Turvallisuusluokiteltuja asiakirjoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta.
Turvallisuusluokan I asiakirjaa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla.
Turvallisuusluokan II—IV asiakirjaa saa käsitellä turvallisuusalueilla ja niiden ulkopuolella kuitenkin siten, että:
1) turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle;
2) turvallisuusluokan II ja III paperiasiakirjat on säilytettävä turva-alueella;
3) turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle;
4) turvallisuusluokan IV paperiasiakirjat on säilytettävä turvallisuusalueella.
Sen estämättä, mitä 3 momentin 1 ja 3 kohdassa säädetään tietojärjestelmän sijoittamisesta turvallisuusalueille, turvallisuusluokan II—IV asiakirjoja saa käsitellä myös 9 §:n 1 kohdassa tarkoitetuilla hallinnollisilla alueilla ja niiden ulkopuolella 11 ja 12 §:n vaatimukset täyttävän päätelaitteen ja tietoliikennejärjestelyn avulla. Turvallisuusluokan II asiakirjan käsittelyyn käy-tetty päätelaite on kuitenkin säilytettävä turva-alueella. Jos turvallisuusluokan III tai IV sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvalli-suusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huo-lehdittava.

Tämä ohje on laadittu tukemaan tiedonhallintalain ja turvallisuusluokitteluasetuksen täytäntöönpanoa. Ohje ei ole velvoittava. Ohje sisältää parhaita käytäntöjä, joiden mukaan toimimalla pystytään saattamaan yleiset tietoon kohdistuvat riskit siedettävälle tasolle. Kukin viranomainen on vastuussa oman tietojenkäsittelynsä turvallisuudesta, ja riittävien suojausten toteuttamisesta riskienarviointinsa pohjalta.

TIETOJEN KÄSITTELYN JA SÄILYTYKSEN PERUSPERIAATTEET

TURVALLISUUS-LUOKKA	KÄSITTELY		SÄILYTYS	
	Hallinnollinen alue	Turva-alue	Hallinnollinen alue	Turva-alue
TL I ERITTÄIN SALAINEN	ei	ok, jos pääsy tietoihin on suojattu sivullisilta	ei	kassakaapissa tai holvissa
TL II SALAINEN	ok, jos pääsy tietoihin on suojattu sivullisilta	ok, jos pääsy tietoihin on suojattu sivullisilta	ei	kassakaapissa tai holvissa
TL III LUOTTAMUKSELLINEN	ok, jos pääsy tietoihin on	ok, jos pääsy tietoihin on	ei	kassakaapissa tai holvissa

	suojattu sivullisilta	suojattu sivullisilta		
TL IV KÄYTTÖ RAJOITETTU	ok, jos pääsy tietoihin on suojattu sivullisilta	ok, jos pääsy tietoihin on suojattu sivullisilta	soveltuvassa lukitussa toimistokalusteessa	soveltuvassa lukitussa toimistokalusteessa

Sähköistä käsittelyä tai säilyttämistä turvallisuusalueen ulkopuolella on käsitelty luvussa 5.

1. RISKIEN ARVIOINTI

Tiedon käsittelyn ja säilytyksen suojaamiseksi valittavien fyysisten turvatoimien on perustuttava viranomaisen tekemään riskien arviointiin. Riskinhallintaprosessissa on otettava huomioon kaikki asiaankuuluvat tekijät, erityisesti seuraavat:
a) Turvallisuusluokiteltujen tietojen turvallisuusluokka;
b) Turvallisuusluokiteltujen tietojen käsittelytapa ja määrä pitäen mielessä, että niiden suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista;
c) Turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö; rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa; ja
d) Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille

2. TIETOJEN SÄILYTTÄMINEN

Turvallisuusluokitellut tiedot, jotka kuuluvat KÄYTTÖ RAJOITETTU -turvallisuusluokkaan, on säilytettävä soveltuvissa lukituissa toimistokalusteissa hallinnollisella alueella tai turva-alueella. Niitä voidaan tilapäisesti säilyttää turva-alueen tai hallinnollisen alueen ulkopuolella, jos tietojen haltija on sitoutunut noudattamaan viranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä.

Turvallisuusluokitellut tiedot, jotka kuuluvat LUOTTAMUKSELLINEN, SALAINEN tai ERITTÄIN SALAINEN-turvallisuusluokkaan, on säilytettävä turva-alueella joko kassakaapissa tai holvissa. Sähköistä käsittelyä tai säilyttämistä turvallisuusalueen ulkopuolella on käsitelty luvussa 5.

3. TIETOJEN KÄSITTELYN VÄHIMMÄISVAATIMUKSET

Turvallisuusluokiteltuja tietoja, jotka kuuluvat KÄYTTÖ RAJOITETTU, LUOTTAMUKSELLINEN tai SALAINEN-turvallisuusluokkaan on käsiteltävä hallinnollisella alueella tai turva-alueella. Turvallisuusluokiteltuja tietoja, jotka kuuluvat ERITTÄIN SALAINEN -turvallisuusluokkaan on käsiteltävä turva-alueella.

Asiakirjojen käsittely on mahdollista myös turvallisuusalueiden ulkopuolella, mikäli on toteutettu korvaavia toimenpiteitä sen varmistamiseksi, että pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta.

Tiedon käsittelyn tulee täyttää taulukossa esitettävät vähimmäisvaatimukset. Vähimmäisvaatimukset tulee täyttyä riippumatta siitä, millä turvallisuusalueella tietoa käsitellään. Vähimmäisvaatimusten lisäksi viranomaisen tulee suunnitella ja toteuttaa riskien arviointiin (kohta 1) perustuvat muut

riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä.

4. SÄHKÖINEN KÄSITTELY HALLINNOLLISELLA ALUEELLA

Tiedon käsittelyyn käytettävän tietojärjestelmän tai tietoliikennejärjestelyn tulee olla kyseisen turvallisuusluokan mukaisesti suojattu. Esimerkiksi turvallisuusluokan III mukaisesti suojattu päätelaite voidaan tuoda hallinnolliselle alueelle tai sen ulkopuolelle, josta päätelaite ottaa turvallisuusluokan III mukaisella liikennesalauksella suojatun yhteyden turva-alueella sijaitsevaan turvallisuusluokan III tietovarantoon tietojen käsittelyn ajaksi. Päätelaitetta ei voi jättää ilman valvontaa hallinnolliselle alueelle, vaan se tulee palauttaa käsittelyn jälkeen säilytettäväksi turva-alueelle, ellei päätelaitteen luottamuksellisuudesta, eheydestä ja käytettävyydestä pystytä muuten varmistumaan (vrt. luku 5 alla). Turvallisuusluokkien III tai II kiinteää tietoverkkoa ei voi ulottaa hallinnolliselle alueelle.

5. TURVALLISUUSLUOKKIEN IV TAI III TIETOJEN KÄSITTELY JA SÄILYTTÄMINEN PÄÄTELAITTEESSA
Tilanteissa, joissa turvallisuusluokan IV tai III tietoa käsitellään ja säilytetään kyseisen turvallisuusluokan mukaisessa päätelaitteessa turvallisuusalueiden ulkopuolella, tai turvallisuusluokan III tietoja hallinnollisella alueella, päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja erityisesti päätelaitteen kyseiselle turvallisuusluokalle riittävästä eheydestä tulee huolehtia.

Päätelaitteen eheys tulee pystyä varmistamaan riittävällä tasolla, jotta tiedon luottamuksellisuus ei vaarannu päätelaitteen eheyden menetyksen seurauksena. Tyypillisin tapa eheydestä varmistumiseen on päätelaitteen suojaaminen turvallisuusalueiden fyysisen pääsynhallinnan menettelyin, mukaan lukien esimerkiksi kaikki tietojärjestelmään liittyvät fyysiset palvelimet, verkkolaitteet, päätelaitteet sekä esimerkiksi kaapeloinnit. Esimerkiksi turvallisuusluokan IV tietojärjestelmän eheyden suojaamisessa yleisiä turvallisuusluokiteltuun tietoon kohdistuvia riskejä vastaan voi riittää tietojärjestelmän tietovarantojen sijoittaminen hallinnolliselle tai turva-alueelle, sekä riittävällä salauksella varustettujen päätelaitteiden osalta myös rajattu säilytys muussa lukittavassa tilassa, esimerkiksi virkamiehen kotona.

Turvallisuusluokan III tietojärjestelmät tulisi kokonaisuudessaan sijoittaa turva-alueelle. Mikäli turvallisuusluokan III tietojen käsittelyyn käytettävää päätelaitetta joudutaan säilyttämään hallinnollisella alueella tai jopa turvallisuusalueiden ulkopuolella, voidaan fyysisen pääsynhallinnan tuoman eheyssuojauksen puuttumista pyrkiä riskiperustaisesti kompensoimaan esimerkiksi päätelaitteen sijoittamisella luvattoman pääsyn paljastavaan koteloon tai pakkaukseen. Kaupallisesti on saatavilla esimerkiksi niin sanottuja turvasalkkuja, jotka pyrkivät havaitsemaan salkun sisältöön kohdistuvat luvattomat pääsy-yritykset siten, että luvattomasta pääsystä tuotetaan ilmoitus päätelaitteen luvalliselle käyttäjälle tai käyttäjän organisaatiolle, tai/ja että pääsystä jää jälki kyseiseen koteloon tai pakkaukseen.

Viranomaisten tulee riskienarvioinnissaan kuitenkin huomioida, että turvallisuusalueiden ulkopuolella toimiessa sekä turvallisuusluokiteltuun tietoon, että sen käsittelyyn käytettäviin päätelaitteisiin kohdistuu erityisesti turvallisuusluokasta III lähtien riskejä, joiden riittävä pienentäminen voi olla useissa käyttötapauksissa erittäin haastavaa, ellei jopa mahdotonta. Käsittelyssä tulee huomioida lisäksi salakatselulta ja -kuuntelulta suojautuminen, sekä riskipohjaisesti myös esimerkiksi hajasäteilyriskejä vastaan suojautuminen. Turvallisuusluokan III päätelaitteen säilyttämisessä on otettava huomioon myös

kansainväliset tietoturvavelvoitteet, joissa turva-alueen ulkopuolinen säilyttäminen voi olla kokonaan kielletty.

PAPERIASIAKIRJOJEN KÄSITTELY	
TURVALLISUUDEN OSA-ALUE	VÄHIMMÄISVAATIMUS
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon.
Salaa katselun vastatoimenpiteet	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet tällaisen riskin hallitsemiseksi
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi Käsittelyalue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta

TIEDON KÄSITTELY SÄHKÖISESTI	
TURVALLISUUDEN OSA-ALUE	VÄHIMMÄISVAATIMUS
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon.
Salaa katselun vastatoimenpiteet	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet tällaisen riskin hallitsemiseksi
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään jollakin alueella, jolla tietoja käsitellään, käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi

	Käsittelyalue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta
Tempest-riskit (ainoastaan TL I - III)	Käsiteltäessä sähköisessä muodossa tietoja, jotka kuuluvat LUOTTAMUKSELLINEN- tai sitä korkeampaan turvallisuusluokkaan, on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi.

TIEDON KÄSITTELY SUULLISESTI	
TURVALLISUUDEN OSA-ALUE	VÄHIMMÄISVAATIMUS
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos sivulliset henkilöt eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon. Äänieristyksen osalta tulee huomioida, että myös alueen sisällä voi työskennellä henkilöitä, joilla ei ole tiedonsaantitarvetta keskusteltavaan tietoon
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Käsittelyalueella on oltava tunkeutumisen ilmaisujärjestelmä ja alue on pidettävä lukittuna silloin, kun sitä ei käytetä Käsittelyalueelle tulevia henkilöitä ja aineistoja on valvottava Käsittelyalue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta Käsittelyalueella ei saa olla luvattomia tietoliikenneyhteyksiä, luvattomia puhelimia eikä muita luvattomia viestintävälineitä eikä elektronisia laitteita. Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi