettävyysvaatimukset ja mitoittaa toipumismekanismit riskienarvioinnin mukaisesti niihin.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Suunnitelmissa otetaan huomioon salassa pidettävien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys 2) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä	Kuten perustasolla.	Kuten perustasolla.	JHTT 5 ISO/IEC 27002 14.1, VAHTI 8/2006, 2009/xxx/EC:n 5. artiklan kohdat 3 ja 4	Vrt. dokumentointivaatimus I 702.0 ja riskienarviointivaatimus I 104.0. vrt. JHTT 5

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 702.0 **Pääkysymys:** **Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen?** *Lisäkysymykset:* *Onnistuuko toipuminen jos järjestelmän tai verkon vastuuhenkilö ei ole käytettävissä?* *Miten nopeasti toipuminen onnistuu? Seurataanko säännöllisesti, että suojattavaa tietoa käsittelevän ympäristön dokumentaatio on ajan tasalla? Miten menetellään, mikäli tiedoissa on puutteita?*	Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 2) Eroavaisuuksia käsitellään tietoturvapoikkeamina.	Kuten perustasolla.	Kuten perustasolla.	JHTT 5 ISO/IEC 27002 14.1, ISO/IEC 27002 10.1, VAHTI 2/2001, VAHTI 5/2004, VAHTI 8/2006, http://www.interpol.int/public/technologycrime/crimeprev/companychecklist.asp	Käytännössä tämä vaatii usein verkon rakenteen, IP-osoitteiden, vyöhykkeiden, segmenttien, palomuurisäännöstöjen, verkkolaitteiden käyttöjärjestelmä-/firmware-versioiden, palvelinten ja tuotantojärjestelmien ohjelmistoversioiden ja asetusten, ja vastaavien tietojen, dokumentointia sillä tarkkuudella, että vikaantumisesta pystytään toipumaan liiketoimintavaatimusten mukaisesti. Riippuen organisaation toimialasta ja tehtävistä, dokumentaation kattavuudelta saatetaan vaatia sitä, että ulkopuolinen osaa sen perusteella saattaa vikaantuneet verkot ja järjestelmät käyttökuntoon. Tulee myös huolehtia siitä, että dokumentaatio pidetään ajan tasalla. Yksi tapa ylläpitää dokumentaatiota on wiki, johon päivitetään verkon ja järjestelmien muutokset sitä mukaa, kun niitä tulee. Markkinoilla on myös muita soveltuvia tuotteita.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 703.0 **Pääkysymys:** **Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?** *Lisäkysymykset:* *Käytetäänkö vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä?* *Käytetäänkö salassa pidettävän tiedon käsittelyyn vain viranomaisen hyväksymiä tiloja, verkkoja ja järjestelmiä? Miten varmistutaan tietojärjestelmien eheydestä?*	1) Käytössä selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään. 2) Turvaluokitellun tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä tiloja, verkkoja ja järjestelmiä.	Kuten perustasolla.	Kuten perustasolla.	JHTT 5G ISO/IEC 27002 10.3.2, ISO/IEC 27002 12.1.1, ISO/IEC 27002 12.4.1, VAHTI 8/2006, 2009/xxx/EC:n 9. artiklan kohta 3, 2009/xxx/EC:n 10. artiklan kohta 4	vrt. JHTT 5

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 704.0 **Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?**	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Turvallisesta etä- ja matkatyöskentelystä on henkilöstön saatavilla ohje. 2) Laitteita, tietoaineistoja tai ohjelmia ei siirretä pois työpaikalta ilman ennalta saatua valtuutusta. 3) Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja todennusmenettelyjä. 4) Suojaustason IV tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle. 5) Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei jätetä valvomatta julkisille paikoille, kannettavat tietokoneet kuljetetaan matkustaessa käsimatkatavarana. 6) Vain hyväksyttyjä etätyöyhteyksiä käytetään.	Suojaustason III järjestelmien etähallinta on lähtökohtaisesti estetty. Etähallinta on sallittu vain viranomaisen erikseen hyväksymällä menettelyllä.	Suojaustason II järjestelmien etähallinta on estetty.	ISO/IEC 27002 10.8.3, ISO/IEC 27002 11.4.2, ISO/IEC 27002 11.7.1, ISO/IEC 27002 11.7.2, ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.5, ISO/IEC 27002 9.2.7, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006	Suojaustasolla III hyväksyttävä etähallintamenettely huomioi mm. etähallintapisteiden fyysisen ja loogisen pääsynvalvonnan, hallintaan käytetyt laitteistot ja ohjelmistot, hallintaliikenteen salauksen, ja edellä mainittujen elementtien luotettavuuden erityisesti luottamuksellisuuden ja eheyden suhteen.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 705.0 **Ovatko kehitys-/testaus- ja tuotantojärjestelmät erilliset?**	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. Tuotantojärjestelmän oltava erillinen, jotta kehitys- tai testaustoimet eivät aiheuta tuotantokatkoksia. 2) Ennen uuden järjestelmän käyttöönottoa testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan.	Edellisen tason suositusten lisäksi seuraava vaatimus: Suojaustason IV tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli ko. ympäristön turvataso on alhaisempi kuin tuotantoympäristön.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 10.1.4, PCI DSS 6.3.2, PCI DSS 6.3.4, PCI DSS 6.3.5, PCI DSS 6.3.6	Tuotantodataa voidaan kopioida kehitys-/testausympäristöön, mikäli data sanitoidaan siten, että luottamuksellisuus ei vaarannu. Vrt. muutoshallinta: I 109.0.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 706.0 **Pääkysymys:** **Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?** *Lisäkysymykset:* *Onko tietoturvatiedotteiden seuranta vastuutettu?* *Onko turvapäivitysten asentamiseen luotu menettelytavat? Valvotaanko niiden toteutumista?*	Viranomaisten (esim. CERT), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti.	Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan säännöllisesti haavoittuvuuksien löytämiseksi.	Kuten perustasolla ja lisäksi: skannaus suoritetaan vähintään vuosittain ja merkittävien muutosten jälkeen.	Kuten perustasolla ja lisäksi: skannaus suoritetaan vähintään vuosittain ja merkittävien muutosten jälkeen.	ISO/IEC 27002 12.6.1, ISF-SOGP CI3.6, PCI DSS 6.1, PCI DSS 6.2, PCI DSS 11.2, VAHTI 8/2006	Suositustasolle esimerkkejä käytännön toteutuksesta: Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen, ja ne asennetaan käyttöjärjestelmiin, verkkolaitteisiin (lähinnä firmwaret), palvelinsovelluksiin jne. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla. Suojaustaso III: ”Merkittäviin muutoksiin” voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien mukaan tuonnit ja/tai vanhojen merkittävät päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 707.0 **Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?**	Käyttäjät velvoitetaan seuraavaan käytäntöön: a. Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. b. Aktiiviset istunnot päätetään työn päättyessä ja tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). c. Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä.	Mikäli turvaluokiteltua tietoa sisältävä laite joudutaan jättämään tilaan, jossa siihen on fyysinen pääsy ei-luotetuilla (arvioitava tapauskohtaisesti: esim. organisaation ulkopuolisilla), salaus on aktivoitava laitteelta poistuttaessa.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 11.3.2	Vrt. työasemien ja vastaavien automaattinen lukittuminen: I 502.0
I 708.0 **Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?** *Lisäkysymys:* *Onko huolehdittu siitä, että kriittiset ylläpitotoimet vaativat kahden tai useamman henkilön hyväksynnän?*	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	Ei auditointivaatimusta.	Ei auditointivaatimusta.	Ei auditointivaatimusta.	ISO/IEC 27002 11.3.3, VAHTI 8/2006	

Kysymys	Lähtötason suositukset	Perustason (IV) vaatimukset	Korotetun tason (III) vaatimukset	Korkean tason (II) vaatimukset	Lähde/viite	Kommentit
I 709.0 **Pääkysymys:** **Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä?** *Lisäkysymys:* *Onko huolehdittu siitä, että kriittiset ylläpitotoimet vaativat kahden tai useamman henkilön hyväksynnän?*	Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään organisaation suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.	Vaarillisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, niitä varten on luotava valvontamekanismi.	Vaarillisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, niitä varten on oltava valvontamekanismi. Järjestelmäkohtaisesti määritetään ne kriittiset toimet, joihin erityisvalvonta kohdistetaan.	Vaarillisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, niitä varten on oltava valvontamekanismi. Järjestelmäkohtaisesti määritetään ne kriittiset toimet, joihin erityisvalvonta kohdistetaan.	JHTT 5 ISO/IEC 27002 10.1.3, VAHTI 8/2006	
I 710.0 **Onko riittävästä varmuuskopioinnista huolehdittu?**	Riittävästä varmuuskopioinnista on huolehdittu. Huolehdittava, että: 1) Varmistusten taajuus on suhteessa varmistettavan tiedon kriittisyyteen. 2) Varmuuskopioinnin oikea toiminta ja palautusprosessi testataan säännöllisesti. 3) Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. 4) Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä.	Edellisen tason suositusten lisäksi seuraavat vaatimukset: 1) Salassa pidettävää tietoa sisältävät varmuuskopiot säilytetään tiedon suojaustason tai turvallisuusluokan edellyttämässä tilassa ja tarvittaessa salakirjoitettuna. 2) Varmistusmedioista on olemassa listat. 3) Palautusprosessi on dokumentoitu.	Kuten perustasolla.	Kuten perustasolla.	ISO/IEC 27002 10.5.1, PCI DSS 9.5	Suositusten kohta 3: Tapauskohtaisesti voidaan vaatia kaikkein toimintakriittisimmän tiedon suojakopion säilyttämistä erillisessä rakennuksessa, toimipisteessä tai esimerkiksi pankissa.

Järjestelmässä [järjestelmän nimi] olevat tietotyypit, niiden sijainti ja luokittelu.
FM = Fataali merkitys
EM = Erittäin iso merkitys
M = Merkittävä
VM = Vähäinen merkitys

Tieto A: Tietotyyppi ”1”, joka sisältää tarkemmin esitettynä tietoja [kuvaus1], jotka ovat [kuvaus2] sekä tietoja [kuvaus3], jotka ovat [kuvaus4].
Luokitus:

	A				LL				LA			
	FM	**EM**	**M**	**VM**	**FM**	**EM**	**M**	**VM**	**FM**	**EM**	**M**	**VM**
Luottamuksellisuus	■	□	□	□	■	□	□	□	■	□	□	□
Käytettävyys	■	□	□	□	■	□	□	□	□	□	■	□
Eheys	■	□	□	□	■	□	□	□	□	■	□	□
Kiistämättömyys	■	□	□	□	■	□	□	□	□	■	□	□

Mikä on tiedon ”kotipesä”?
- Tiedot sijaitsevat palvelimessa [palvelimen nimi/kuvaus]. Osa [x] on salattuna ja osa [y] on selkokielisenä.

Kuka pääsee tietoja hakemaan ja millä järjestelmällä?
- Käyttäjät pääsevät työtehtävistään riippuen tulostamaan tietoja [y] tai kuittaamaan tietoja [x] käytetyksi. Tietoja [x] ei siirretä kotipesästä muualle.

Missä tiedot voivat ”kotipesän” lisäksi olla?
- Asiakkaalla (LA:lla) tai ”välittäjällä (LL) tietojen [y] osalta voi olla printattuna. Tietojen [x] säilytys tai siirto muualle on sopimusten/ohjeiden mukaisesti kielletty.

Kansallisen turvallisuusauditointikriteeristön 20.11.2009 **LIITE 2**

MÄÄRITELMIÄ

1) Yrityssalaisuuksia sekä liike- ja ammattisalaisuuksia kutsutaan tässä kriteeristössä sensitiiviseksi tiedoksi.
2) Valtionhallinnon salassa pidettävä tieto –käsite kattaa suojaustasoihin I – IV kuuluvan tiedon ja turvallisuusluokkiin I – IV kuuluvan tiedon[1].

3) Tietoturvallisuustasojen vastineet suojaustasoissa ja turvallisuusluokissa ovat:
   PERUSTASO – SUOJAUSTASO IV – TURVALLISUUSLUOKKA IV (KÄYTTÖ RAJOITETTU)
   KOROTETTU TASO – SUOJAUSTASO III – TURVALLISUUSLUOKKA III (LUOTTAMUKSELLINEN)
   KORKEA TASO – SUOJAUSTASO II – TURVALLISUUSLUOKKA II (SALAINEN)

4) Tiedon luokitteluperusteet tiedon suojaustasoittain/turvallisuusluokittain ovat seuraavat:
   IV: jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa (yleisille eduille)
   III: jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa (yleiselle edulle, kv. suhteille, maanpuolustukselle, valtion turvallisuudelle)
   II: jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa (yleiselle edulle, kv. suhteille, maanpuolustukselle, valtion turvallisuudelle)
   I: jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa (yleiselle edulle, kv. suhteille, maanpuolustukselle, valtion turvallisuudelle)

1 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, luonnos, marraskuu 2009

Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

ISBN: 978-951-25-2077-0 (nid.)
ISBN: 978-951-25-2078-7 (pdf)

www.defmin.fi