

VALTIONHALLINNON TIETOAINESTOJEN KÄSITTELYN TIETOTURVALLISUUSOHJE

SISÄLLYSLUETTELO

1 YLEISTÄ	5
1.1 Ohjeen tarkoitus ja rajaus	5
1.2 Ohjeen valmistelusta	6
1.3 Viranomaisia koskevat tietoturvallisuusvelvoitteet	6
2 TIETOAINEISTOJEN TURVALUOKITTELU JA MERKINNÄT	7
3 TIETOAINEISTOJEN KÄSITTELYN TIETOTURVALLISUUSVAATIMUKSET	9
3.1 Käsittelylle asetettavat vaatimukset	9
3.2 Asian vireille tulo sekä asiakirjan ja tietojen luokittelu ja merkintä	10
3.3 Asiakirjan ja tietojen jakelu, luovutus, tulostus ja vastaanotto	12
3.4 Asiakirjan ja tietojen käsittely, säilytys ja arkistointi	15
3.5 Asiakirjan hävittäminen ja käytöstä poistaminen	18
4 KÄSITTELYN EHEYDELLE JA KÄYTETTÄVYYDELLE ASETETTAVAT VAATIMUKSET	19
LIITE 1: TIETOAINEISTOJEN KÄSITTELYN LÄHTÖKOHTIA VALTIONHALLINNOSSA	21
LIITE 2: SALASSA PIDETTÄVIEN TIETOJEN JA ASIAKIRJOJEN TURVALUOKITTELU- JA MERKINTÄOHJE	24
Liite 2.1: Asiakirjojen ja tietojen luokittelun käsitteitä	28
Liite 2.2: Salassa pidettävien asiakirjojen leimat	29
LIITE 3: Ohjeen rajaus	30

Sisältöalue

Valtionhallinnon asiakirjat

Säännökset, joihin ohjeen antamisen toimivalta perustuu

VNOS (1522/1995, muut. 8566/27.8.1999)
19§:n 19 kohta

Kohderyhmät

Ministeriöt, virastot ja laitokset

Voimassaoloaika

Toistaiseksi

VALTIONHALLINNON TIETOAINEISTOJEN KÄSITTELYN TIETOTURVALLISUUSOHJE

1 YLEISTÄ

1.1 OHJEEN TARKOITUS JA RAJAUS

Ohjeen tarkoituksena on parantaa ministeriöiden, virastojen ja laitosten tietoaineistojen käsittelyn elinkaaren eri vaiheiden tietoturvallisuutta sekä määritellä asiakirjojen luokittelun pohjalta yhteneviä käsittelyperiaatteita.

Tietoaineistoilla tarkoitetaan tässä ohjeessa paperilla, sähköisillä tai muilla tietovälineillä olevia asiakirjoja ja tietoja. Asiakirjoilla tarkoitetaan viranomaisen toiminnan julkisuudesta annetun lain (621/1999, jatkossa JulkL) 5 §:ssä määriteltyä asiakirjoja. Ohje on tarkoitettu erityisesti paperi- ja tiedostotyyppisten aineistojen käsittelyohjeeksi, mutta sitä voidaan hyödyntää myös muunmuotoisen aineiston käsittelyohjeena (esim. tietokanta, varmuuskopiot, sähköpostiviestit, digitaalinen kuva jne.).

Ohjeeseen sisältyy linjaukset asiakirjojen ja tietojen luokittelusta ja suojaamisesta sekä käsittelyn elinkaaren eri vaiheiden turvallisuusvaatimuksista ja suositeltavista käytännöistä. Ohjeessa määritellään hyvän tiedonhallintatavan ja tietoturvallisuuden varmistamistarpeiden mukaiset tietojen luokituskäytännöt erityisesti luottamuksellisuuden osalta sekä tähän luokitteluun perustuvat tietojen käsittelyohjeet. Lisäksi on määritelty yleisesti eheyteen ja käytettävyyteen liittyviä vaatimuksia (luku 4).

Ohjeessa määritellään tietojen ja asiakirjojen tietoturvallisuusvaatimuksia sekä manuaalisen että sähköisen käsittelyprosessin eri vaiheissa, joita ovat mm. luonti, jakelu, käsittely ja hävittäminen. Valtiovarainministeriön 19.1.2000 antamassa ohjeessa "Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje" (VM 5/01/2000, liitteenä) on määritelty turvaluokittelun ja merkintöjen käytäntöjä luottamuksellisuuden osalta. Tässä ohjeessa käytetään lähtökohtana ko. ohjeen määrityksiä. **Tietoturvallisuusvaatimukset määritellään luvussa 3.**

JulkL sekä sen perusteella annettu asetus (1030/1999, jäljempänä JulkA) tulivat voimaan 1.12.1999. Tämä ohje täydentää JulkA:n sääntelyä. Esimerkiksi JulkA 3 §:ssä on määritelty suojattavia tietoai-

neistoja koskevat yleiset, minimitason turvallisuustoimenpiteet. Aineistojen käsittelyä koskevat vaatimukset kohdistuvat tiedon koko elinkaareen.

Ohjeessa on otettu huomioon erityisesti asianhallinta-tyyppinen asiantuntijatyö, jossa käsitellään paperisia ja sähköisiä asiakirjoja. Ohjetta suositellaan käytettäväksi soveltuvin osin myös vakio-
muotoisessa tietojärjestelmien ja tietokantojen hyväksikäyttöön perustuvassa tiedonkäsittelyssä.

Ohjeen turvaluokittelu koskee erityisesti JulkL voimaantulon jälkeen laadittuja asiakirjoja, mutta sitä suositellaan käytettäväksi viranomaisen harkinnan mukaan valikoiden myös ennen JulkL voimaantuloa laadittuihin asiakirjoihin.

Tämä ohje on yleisluontoinen, joten ministeriöt antanevat tarvittaessa hallinnonalaansa koskevia täsmennyksiä tämän ohjeen pohjalta. Tämän ohjeen ja mahdollisesti hallinnonalakohtaisten täsmennysten pohjalta tehtävä organisaatiokohtainen ohje voidaan teknisesti liittää osaksi tietojenkäsittelyn turvaamissuunnitelmaa. Kukin organisaatio tarkentaa vaatimuksia omassa ohjeistuksessaan toiminnan tarpeiden ja tietoturvallisuusvaatimusten perusteella. Yksityiskohtaisemmat ohjeet näkyvät lopulta mm. tietojärjestelmien kuvauksissa, käyttöohjeissa ja arkistonmuodostussuunnitelmassa. Ministeriön, viraston ja laitoksen tulee huolehtia henkilöstön perehdyttämisestä tietoaineiston käsittelyn ohjeistukseen.

Asiakirjojen sisällön, luokittelun ja käsittelyn virastokohtainen arviointi on tarpeen tietoturvallisuuden varmistamiseksi osana toiminnan sekä sen laadun ja jatkuvuuden varmistamista. Tätä ohjetta on syytä käyttää ko. arvioinnin tukena.

Liitteessä 3 on listattu asiakokonaisuuksia, joita ohjeeseen ei sisälly ja joilla on liittymiä ohjeeseen.

1.2 OHJEEN VALMISTELUSTA

Ohje on valmisteltu valtionhallinnon tietoturvallisuuden johtoryhmän alkuvuodesta 1999 asettamassa jaostossa, jossa on ollut edustus valtioneuvoston kansliasta, oikeusministeriöstä, sisäasiainministeriöstä, valtiovarainministeriöstä, liikenneministeriöstä, tietosuojavaltuutetun toimistosta, Ilmailulaitoksesta ja Suomen Kuntaliitosta.

Ohjeen luonnos oli jaoston valmistelutyön jälkeen koko valtionhallinnon kattaneella lausuntokierroksella touko-kesäkuussa 2000. Lausuntoja saatiin 42 ja ne on otettu huomioon ohjeessa.

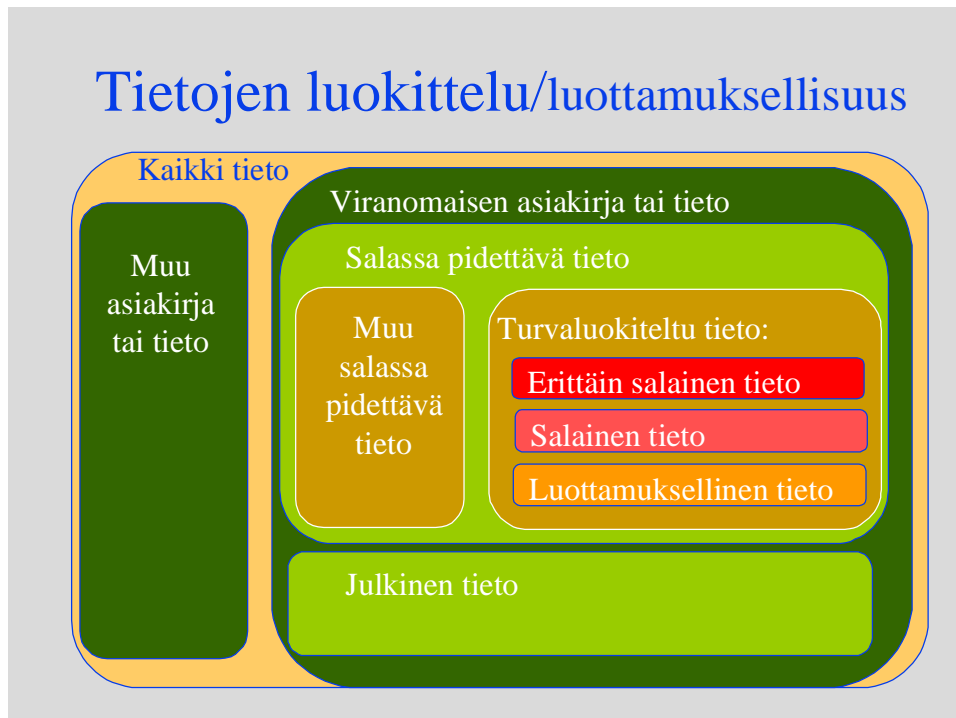
Valtiovarainministeriö on myös antanut suosituksen julkisuuslain vaatiman tietojärjestelmäselosteen laatimiseksi (VM 7/01/2000), joka on otettu huomioon tässä ohjeessa.

1.3 VIRANOMAISIA KOSKEVAT TIETOTURVALLISUUSVELVOITTEET

Useat lait, asetukset sekä määräykset ja ohjeet sisältävät viranomaisia koskevia tietoturvallisuusvelvoitteita. Näitä on esitetty liitteessä 1, jossa on myös tarkemmin kerrottu lainsäädännöstä tietoa-
neistojen käsittelyn lähtökohtana. Velvoitteiden täyttämiseksi keskeistä on tietoa-
neistojen turvaluokittelu ja käsittelyn tietoturvallisuudesta huolehtiminen turvaluokalle asetettujen tietoturval-
lisuusvaatimusten mukaisesti.

2 TIETOAINEISTOJEN TURVALUOKITTELU JA MERKINNÄT

Valtiovarainministeriö antoi salassa pidettävien tietojen ja asiakirjojen turvaluokittelua ja merkintää koskevan ohjeen (VM 5/01/2000), joka on tämän ohjeen liitteenä 2. Oheisessa kuvassa on esitettynä kyseisen ohjeen mukainen tietojen luokittelu luottamuksellisuuden suhteen:



Ohjeen mukaan salassa pidettävät asiakirjat voidaan jakaa turvaluokiteltaviin ja muihin salassa pidettäviin tietoihin tai asiakirjoihin. Ohjeen mukaan asiakirja on turvaluokiteltava asiakirja silloin, kun se on JulKL 24.1 §:n 1, 2, 5, 7, 8, 9, 10 tai 11 kohtien mukaan salassa pidettävä. Tällaiset asiakirjat käsittelevät yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi arkaluonteista, salassa pidettävää tietoa.

Ohjeen mukaan I turvaluokkaan kuuluvat asiakirjat varustetaan leimalla tai merkinnällä ”Erittäin salainen”, II turvaluokan asiakirjat varustetaan merkinnällä ”Salainen” ja III turvaluokan asiakirjat merkinnällä ”Luottamuksellinen”.

Ohjeen mukaan tiedoille tai asiakirjoille, joka on JulKL 24.1 §:n jonkun muulle kuin edellä mainitun säännöksen (24.1 §:n kohdat 1, 2, 5, 7, 8, 9, 10 tai 11) perusteella salassa pidettävä, ei suositella turvaluokittelua. Tällainen tieto tai asiakirja varustetaan ensimmäisen sivun ylälaitaan sijoitettavalla leimalla ”Salassa pidettävä” ja sitä saavat käsitellä vain tehtävissään kyseisen asiakirjan tietoja tarvitsevat henkilöt. Huomattava osa eräiden hallinnonalojen (esim. opetushallinto ja sosiaali- ja terveyssektori) tiedoista ja asiakirjoista kuuluu tähän ryhmään. Koska muut salassa pidettävät asiakirjat ja tiedot voivat olla organisaatioittain hyvinkin eri tyyppisiä, on organisaatiokohtaisten, tarkentavien ohjeiden tekeminen erityisen tärkeää näiden tietojen ja asiakirjojen osalta. **Muille salassa pidettäville asiakirjoille suositellaan pääsääntöisesti III turvaluokan käsittelysääntöjen soveltamista.** Salassa pidettävien henkilötietojen käsittelyssä on usein tarpeellista soveltaa II turvaluokan käsittelysääntöjä.

3 TIETOAINEISTOJEN KÄSITTELYN TIETOTURVALLISUUSVAATIMUKSET

3.1 KÄSITTELYLLE ASETETTAVAT VAATIMUKSET

Tässä luvussa annetaan **salassa pidettäviä asiakirjoja koskevat käsittelyohjeet**. Ohjeet vastaavat valtiovarainministeriön ohjeessa 5/01/2000 ("Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje 19.1.2000) määriteltyjä periaatteita. Asiakirja turvaluokitellaan silloin, kun se on määrätty pidettäväksi salassa JulkL:n 24.1 §:n kohtien 1, 2, 5, 7, 8, 9, 10 tai 11 perusteella.

Kaikki turvaluokitellut ja muut salassa pidettävät asiakirjat ja tiedot on pidettävä salassa eikä niiden sisältämiä salassa pidettäviä tietoja saa antaa sivullisten käyttöön. Kyseisten asiakirjojen eri turvaluokkien mukaiset käsittelyvaatimukset riippuvat asiakirjojen sisältämien tietojen paljastumisen aiheuttaman uhan merkittävydestä yhteiskunnalle tai sille kohteelle, jonka etujen suojaamiseksi asiakirja on säädetty salassa pidettäväksi .

Jäljempänä on käsittelyvaatimukset esitetty siten, että kaikkien turvaluokkien perusvaatimukset on esitetty III turvaluokan (luottamuksellinen) kohdalla. II turvaluokan (salainen) kohdalla on esitetty perusvaatimuksien lisäksi toteutettavat toimenpiteet tai tarkennettu perusvaatimuksien sisältöä. Vastaavasti I turvaluokan (erittäin salainen) kohdalla on lisätty tai tarkennettu aiempien turvaluokkien vaatimuksia.

Muiden kuin turvaluokiteltujen salassa pidettävien asiakirjojen osalta suositellaan noudatettavaksi pääsääntöisesti III turvaluokalle asetettuja käsittelyvaatimuksia. Myös pääosa salassa pidettävistä EU-asiakirjoista tulee käsitellä III turvaluokan käsittelyvaatimusten mukaisesti. Salassa pidettävien henkilötietojen osalta on noudatettava vähintään III turvaluokan käsittelyvaatimuksia. Muiden kuin turvaluokiteltujen salassa pidettävien asiakirjojen käsittelyssä voidaan tarpeen mukaan soveltaa II turvaluokan käsittelyvaatimuksia .

Turvaluokiteltujen asiakirjojen käsittelyvaatimukset esitetään asiakirjan elinkaaren seuraaville neljälle pääasialliselle käsittelyvaiheelle:

- asian vireille tulo ja asiakirjan luokittelu ja merkintä
- asiakirjan jakelu, luovutus, tulostus ja vastaanotto
- asiakirjan käsittely, säilytys ja arkistointi
- asiakirjan hävittäminen ja käytöstä poistaminen

Eräillä hallinnonaloilla on tarpeita käyttää em. mainittujen turvaluokkien lisäksi salassa pidettävissä aineistoissa turvaluokkaa IV (viranomaiskäyttö). Tähän turvaluokkaan kirjattavalle aineistolle on tyypillistä laaja käsittelytarve, korkea käytettävyys, soveltuvuus päivittäiseen työskentelyyn ja tiedon paljastumisen aiheuttama vähäinen vahinko salassa pidon perusteena olevalle asialle. Tässä ohjeessa ei kuvata tämän, valtionhallinnossa joillakin hallinnonaloilla käytössä olevan turvaluokan tietoturvallisuusvaatimuksia, jotka on mahdollista viranomaisessa määritellä valikoiden III turvaluokan käsittelyvaatimuksista.

3.2 ASIAN VIREILLE TULO SEKÄ ASIAKIRJAN JA TIETOJEN LUOKITTELU JA MERKINTÄ

Asia voi tulla vireille joko ulkopuolisen toimesta tai viranomaisen omasta aloitteesta. Asian tultua vireille vastuullinen viranomainen pääsääntöisesti kokoaa eri lähteistä asiaan liittyvää tietoa ja muodostaa hallussaan olevien tietojen perusteella asiakirjan tai tallentaa tiedot käytössään oleviin tietokantoihin.

Asiakirjan ja tietojen turvaluokka arvioidaan sen mukaan, millaista vahinkoa suojattavalle kohteelle saattaisi aiheutua salassa pidettävien tietojen joutumisesta sivullisten haltuun. Asiakirjan turvaluokan määrittelee ja vahvistaa henkilö, jolle asianomainen viranomainen on kyseisen oikeuden luovuttanut. Tiedon omistajien tulee luokitella olemassa oleva ja tuleva tieto tämän ohjeen tai viranomaisen antaman tarkennetun ohjeen perusteella eri luottamuksellisuusluokkiin. Tiedot luokittelee se henkilö, joka antaa asiaan liittyvän toimeksiannon tai ensimmäisen kerran luo tiedot.

Keskeistä on tiedon omistajan vastuu tiedoista. **Omistaja on viranomaisessa tyypillisesti se henkilö, jolla on oikeus päättää kyseisen aineiston käsittelystä ja käytöstä.** Viranomaisen tulisi määritellä kaikille tietoaaineistoilleen ja järjestelmilleen omistajat. Merkintöjä, kuten leimat ja vinoviivat, voidaan toteuttaa valmiiksi esim. sähköisiin asiakirja- ja lomakepohjiin. Turvaluokka tulee tiedostaa koko tietoaaineiston elinkaaren ajan.

- **Yleiset vaatimukset kaikille salassa pidettäville tietoaaineistoille** (Koskevat III turvaluokkaa "luottamuksellinen", II turvaluokkaa, I turvaluokkaa, muita salassa pidettäviä kuten salassa pidettävät EU-asiakirjat ja henkilötiedot)
 - Kerättäessä ja luovutettaessa tietoaaineistoa sekä valmisteltaessa ja luotaessa asiakirjaa on otettava huomioon asiakirjan julkisuudesta ja salassa pidosta säädetty normit sekä niiden käsittelystä annetut ohjeet (kts. luku 1.3 ja liite 1). Se edellyttää muun muassa aineiston luottamuksellisuuden arviointia. Samalla on määriteltävä aineiston käsittelyn eri vaiheille ja muodoille asetettavat vaatimukset sekä suunniteltava näiden toteuttaminen. Asiakirja ja tieto tulee luokitella sellaiseen turvaluokkaan, jonka käsittelysäännöt tukevat ko. aineiston tietoturvatarpeita.
 - Mikäli samassa tietojärjestelmässä on sekä julkisiksi että turvaluokitelluiksi määriteltyjä kenttiä, on järjestelmässä luokittelu tehtävä kenttäkohtaisesti. Kenttäkohtaiset merkinnät voidaan määritellä tietojärjestelmän käsittelysääntöihin.
 - Mikäli tietty kenttä voi tietojärjestelmässä sisältää joko julkista tai salaista tietoa, on jokaiselle yksittäiselle tiedolle oltava luokittelutieto, joka täytetään tallennettaessa.
 - Mikäli samassa asiakirjassa on sekä julkista että salassa pidettävää tietoa, tulee erityisesti hallinnollisten asiakirjojen osalta julkiset ja salassa pidettävät osat kyetä erottelemaan toisistaan.
 - Viranomaisella on oltava periaatteet tietoaaineistojen omistajuudesta ja luokittelumerkinnöistä sekä niihin liittyvistä vastuista. Asiakirjan laadintaan ja tietojen tallennukseen sekä siihen liittyvien tietojen käsittelemiseen voivat osallistua henkilöt, joilla on siihen asianmukainen valtuutus.
 - **Turvaluokiteltu asiakirja merkitään salassa pidettävien tietojen ja asiakirjojen luokittelua ja merkintää koskevan ohjeen (VM5/01/2000) mukaan** siten, että sitä vastaanottava, laativa tai käsittelevä henkilö tietää, millä tavalla kyseistä aineistoa on käsiteltävä ja

- säilytettävä. Merkinnän tekee aineiston laatija, ensimmäinen vastaanottaja tai se, jolla on oikeus päättää kyseisen aineiston käsittelystä ja käytöstä (jäljempänä ”omistaja”). Turvaluokittelun vahvistaa asiakirjan allekirjoittaja/vahvistaja/ laatija joko manuaalisella tai sähköisellä allekirjoituksellaan.
- Asiakirjan turvaluokka ilmaistaan asiakirjan metatietorakenteessa esim. dokumenttien hallintajärjestelmässä.
 - Turvaluokkamerkintä tulee tehdä kaikkiin turvaluokiteltuihin asiakirjoihin. Muihin salassa pidettäviin aineistoihin salassapitomerkinän tarve harkitaan virastossa: pääsääntöisesti sitä suositellaan tehtäväksi.
 - **III turvaluokan asiakirja** sisältää salassa pidettävää tietoa. Turvaluokan osoittava merkintä tehdään asiakirjan etusivun oikeaan yläkulmaan punaisella leimalla tai sähköisesti aineiston ensimmäiselle sivulle.
 - Asiakirjan sivut on numeroitava.
- **Lisävaatimuksia II turvaluokalle (salainen) ja I turvaluokalle (erittäin salainen) ja erälle salassa pidettäville henkilötiedoille**
- Asiakirjan laadintaan, tietojen tallennukseen ja käsittelyyn voi osallistua henkilö, joka on nimetty kyseistä asiaa hoitamaan.
 - Asiakirjat kirjataan salaiseen diaariin.
 - **II turvaluokan asiakirja** sisältää erittäin arkaluonteista, salassa pidettävää tietoa.
 - Paperimuotoisen asiakirjan turvaluokka merkitään vinosti arkin halki kulkevalla punaisella viivalla ja ensimmäisen sivun ylälaitaan sijoitettavalla punaisella turvaluokan osoittavalla leimalla tai merkinnällä (tarkemmin VM:n ohje 5/01/2000).
 - Sähköisessä muodossa olevassa asiakirjassa on turvaluokkaa osoittavan merkinnän oltava jatkuvasti näkyvissä.
 - Jokaiselle sivulle on merkittävä asiakirjan kokonaissivumäärä.
 - Aineiston omistaja on kerrottava ellei se ilmene asiakirjan allekirjoituksesta.
- **Lisävaatimuksia I turvaluokalle (erittäin salainen)**
- Asiakirjan laadintaan, tietojen tallennukseen ja käsittelyyn voi osallistua vain henkilö, jolla on viranomaisen johdon valtuutus kyseisen asian käsittelyyn.
 - **I turvaluokan asiakirja** sisältää äärimmäisen arkaluonteista, salassa pidettävää tietoa.
 - Turvaluokan osoittava merkintä tehdään sekä manuaalisessa että sähköisessä muodossa joka sivulle. Paperimuotoisen asiakirjan turvaluokka merkitään vinosti arkin halki kulkevalla punaisella viivalla ja jokaisen sivun ylälaitaan sijoitettavalla punaisella turvaluokan osoittavalla leimalla tai merkinnällä (tarkemmin VM:n ohje 5/01/2000).
 - Laaditut asiakirjan kopiot ja kaksoiskappaleet on numeroitava.
 - Erittäin salaiset tiedot on tarkoitettu vain erikseen nimetyille henkilöille.
 - Kullakin asiakirjan kopiolla on oltava nimetty haltija.
 - Aineiston omistaja on aina kerrottava.
 - Turvaluokkaan "erittäin salainen" tulee pääasiassa kirjata vain sellaista tietoa, jota ei tarvita päivittäisessä käytössä.

3.3 ASIAKIRJAN JA TIETOJEN JAKELU, LUOVUTUS, TULOSTUS JA VASTAANOTTO

Asiakirjan laadinnan yhteydessä määritetään, kuka päättää asiakirjan jakelusta sekä kenelle ja millä tavalla asiakirja jaetaan ja mitä vaatimuksia jakelulle asetetaan. Asiakirja jaetaan valvotusti näiden periaatteiden mukaisesti.

Kun asiakirja luovutetaan vastaanottajalle, se siirtyy tietosisältöineen vastaanottajan hallintaan kaikkine siihen liitettyine käsittely- ja käyttöoikeuksineen sekä -velvollisuuksineen.

Asiakirja siirretään sähköisesti tai kuljetetaan manuaalisesti aineiston hallintaan, käsittelyyn ja käyttöön oikeutetulta osapuolelta vastaavat oikeudet omaavalle toiselle osapuolelle.

Laadittu sähköinen asiakirja tulostetaan paperimuotoiseksi ja sähköinen tai paperimuotoinen asiakirja monistetaan alkuperäisen asiakirjan kanssa identtiseksi.

- **Yleiset vaatimukset kaikille salassa pidettäville tietoaineistoille** (Koskevat III turvaluokkaa "luottamuksellinen", II turvaluokkaa, I turvaluokkaa, muita salassa pidettäviä kuten salassa pidettävät EU-asiakirjat ja henkilötiedot)
 - Turvaluokiteltu asiakirja tulee jakaa siten, että asiattomat eivät pääse käsiinsä salassa pidettävään tietoon. Turvaluokiteltu asiakirja jaetaan omistajan merkinnän yhteydessä tekemän jakeluluettelon mukaan. Asiakirjasta on pääsääntöisesti käytävä ilmi, kenelle aineistoa saa jakaa ja mitä vaatimuksia asetetaan jakelutavalle ja -muodolle.
 - Manuaalisen ja sähköisen asiakirjan vastaanotto/luovutus on dokumentoitava.
 - Tietojärjestelmissä tietojen jakelu hoidetaan käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä.
 - Vastaanottaja on määriteltävä asiakirjassa henkilön, tehtävän tai organisaation tarkkuudella.
 - Manuaalisesti jaettaessa tulee käyttää läpinäkymätöntä kirjekuorta.
 - Sähköisesti jaettaessa on huolehdittava siitä, ettei asiakirjan sisältämiä tietoja joudu sivullisten haltuun (esim. asiakirjan riittävän salauksen avulla). Tietoja ei saa siirtää selväkielisinä yleisissä tietoverkoissa. Sähköpostia käytettäessä on varmistauduttava vastaanottajan osoitteesta.
 - Vastaanottaja voi päättää jakelun laajentamisesta lainsäädännön puitteissa.
 - Viranomaisen on varmistettava, että luokitellun asiakirjan saa luovuttaa ja ottaa vastaan ainoastaan sellainen henkilö, jolla tehtäviinsä liittyen on siihen oikeus. Tämän tulee tapahtua siten, että salassa pidettävä tieto ei paljastu asiattomille. Luokitellun asiakirjan luovuttajan ja vastaavasti vastaanottajan on varmistettava, että toisella osapuolella on oikeus ottaa vastaan ja luovuttaa kyseinen asiakirja. Noudatettavasta menettelystä on viranomaisen annettava sisäiset ohjeet.
 - Valtionhallinnon yksikkö voi luovuttaa luottamuksellisen aineiston sellaiselle yhteistyökumppanille, jonka kanssa yksiköllä on voimassa tietojen käsitteä koskeva turvallisuussopimus ja asianomainen on allekirjoittanut yksikön määrittelemän vaitiolositoumuksen. Turvallisuussopimus ei saa olla ristiriidassa lainsäädännön kanssa.

- Jos viranomaiselta pyydetään tietoa turvaluokitellusta asiakirjasta, joka on toisen viranomaisen laatima, viranomaisen tulee JulkL 15§:een vedoten siirtää luovutuspyynnön ratkaisu asiakirjan laatineelle viranomaiselle.
- Kun luokiteltua asiakirjaa kuljetetaan ja siirretään on huolehdittava siitä, että salassa pidettävä tieto ei paljastu asiattomille. Tällaista asiakirjaa saa kuljettaa ja siirtää vain henkilö, jolla on tähän oikeus ja vain riittävän turvallisuustavalla. Luokitellun asiakirjan kuljetusta ja siirtoa on valvottava.
- Asiakirja osoitetaan henkilölle, määrättyä tehtävää hoitavalle tai organisaatiolle.
- Asiakirjan sisältämistä tiedoista voidaan rajoitetusti puhua puhelimesta, kun toinen osapuoli on tunnistettu.
- Telefaksia voidaan asiakirjan siirtämiseen käyttää vain poikkeustapauksissa ja tällöin on vastaanoton tapahduttava valvotusti. Suositeltavaa on käyttää salaavia fax-laitteita.
- Kun salassa pidettävää asiakirjaa tulostetaan tai monistetaan, on huolehdittava siitä, etteivät asiattomat pääse käsiksi salassa pidettävään tietoon. Luokiteltua asiakirjaa saa monistaa vain sellainen henkilö, jonka viranomaisen on tehtävään valtuuttanut. Tulostimien sijoittelussa tulee ottaa huomioon mahdollinen tarve tulostaa turvaluokiteltuja ja muita salassa pidettäviä aineistoja.
- Sähköistä tietovälinettä (kuten levyke) käsiteltäessä sovelletaan siihen samoja vaatimuksia kuin manuaalisen asiakirjan käsittelyyn.
- Asiakirjan kopiassa on oltava samanlaiset luokittelumerkinnot kuin alkuperäisessä asiakirjassa. Merkintöjen väri voi kuitenkin olla mustavalkoinen, jolloin samalla ilmenee, ettei kysymys ole alkuperäisestä asiakirjasta.
- Kopiota on käsiteltävä ja säilytettävä kuten alkuperäistä asiakirjaa.
- Jos henkilön oikeus aineiston käsittelyyn poistuu, on kaikki hänen hallussaan olevat kopiot hävitettävä.
- **Lisävaatimuksia II turvaluokalle (salainen) ja I turvaluokalle (erittäin salainen) ja erälle salassa pidettäville henkilötiedoille**
 - Vastaanottaja on määriteltävä asiakirjassa henkilön tai organisaation tarkkuudella.
 - Asiakirjaa ei saa jakaa yhdessä julkisen aineiston kanssa.
 - Manuaalisesti jaettaessa varmistettava, ettei tekstiä voida lukea kirjekuoren läpi. Käytettävä esim. mustaa sisäkuorta suljetun kuoren sisällä.
 - Manuaalisesti jaettaessa käytettävä lähettiä tai kirjattua postia.
 - Sähköisesti jaettaessa asiakirja on aina salattava.
 - Sähköisesti jaettaessa on käytettävä menettelyä, joka tarkistaa vastaanottajan ja takaa lukukuittauksen.
 - Suositellaan, että vastaanottaja kuittaa saaneensa aineiston.
 - Asiakirjasta ei saa antaa tietoja ulkopuolisille ilman tiedon omistajan lupaa.
 - Asiakirjan saa luovuttaa ja ottaa vastaan viranomaisen nimeämä henkilö, jolla on tehtäviinsä liittyen siihen oikeus.
 - Sähköisen aineiston käsittelijä on tunnistettava luotettavasti (esimerkiksi ns. vahvan tunnistuksen käyttö on suositeltavaa).
 - Manuaalisen asiakirjan luovutus ja vastaanotto on kirjattava ja kuitattava.

- Sähköisen asiakirjan vastaanotto on kirjattava ja sen oikeellisuus on varmistettava.
- Asiakirjan sisältämistä tiedoista voidaan puhua puhelimesta, kun toinen osapuoli on luotettavasti tunnistettu ja vain siten, ettei salainen tietosisältö puheessa paljastu mahdolliselle kuuntelijalle.
- Asiakirjaa saa monistaa vain viranomaisen siihen erikseen valtuuttama henkilö. Asiakirjan asiaton kopiointi ja tulostaminen on kiellettyä.
- Kopioiden määrä, päivämäärä ja jakelu tulee kirjata.
- Kopia on käsiteltävä kuten alkuperäistä asiakirjaa.
- Sähköisen asiakirjan tulostaminen suositellaan tehtäväksi vain suoraan työasemaan liitettyllä tulostimella.
- Asiakirja ja sen kopiot tulostetaan ja monistetaan paperille, jonka poikki kulkee punainen vinoviiva vasemmalta alas oikealle ja jossa on ensimmäisen sivun yläalareunassa punainen turvaluokan osoittava leima tai merkintä (tarkemmin VM:n ohje 5/01/2000).
- Asiakirjan ja tietojen tulostamisesta tulee pitää lokitietoja.
- Asiakirja ei saa olla matkalla viikonlopun yli.

- **Lisävaatimuksia I turvaluokalle (erittäin salainen)**
 - Jakelun saa kohdistaa ainoastaan nimetyille henkilöille.
 - Vastaanottajan on aina kuitattava lähetys saaduksi. Kuittauksesta on ilmentävä lähetyksen vastaanottaja sekä vastaanoton tarkka aika.
 - Asiakirjaa ei saa jakaa muun aineiston kanssa.
 - Asiakirjaa ei saa jakaa, luovuttaa eikä siirtää sähköisessä muodossa.
 - Jakelun mahdollisesta muutoksesta päättää aina asiakirjan omistaja.
 - Asiakirjan vastaanottaja ei saa luovuttaa oikeuksiaan kenellekään, koska asiakirja on tarkoitettu ainoastaan nimetyille henkilöille.
 - Oikeudet vastaanottoon ja luovutukseen on varmistettava.
 - Manuaalinen asiakirja kuljetetaan luotettavan lähetin avulla.
 - Kirjatussa postissa voidaan asiakirja lähettää vain perustelluissa poikkeustapauksissa.
 - Asiakirjan sisältämiä tietoja ei saa käsitellä puhelimesta eikä telefaksin välityksellä.
 - Omistaja kontrolloi kuljetusta, kopiointia ja kopioiden käsittelyä.
 - Numeroitua ja vastaanottajan nimellä varustettua kopiota käsitellään kuten alkuperäistä.
 - Sähköisen asiakirjan saa tulostaa vain suoraan työasemaan liitettyllä tulostimella.
 - Asiakirja ja sen kopiot tulostetaan ja monistetaan paperille, jonka poikki kulkee punainen vinoviiva vasemmalta alas oikealle ja jossa on jokaisen sivun yläalareunassa punainen turvaluokan osoittava leima tai merkintä (tarkemmin VM:n ohje 5/01/2000).
 - Asiakirjan kopiosta on käytävä ilmi, kuka on kopion ottanut, koska kopiointi on tapahtunut ja kenen luvalla se on suoritettu.

3.4 ASIAKIRJAN JA TIETOJEN KÄSITTELY, SÄILYTYS JA ARKISTOINTI

Asiakirjan ja tietojen käyttöoikeuksia varten on viranomaisen määriteltävä periaatteet ja menettelytavat, joiden mukaan myönnetään oikeuksia ja valtuuksia käsitellä asiakirjoja. On määriteltävä, kenellä on oikeus päättää käyttöoikeuksista ja kuka viranomaisessa saa käsitellä mitään aineistoa ja millä tavalla.

Asiakirjan käsittelyn yhteydessä määritellään, miten paperimuotoista ja sähköistä asiakirjaa käsitellään ja kohdellaan eri tilanteissa sekä miten tämän käsittelyn ja kohtelun asianmukaisuutta valvotaan.

Asiakirjat ja tiedot tallennetaan tietojärjestelmiin ja niitä säilytetään tilapäisesti tai arkistoidaan pitkäaikaisesti muualla kuin välittömässä toimipaikan tai etätyöpisteen työtilassa. Pysyvästi säilytettävien, turvaluokiteltujen asiakirjojen arkistointiin tulee kiinnittää erityistä huomiota.

- **Yleiset vaatimukset kaikille salassa pidettäville tietoaineistoille** (Koskevat III turvaluokkaa "luottamuksellinen", II turvaluokkaa, I turvaluokkaa, muita salassa pidettäviä kuten salassa pidettävät EU-asiakirjat ja henkilötiedot)
 - Viranomaisen on varmistettava ja valvottava, että salassa pidettävää tietoaineistoa voivat käsitellä ja käsittelyyn osallistua vain siihen oikeutetut henkilöt. Salassa pidettävän aineiston osalta on määriteltävä, kuka saa käsitellä eri luokkiin kuuluvia asiakirjoja ja tietoja. Vain nimetyt henkilöt saavat käsitellä salaista tietoa. Salassa pidettävien tietojen käyttö- ja käsittelyoikeus edellyttää selkeää viran, toimen tai muun tehtävän vaatimaa tarvetta.
 - Viranomainen nimeää tietoaineistojen omistajat, joilla on oikeus valtuuttaa salassa pidettävien asiakirjojen ja tietojen käsittelijät.
 - Asiakirjan tai tietojen käsittelyoikeus (lukuoikeus) on vain sellaisella henkilöllä, jolla on tehtäviinsä liittyen siihen oikeus.
 - Asiakirjan tai tietojen muutosoikeus on vain nimetyllä henkilöllä, jonka viranomainen on tähän valtuuttanut.
 - Salassa pidettävien asiakirjojen hakemistoihin tai itse tietoihin on pääsyoikeus vain sellaisella henkilöllä, jonka viranomainen on tähän valtuuttanut.
 - Luokiteltua asiakirjaa käsiteltäessä ja käytettäessä on varmistettava, että asiattomat eivät pääse käsiksi salassa pidettävään tietoon. Asiakirjan sisältämiä tietoja saa käyttää vain niiden käyttötarkoituksen mukaan ja käytön asianmukaisuutta on valvottava.
 - Yleinen tavoite on pitää salassa pidettävä ja julkinen aineisto erillään toisistaan. Mikäli tämä ei joissain tapauksissa ole mahdollista, suojausto on valittava tiukemman suojausluokan mukaisesti.
 - Salassa pidettäviä asioita ei saa käsitellä julkisilla paikoilla.
 - Asiakirjaa ei saa jättää esille tai avoimiin paikkoihin ilman valvontaa.
 - Asiakirjaa tai tietoja ei saa jättää näkyviin tietokoneen näyttörudulle poistuttaessa sen äärestä.
 - Asiakirjaa tai sen osaa ei saa liittää suljetun lähiverkon ulkopuolelle lähetettävään sähköpostiin tai julkiseen asiakirja-aineistoon, ellei sitä ole salattu.
 - Asiakirjan tai tietojen käsittelyn tulee kirjautua sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse

- asiakirjaan. Sähköisen käsittelyn suositeltava kirjaamispaikka on loki tai vastaava sähköinen apuväline.
- Salassa pidettävä asiakirja on säilytettävä ja se on arkistoitava siten, etteivät asiattomat pääse käsiksi salassa pidettävään tietoon. Salassa pidettävä asiakirja on tallennuksen ja arkistoinnin yhteydessä erotettava julkisesta aineistosta. Asiakirjasta otetut kopiot ja varmistukset on säilytettävä samalla tavalla kuin alkuperäinen aineisto. Viranomaisen on valvottava hallussaan olevan salassa pidettävän asiakirjan säilytystä ja arkistointia.
 - Varmuuskopionauhoja ja palvelintietokoneilla olevia tietoja tulee käsitellä niissä olevan turvaluokitukseltaan vaativammassa luokassa (esim. I turvaluokka tai II turvaluokka tilanteen mukaan) olevan turvaluokituksen käsittelyn ohjeiden mukaisesti.
 - Asiakirja on säilytettävä ennen arkistointia lukitussa tilassa, esimerkiksi kaapissa, laukussa tai vastaavassa suljetussa tilassa. Tämä koskee myös siirrettävää tietovälinettä, varmuuskopioita ja vastaavia.
 - Asiakirjan säilytystä viranomaisen toimipaikan ulkopuolella on valvottava, sähköinen asiakirja on säilytettävä tällöin salattuna.
 - Asiakirja on arkistoitava lukittuun ja fyysisen suojauksen vaatimukset täyttävään arkistotilaan.
 - Jos henkilön oikeus aineiston käsittelyyn poistuu, on kaikki hänen hallussaan olevat kopiot joko hävitettävä tai siirrettävä seuraajan haltuun. Tästä toimenpiteestä tulee tehdä tarvittavat kirjaukset ja kuittaukset.
- **Lisävaatimuksia II turvaluokalle (salainen) ja I turvaluokalle (erittäin salainen) ja erälle salassa pidettävälle henkilötiedoille**
- Asiakirjaa tai tietoja saa käsitellä ainoastaan nimetty tai viranomaisen kyseistä asiaa käsittelemään valtuuttama henkilö.
 - Omistaja määrittää käsittelyoikeudet.
 - Asiakirjan käsittelijän oikeus asian käsittelyyn on tarvittaessa varmistettava.
 - Asiakirjan tai tietojen lukuoikeus on vain nimetyillä henkilöillä.
 - Asiakirjan tai tietojen muutosoikeus on vain sen omistajalla tai omistajan valtuuttamalla henkilöillä.
 - Manuaalinen asiakirja on sijoitettava aina lukittuun tilaan, kun poistutaan tilapäisestäkin sen äärestä.
 - Asiakirjaa tai tietoja saa käsitellä vain sellaisella laitteella ja sellaisessa käsittely-ympäristössä, jonka viranomainen on hyväksynyt salassa pidettävien tietojen käsittelyyn.
 - Poistuttaessa tällaisen laitteen luota tilapäisestäkin on varmistettava, etteivät asiattomat pääse käsiksi aineistoon.
 - Asiakirjan tietoja saa käsitellä ja niistä keskustella vain paikoilla ja tiloissa, missä tieto ei paljastu asiattomille.
 - Asiakirjaa saa käsitellä vain sellaisella työasemalla tai suljetussa toimipisteen verkossa, josta ei ole pääsyä yleiseen avoimeen tietoverkkoon (esim. Internet, Datnet, LanLink).
 - Salassa pidettävä asiakirja-aineisto on selvästi erotettava julkisesta aineistosta.
 - Asiakirjan tai tietojen sähköisen käsittelyn on kirjauduttava ja omistajan on valvottava sitä.

- On pidettävä kirjaa henkilöistä, jotka ovat saaneet tutustua ko. asiakirjaan.
- Asiakirja on säilytettävä väliaikaisestikin murtosuojatussa tilassa tai paikassa, esimerkiksi holvissa tai kassakaapissa. Tämä koskee myös levykeitä ja varmuuskopioita.
- Asiakirja on toimipaikan ulkopuolella säilytettävä suojatussa ja lukitussa tilassa kuten holvissa, kaapissa tai laukussa. Säilytystä on jatkuvasti valvottava.
- Asiakirjaa ja tietoja säilytetään työpaikalla ja riittävän vahvasti salakirjoitettuna työasematietokoneen kiintolevyllä, palvelinkoneella tai lisäkiintolevyllä.
- Asiakirja tai tiedot on arkistoitava murtosuojatussa tilassa tai holvissa.
- Asiakirja tai tiedot arkistoidaan erillisellä tietovälineellä, jota käsitellään kuten paperia.
- Arkistointia sekä arkiston käyttäjiä ja käyttöä on valvottava.

- **Lisävaatimuksia I turvaluokalle (erittäin salainen)**
 - Oikeus asiakirjan näkemiseen ja sen tietojen käyttämiseen on vain omistajan nimeämällä henkilöllä.
 - Mahdolliset muut käsittelijät voidaan nimetä vain omistajan kanssa tehdyn sopimuksen perusteella.
 - Asiakirjan tietojen käsittelijän henkilöllisyys ja henkilön luotettavuus on aina varmistettava.
 - Asiakirjan omistaja kontrolloi jatkuvasti sen käsittelyä.
 - Asiakirja-aineistoa saa käsitellä vain sellaisella teknisellä laitteella, jonka viranomainen on erikseen hyväksynyt kyseisen aineiston käsittelyyn.
 - Asiakirjan ja sen tietojen käsittelyssä ja siitä keskusteltaessa saavat mukana olla vain erikseen nimetyt ja asiakirjan omistajan hyväksymät henkilöt.
 - Asiakirjan tietoja ei saa käsitellä tietoverkkoon kytketyllä laitteella (poikkeuksena täysin viraston sisäiset tietoverkot, joista ei ole mitään yhteyttä ulkoisiin verkkoihin).
 - Asiakirjaa saa luonnin jälkeen käsitellä sähköisesti vain sen omistaja.
 - Erittäin salaisia asioita käsitellään pääasiassa paperiasiakirjoina.
 - Jokainen asiakirjan käsittelijä merkitsee asiakirjaan päivämäärän ja allekirjoituksen.
 - Asiakirjaa säilytetään aina sen käsittelyn keskeytyessä tarkoitusta varten erikseen hyväksytyssä tilassa tai holvissa.
 - Asiakirjaa ei saa säilyttää työaseman kiintolevyllä edes työskentelyn aikana eli järjestelmän mahdollisesti tekemät varmuustallennukset tulee hävittää pikaisesti.
 - Asiakirjaa säilytetään sähköisessä muodossa aina vahvasti salattuna.
 - Vain asiakirjan omistaja voi arkistoida asiakirjan sähköisessä muodossa.
 - Tarvittaessa asiakirja voidaan arkistoida manuaalisessa muodossa erillään kaikesta muusta tietoaaineistosta. Arkistointiin käytettävän tilan on täytettävä salassa pidettävän aineiston arkistoinnille asetetut fyysiset vaatimukset.

3.5 ASIAKIRJAN HÄVITTÄMINEN JA KÄYTÖSTÄ POISTAMINEN

Tarpeettomaksi tullut asiakirja poistetaan käytöstä joko tuhoamalla se fyysisesti tai saattamalla se muuten sellaiseen muotoon, ettei sen sisältämää tietoa voida käyttää. Hävittää saa vain asiakirjoja, joita Arkistolaitos ei ole määrännyt pysyvästi säilytettäväksi. Säilytysajat tulee määrittellä arkistonmuodostussuunnitelmassa, joka näin ohjaa asiakirjojen hävittämistä tai pysyvää säilyttämistä.

Salassa pidettävä asiakirja on poistettava käytöstä ja hävitettävä siten, etteivät asiattomat pääse käsiinsä salassa pidettävään tietoon. Tällainen aineisto on hävittämisen yhteydessä eroteltava muusta aineistosta. Salassa pidettävää aineistoa saa hävittää vain viranomaisen siihen oikeuttama henkilö ja hävittämisessä on käytettävä riittävän turvallisia menetelmiä. Salassa pidettävän aineiston hävittäminen on aina suoritettava valvotusti. VM on antanut yleisohjeen tarpeettomiksi tulleiden tietoa-ineistojen hävittämisestä 19.4.2000 (VM 21/01/2000).

- **Yleiset vaatimukset kaikille salassa pidettäville tietoaineistoille** (Koskevat III turvaluokkaa "luottamuksellinen", II turvaluokkaa, I turvaluokkaa, muita salassa pidettäviä kuten salassa pidettävät EU-asiakirjat ja henkilötiedot)
 - Asiakirjojen pysyvää säilyttämistä verrattuna hävittämiseen tulee arvioida sen riskin kannalta, jonka hävittäminen aiheuttaa toiminnan jatkuvuudelle.
 - Järjestelmän tekemiä väliaikaistiedostoja ei tule säilyttää tarpeettomasti. Tarpeettomat asiakirjakopiot hävitetään käyttötarpeen päätyttyä. Muut kuin arkistolaitoksen päätöksellä pysyvään säilytykseen määrätty asiakirjat tulee hävittää välittömästi sen jälkeen, kun niille arkistonmuodostussuunnitelmassa vahvistettu säilytysaika on kulunut umpeen.
 - Käytännössä hävittämisen luettelointia kannattaa yhdistää mahdollisuuksien mukaan muuhun Arkistolaitoksen edellyttämään hävittämisen rekisteröintiin.
 - Manuaalinen asiakirja tai tietoväline, jolla asiakirjaa säilytetään hävitetään silppuamalla se tarkoitusta varten rakennetulla laitteella (silppukoko max 4mmx60mm) tai hävittämällä se muulla varmalla tavalla.
 - Sähköinen asiakirja hävitetään päällekirjoittamalla teksti niin moneen kertaan, että alkuperäisen tiedon häviäminen voidaan varmistaa tai tuhoamalla kiintolevy varmalla ja luotettavalla tavalla.
 - Asiakirjan hävittämisestä päättää sen käsittelystä päättävä viranomainen tai henkilö. Asiakirjan hävitystä on valvottava ja siitä on pidettävä kirjaa.
- **Lisävaatimuksia II turvaluokalle (salainen) ja I turvaluokalle (erittäin salainen) ja erälle salassa pidettäville henkilötiedoille**
 - Vain asiakirjan omistaja voi käyttää tyhjättyä tietovälinettä uudelleen.
 - Hävittämisestä on pidettävä kirjaa: mm. kuka on toimituksen suorittanut ja millä menetelmällä hävitys on suoritettu.
- **Lisävaatimuksia I turvaluokalle (erittäin salainen)**
 - Kaikki kopiot on palautettava omistajalle, ellei omistajan kanssa toisin sovita.
 - Paperimuotoinen aineisto on hävitettävä silppuamalla (max silppukoko 0.8mmx15mm).
 - Sähköinen aineisto on tuhottava yhtä luotettavasti kuin paperimuotoinen, esimerkiksi päällekirjoittamalla tai tuhoamalla tietoväline. Tietovälineen uudelleen käyttö on sallittu vain asiakirjan omistajalle.

4 KÄSITTELYN EHEYDELLE JA KÄYTETTÄVYYDELLE ASETETTAVAT VAATIMUKSET

Asiakirjojen ja tietojen käsittelylle asetetaan vaatimuksia myös sen mukaan, minkälaisia riskejä toiminnan ja sen jatkuvuuden kannalta sisältyy siihen, että tiedot eivät ole oikeita, asianmukaisia tai tarvittaessa käytettävissä ja minkälaista haittaa ja vahinkoa tästä voi aiheutua toiminnalle.

Kunkin organisaation on määriteltävä omista lähtökohdistaan vaatimuksensa tietoaineiston eheydelle ja käytettävyydelle ja kunkin organisaation on luokiteltava aineistonsa siten, että luokitus vastaa sen omia tavoitteita ja tarpeita.

Eheyden ja käytettävyyden perusteella tehdyt luokitukset ja niiden mukaisesti määritetyt vaatimukset eivät koske automaattisesti muita organisaatioita, joten tässä ei esitetä luokittelulle yleisiä malleja. Tässä määritellään vain tietoaineiston käsittelylle asetettavia yleisiä vaatimuksia aineiston eheyden ja käytettävyyden suhteen.

- Kun kerätään ja vastaanotetaan tietoaineistoa ja luodaan asiakirja, on varmistettava toiminnan ja sen jatkuvuuden kannalta tärkeän tiedon eheydestä ja käytettävyydestä. On arvioitava luotavan aineiston eheys- ja käytettävyystarpeet sekä määriteltävä aineiston käsittelylle asetettavat vaatimukset.
- On arvioitava, minkälaisia seurauksia eheyden puuttuminen aiheuttaa toiminnalle ja asiakkaille ja mitä vaatimuksia asetetaan tietojen ajantasaisuudelle ja laadulle. Lisäksi on arvioitava, miten kriittisiä tiedot ovat toiminnalle, miten pitkään tiedot voivat olla poissa käytöstä ja minkälaista vahinkoa aiheutuu siitä, etteivät tiedot ole käytettävissä sekä mitä vaatimuksia asetetaan tietojen varmistuksille.
- On laadittava suunnitelma, miten eheyden ja käytettävyyden vaatimukset voidaan toteuttaa toiminnan ja sen jatkuvuuden kannalta merkittävien tietojen osalta.
- Turvaluokitellun asiakirjan osalta on kiinnitettävä huomiota seuraaviin seikkoihin: miten ajantasaista tiedon pitää olla, mitä oikeellisuustarkistuksia pitää tehdä sekä miten pitkään tieto voi olla poissa käytöstä ja mitä vaatimuksia asetetaan tiedon varmistukselle.
- Kun jaetaan, luovutetaan ja vastaanotetaan sekä kuljetetaan tai siirretään tärkeää tietoa, on varmistettava, että tieto ei siinä yhteydessä muutu, tuhoutu tai häviä asiattomasti.
- On varmistettava ja kontrolloitava, että vain oikeutetut henkilöt voivat käsitellä ja muokata tai tuhota tärkeää tietoa. Luokiteltua asiakirjoja ja tietoja saa käsitellä ja käyttää vain sellaisilla tavoilla ja sellaisissa ympäristöissä, jotka eivät vaaranna tiedon eheyttä tai käytettävyyttä.
- Luokiteltu aineisto on säilytettävä siten, että tiedot eivät muutu tai tuhoutu asiattomasti. Lisäksi on varmistettava tietojen käytettävyys. Tällainen aineisto on arkistoitava siten, että tietojen eheys säilyy ja sellaisessa muodossa, että tiedot ovat palautettavissa käyttöön. Tietoaineiston hävittämisen yhteydessä on erikseen varmistettava, että siinä ei tuhota toiminnan kannalta tärkeää tietoa.
- Arkistolaitoksen pysyvästi säilytettäväksi määräämien asiakirjojen eheyden ja käytettävyyden varmistamiseen on kiinnitettävä erityistä huomiota.
- Eheyden kannalta versionhallinta sähköisessä ympäristössä on keskeinen tehtäväalue.

LIITE 1

1 TIETOAINEISTOJEN KÄSITTELYN LÄHTÖKOHTIA VALTIONHALLINNOSSA

1.1 Lainsäädännöstä ja tietoturvallisuusohjeista tietoaineiston käsittelyohjeiden lähtökohtana

Viranomaisten toiminnan julkisuudesta annettu laki (JulkL 621/1999 18.4 §) antaa mahdollisuuden tietoturvallisuutta valtionhallinnossa koskevien ohjeiden ja määräysten antamisen. Lisäksi JulkL ja JulkA määrittävät peruseriaatteet viranomaisten asiakirjojen käsittelystä ja luokittelemisesta.

Viranomaisten tehtävien hoidon tehokkuuden kannalta on tärkeää, että päätöksenteossa tarvittava tieto on nopeasti käytettävissä. Kansalaisten oikeusturvan huolehtimiseksi on varmistettava, että päätöksenteossa käytettävät tiedot ovat oikeita ja asianmukaisia.

Julkisuusperiaatteen mukaan pääsääntönä on viranomaisten asiakirjojen julkisuus, oikeus saada tieto viranomaisen julkisesta asiakirjasta on perusoikeus. Periaatteeseen kuuluu myös, että tiedot, joiden paljastuminen vaarantaa keskeisten yksityisten tai julkisten etujen toteutumista, on pidettävä salassa ja niiden suojaamisesta huolehdittava asianmukaisesti. Viranomaisten henkilörekistereihin talletettujen tietojen käsittelyä säännellään henkilötietolailla (523/1999).

Julkisuus- ja salassapitolainsäädännön kokonaisuudistuksen keskeisenä tavoitteena on toteuttaa hyvää tiedonhallintatapaa viranomaisten tietoaineistojen käsittelyssä. Tätä koskevat säännökset sisältyvät JulkL 18 §:ään sekä JulkA:een.

Hyvällä tiedonhallintavalla pyritään toteuttamaan menettelyt ja toimenpiteet, jotka ottavat huomioon erilaiset viranomaistietoon kohdistuvat vaatimukset. Säännöstö tukee arkistolain (381/1994) tavoitetta huolehtia viranomaisten asiakirjojen saatavuudesta. Hyvän tiedonhallintavan mukaisia velvoitteita ovat (JulkL 18.1 §):

- julkisuusperiaatteen toteutumista palvelevien luetteloiden ja selosteiden laatiminen
- tietoon liittyvien oikeuksien kartoittaminen ja huomioon ottaminen
- hyvän julkisuus- ja salassapitorakenteen toteuttaminen asiakirja- ja tietohallinnossa sekä tietojen eheyden ja suojan turvaaminen
- henkilöstön koulutuksesta ja ohjauksesta sekä toiminnan valvonnasta huolehtiminen.

JulkL, JulkA ja henkilötietolain lisäksi useat muut lait ja ohjeet sisältävät viranomaisia koskevia tietoturvallisuusvelvoitteita:

- Laki sähköisestä asioinnista hallinnossa (1318/1999)
- Asetus valtionhallinnon tietohallinnosta (155/1988 ja muutos 1401/1992)
- Valtioneuvoston ohjesääntö (1522/1995)
- Arkistolaki (831/1994)
- Asetus valtion talousarviosta (1243/1992)
- Henkilökorttilaki (829/1999)
- Väestötietolain muutos (527/1999)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999), sekä lain nojalla annettu asetus (723/1999)
- Telemarkkinalaki (396/1997)

- Laki sähköisestä viestinnän ja automaattisen tietojenkäsittelyn käyttämisestä yleisissä tuomioistuimissa (594/1993)
- Valtion virkamieslaki (750/1994)
- Valmiuslaki (1080/1991)
- Laki ja asetus puolustustaloudellisesta suunnittelukunnasta (1960)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta 11.11.1999
- Valtioneuvoston periaatepäätös valtion tietohallinnon kehittämisestä 2.3.2000
- Tarpeettomaksi tulleiden tietoaineistojen hävittämisohje VM 21/01/2000, 19.4.2000
- Valtionhallinnon tietoturvaluokituskäsitteistö, VAHTI 1/2000
- Tietojärjestelmäselosteen laadintasuositus VM 7/01/2000, 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 5/01/2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvaluokitusohje, VAHTI 2/1999
- Valtion etätyön tietoturvaluokitusohje, VAHTI 1/1999
- Internetin käyttö - ja tietoturvaluokitusohje, VAHTI 1/1998
- Tietoturvaluokituksen tulosohjaus ja kehittämisvälineet, VAHTI 2/1997
- Sähköpostin ja lokitiedostojen käsittely, VAHTI 3/1997
- Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa, 1996 (VM ja PTS)
- Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa, VM 30.12.1998

1.2 Hyvän tiedonhallintavan ja tietojen luokituksen periaatteet

Hyvä tiedonhallintatapa edellyttää tietoaineistojen kartoitusta ja niihin liittyvien vaatimusten arviointia. Kartoitus perustuu arkistonmuodostussuunnitelmaan. Kun arvioidaan hyvän tiedonhallintavan mukaisten toimenpiteiden tarvetta, on selvítettävä, miten toteutetaan esimerkiksi oikeus saada tietoja julkisista asiakirjoista sekä henkilötietojen ja salassa pidettävien tietojen suojaaminen samoin kuin se, miten turvataan tietojen käytettävyys, eheys ja laatu viranomaisten tehtävien hoidossa ja viranomaisten välisessä yhteistyössä. Kartoitus- ja arviointityö edellyttää asian- ja tietojenkäsittelyprosessien läpikäyntiä.

Tietoturvaluokituksella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen **luottamuksellisuutta, eheyttä ja käytettävyyttä** turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvaluokituksen keskeisillä käsitteillä tarkoitetaan seuraavaa:

Luottamuksellisuus; tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja, eikä muutoin käsitellä tietoja.

Eheys; tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.

Käytettävyys; järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Tiedot eivät ole tuhoutuneet tai tuhoavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

Viranomaisen on tunnistettava ne asiaryhmät, joissa salassa pidettäviä tietoja säännönmukaisesti käsitellään. Tiedon luottamuksellisuuden varmistavat toimenpiteet on kohdistettava erityissuojattavaan tietoaineistoon. Tällaisia ovat asiakirjat ja tiedot (Julka 2 §),

- jotka on pidettävä salassa
- joiden luovuttamista rajoitetaan muutoin lailla
- joita lain mukaan saa käyttää vain määrättyyn tarkoitukseen.

Toimenpiteiden oikeaksi mitoittamiseksi suojattava tietoaineisto on luokiteltava, jotta toimenpiteet voidaan toteuttaa ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä tietoaineistoihin kohdistuvat uhkatekijät samoin toimenpiteistä aiheutuvat kustannukset. Viranomainen voi luokitella suojattavat aineistot pääsääntöisesti kolmeen turvaluokkaan, jollei hallinnonalan tarpeista johdu muuta.

Luokat on määritelty sen mukaan, kuinka vakavia seurauksia tietojen asiattomasta paljastumisesta seuraisi suojattaville eduille. Kutakin turvaluokkaa vastaavat erityiset toimenpiteet. Ensimmäiseen turvaluokkaan kuuluviin asiakirjoihin sovelletaan korkeimman turvallisuustason toimenpiteitä. Tähän turvaluokkaan voivat kuulua tietoaineistot, jotka on suojattava Suomen kansainvälisiin suhteisiin, rikosten ehkäisemiseen ja selvittämiseen, yleiseen järjestykseen, poikkeusoloihin varautumiseen, valtion turvallisuuteen, maanpuolustukseen sekä kansantalouteen liittyvien etujen vuoksi. Toiseen ja kolmanteen turvaluokkaan voivat kuulua minkä tahansa edun vuoksi suojattavat tiedot.

Tietoturvallisuusluokituksen perusteita on esitelty myös liitteessä 2.1.

Julka 3 §:ssä on määritelty suojattavia tietoaineistoja koskevat yleiset, minimitason turvallisuustoimenpiteet. Aineistojen käsittelyä koskevat vaatimukset kohdistuvat tiedon koko elinkaareen. Julka ei sisällä yksityiskohtaisempia säännöksiä tietoaineistojen luokitteluksi tietojen eheyden ja käytettävyyden tarpeiden suhteen. Myös tässä esitetään näiltä osin vain yleisiä vaatimuksia.

1.3 Muut tietoaineiston käsittelyyn vaikuttavat tekijät

Turvallisuusvaatimukset kohdistuvat tiedon ohella myös muihin tekijöihin, kuten tietojenkäsittely- ja säilytystilojen suojaamiseen. Valtiovarainministeriö on antanut suosituksen toimitilaturvallisuuden huomioon ottamisesta valtionhallinnossa (VM 1/01/99). Toimitilaturvallisuuteen kuuluvat asiakkaiden valvonta, oman henkilöstön liikkumisen ohjaaminen, fyysinen valvonta, tekniset valvontalaitteistot, rakenteellinen suojaus sekä erikoistilat. Suosituksessa toimitilat on jaettuun neljään turvaluokkaan; perussuojaus, tehostettu perussuojaus, erityissuojaus ja täyssuojaus.

Julka:ssa ei ole säännöksiä henkilöstöturvallisuudesta. Oikeusministeriön asettaman toimikunnan tehtävänä on laatia ehdotus henkilöstöturvallisuutta koskevaksi lainsäädännöksi. Se sisältää ehdotuksen tehtävien turvallisuusluokituksesta sekä siihen liittyvästä henkilöstön suostumukseen perustuvasta tarkastusmenettelystä ja turvallisuusluokituksen rekisteröinnistä.

Kansainvälinen yhteistoiminta esimerkiksi Euroopan unionin, NATO:n ja WEU:n puitteissa edellyttää tietoaineistojen ja asiakirjojen yhtenäisiä luokittelukäytäntöjä. Myös kansainvälinen tietojen, tietojärjestelmien ja tietojenkäsittelyn turvallisuuden standardointi lähtee yhtenäisistä luokittelu- ja käsittelykäytännöistä.

Valtiovarainministeriö
Hallinnon kehittämisosasto

LIITE 2

VM 5/01/2000

19.1.2000

Ministeriöille, virastoille ja laitoksille

Asia **Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje**

1 LÄHTÖKOHDAT

Laki viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä JulkL) sekä sen perusteella annettu asetus (1030/1999, jäljempänä JulkA) tulivat voimaan 1.12.1999. Samalla kumoutui valtioneuvoston vuonna 1975 antama määräys eräiden salaisten asiakirjojen käsittelystä valtionhallinnossa (VNK 1043/140/75).

Valtioneuvosto teki 11.11.1999 valtionhallinnon tietoturvallisuutta koskevan periaatepäätöksen (VM 24:0/2/99/1998).

JulkL 24 §:n 1 momentissa (jäljempänä JulkL 24.1 §) on lueteltu asiakirjat, jotka on pidettävä salassa. Olennaista kyseisiä asiakirjoja luotaessa, muutettaessa, siirrettäessä, arkistoitaaessa, hävitettäessä ja muutoin käsiteltäessä on se, että salassa pidettävien asioiden käsittely on turvaluokkien (määritelmät sivuilla 2 ja 3) mukaan yhdenmukaista kaikissa viranomaisissa ja toisaalta se, että JulkL 18 §:n tarkoitus hyvästä tiedonhallintatavasta toteutuu.

JulkL 38 §:n mukaan ennen lain voimaantuloa käyttöönotetut tietojärjestelmät on suojattava ja niissä olevien tietojen suoja, eheyttä ja laatua turvaavat toimenpiteet on toteutettava JulkL:n asettamien tavoitteiden mukaisina kolmen vuoden kuluessa lain voimaantulosta. Oikeusministeriö valmistelee valtioneuvoston raha-asianvaliokunnan lausuman mukaisesti edellä tarkoitetun siirtymäajan pidentämistä viiteen vuoteen.

Tietojen luokittelua ja asiakirjojen käsittelyä valtionhallinnossa koskevat ohjeet ovat valmisteltavana valtiovarainministeriön asettamassa valtion tietoturvallisuuden johtoryhmässä ja ne on tarkoitus antaa kevään 2000 kuluessa. Ohjeissa tullaan linjaamaan tietojen ja asiakirjojen tietoturvallisuusvaatimuksia sekä manuaalisen että sähköisen käsittelyprosessin eri vaiheissa, joita ovat mm. luonti, muokkaus, tallennus, kopiointi, lähetys, vastaanotto, hävittäminen ja vastaanotto. Työn painopiste on turvaluokiteltujen (määritelmä sivulla 3) tietojen ja aineistojen käsittelyn tietoturvallisuusvaatimusten ohjeistamisessa.

Lisäksi valtiovarainministeriö valmistelee ohjetta salauskäytännöistä.

1.1 Ohjeen tarkoitus

Valtion viranomaisten yhtenäisen käytännön ja tietoturvallisuuden varmistamiseksi sekä päällekkäisen työn välttämiseksi valtiovarainministeriö antaa jo ennen edellä

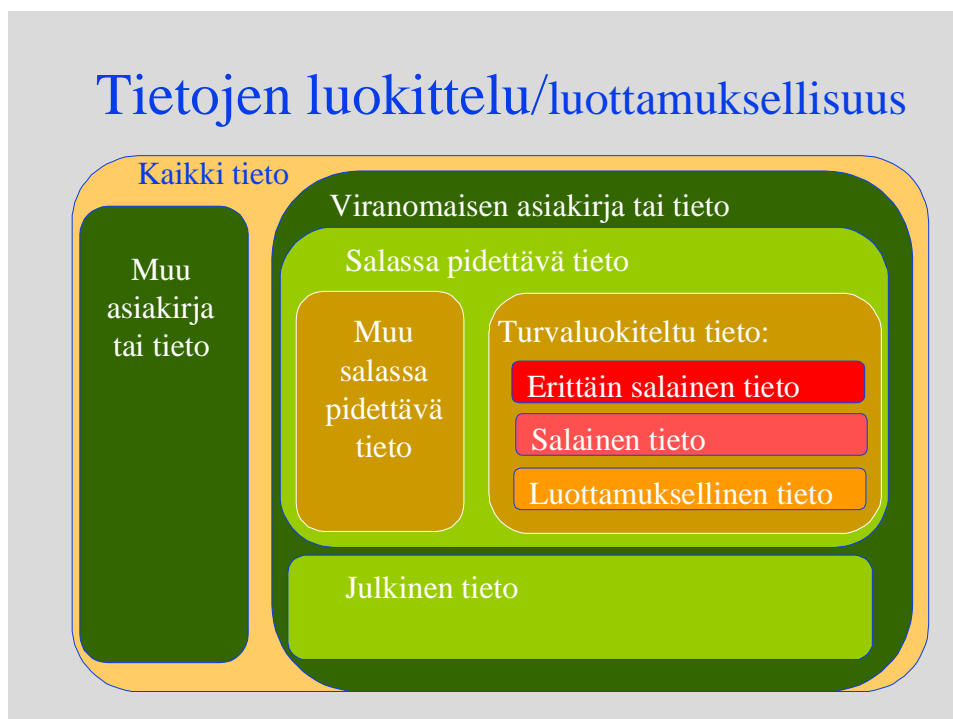
mainitun tietojen luokittelua ja käsittelyä koskevan työn valmistumista valtioneuvoston ohjesäännön (1522/1995) 19 §:n 19 kohdan sekä valtionhallinnon tietohallinnosta annetun asetuksen (155/88, muutettu 1401/92) 1 ja 2 §:n perusteella tämän ohjeen salassa pidettävien tietojen ja asiakirjojen luokituksista ja merkinnöistä valtionhallinnossa. Ohje koskee ministeriöitä sekä valtion virastoja ja laitoksia.

Tässä ohjeessa määritellään turvaluokittelun ja merkintöjen käytäntöjä luottamuksellisuuden osalta. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niiden käyttöön oikeutettujen käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa, tuhota, nähdä tai muutoin käsitellä tietoja.

1.2 Asiakirjojen ja tietojen luokittelu sekä ohjeen soveltamisala

Julkisuuslain soveltamisalan piiriin kuuluvat JulkL 5 §:ssä määritellyt viranomaisen asiakirjat. Tätä ohjetta sovelletaan JulkL 5 §:n 2 momentissa määriteltyihin viranomaisen asiakirjoihin.

Asiakirjoista, joita ei pidetä viranomaisen asiakirjoina, on säädetty JulkL 5 §:n 3 ja 4 momentissa. Tällaisia lain soveltamisalan ulkopuolelle jääviä asiakirjoja ovat mm. virkamiehen laatimat muistiinpanot ja sisäistä koulutusta varten hankitut asiakirjat sekä virkamiehen saamat yksityiskirjeet. Tätä ohjetta on sovellettava sellaisiin virkamiesten luonnoksiin ja muistiinpanoihin samoin kuin viranomaisen sisäisen työskentelyn asiakirjoihin, jotka on säädetty salassa pidettäväksi 5 §:n 5 momentin mukaan, vaikka ne muutoin jäävätkin JulkL:n soveltamisalan ulkopuolelle.



Oheisessa kuvassa on esitetty tietojen ja asiakirjojen luokittelun perusrhymittely luottamuksellisuuden perusteella.

Asiakirjojen ja tietojen luokittelun keskeisiä käsitteitä on selostettu liitteessä 1.

2 VIRANOMAISEN ASIAKIRJOJEN JA TIETOJEN LUOKITTELU JA MERKINNÄT

2.1 Julkiset asiakirjat ja tiedot

Viranomaisten asiakirjat ovat julkisia, jollei toisin ole säädetty. Julkisiin asiakirjoihin ei tarvitse tehdä erityistä luokittelumerkintää.

2.2 Salassa pidettävät asiakirjat ja tiedot

Salassa pidettävät asiakirjat voidaan jakaa turvaluokiteltaviin tietoihin tai asiakirjoihin ja muihin salassa pidettäviin tietoihin tai asiakirjoihin. Jaottelun ja esitetyn turvaluokittelun perusteena ovat mm. toiminnalliset tarpeet, kansalliset ja kansainväliset tietojen ja aineistojen turvaluokittelukäytännöt, JulkL, JulkA, tietoturvallisuustoimenpiteiden ohjeistus-, suunnittelu- ja toteutusmahdollisuudet ja niihin liittyvät kustannusvaikutukset.

2.2.1 Turvaluokiteltavat tiedot tai asiakirjat

Asiakirja on turvaluokiteltava asiakirja silloin, kun se on JulkL 24.1 §:n 1, 2, 5, 7, 8, 9, 10 tai 11-kohtien mukaan salassa pidettävä. Tällaiset asiakirjat käsittelevät yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi arkaluonteista, salassa pidettävää tietoa. **Valtiovarainministeriö suosittaa asiakirjojen ja tietojen turvaluokitteluja ja niitä vastaavia turvamerkintöjä erityisesti sellaisiin salassa pidettäviin tietoihin ja asiakirjoihin, joiden salassapitoperuste on edellä mainittu JulkL 24 §:n kohta.**

Turvaluokiteltavat asiakirjat jaetaan JulkA 2 §:n mukaisesti kolmeen turvaluokkaan, jotka eroavat toisistaan asiakirjan ja sen tietojen suojaamiseksi tarvittavan suojaustason osalta: **I turvaluokkaan** kuuluvat asiakirjat varustetaan leimalla tai merkinnällä ”Erittäin salainen” (engl. top secret), **II turvaluokan** asiakirjat varustetaan merkinnällä ”Salainen” (engl. secret) ja **III turvaluokan** asiakirjat merkinnällä ”Luottamuksellinen” (engl. confidential).

I turvaluokan asiakirja sisältää äärimmäisen arkaluonteista, salassa pidettävää tietoa. Tällainen asiakirja tulostetaan paperille, jonka poikki kulkee punainen vinoviiva ja sen jokaisen sivun ylälaitaan sijoitetaan leima tai merkintä ”**Erittäin salainen**”. Leiman väri on punainen. Tällaisen asiakirjan vastaanottajana on aina henkilö/henkilöt, eivätkä sitä saa ilman aineiston omistajan lupaa käsitellä muut kuin vastaanottajiksi merkityt sekä tällaisen asiakirjan tekniseen (vastaanotto, arkistointi yms.) käsittelyyn vastaanottavassa virastossa tai laitoksessa oikeutetut henkilöt. **I turvaluokan** asiakirjaa ei toistaiseksi saa lähettää sähköisissä tietojärjestelmissä. Manuaalilähetyksessä lähettäjän on aina varmistettava, että lähetys on saapunut vastaanottajaksi merkitylle henkilölle.

II turvaluokan asiakirja sisältää erittäin arkaluonteista, salassa pidettävää tietoa. Tällainen asiakirja tulostetaan paperille, jonka poikki kulkee punainen vinoviiva ja sen ensimmäisen sivun ylälaitaan sijoitetaan leima tai merkintä ”**Salainen**”. Leiman väri on punainen. Tällainen asiakirja voidaan osoittaa henkilölle tai organisaatiolle ja sitä saavat käsitellä vain ne henkilöt, jotka on virastossa oikeutettu käsittelemään salassa pidettäviä asioita. **II turvaluokan** asiakirjan saa lähettää vastaanottajalle sähköisissä tietojärjestelmissä ainoastaan riittävän vahvasti salattuna.

III turvaluokan asiakirja sisältää salassa pidettävää tietoa. III turvaluokan asiakirja tulostetaan normaalille paperille ja sen ensimmäisen sivun ylälaitaan sijoitetaan leima tai merkintä ”**Luottamuksellinen**”. Leiman väri on punainen. Tällainen asiakirja voidaan osoittaa henkilölle tai organisaatiolle ja sitä saavat käsitellä vain ne henkilöt, jotka tehtävässään tarvitsevat kyseisen asiakirjan sisältämiä tietoja. **III turvaluokan** asiakirjan saa lähettää vastaanottajalle sähköisissä tietojärjestelmissä riittävän vahvasti salattuna.

2.2.2 Muut salassa pidettävät tiedot ja asiakirjat

Tieto tai asiakirja, joka on JulkL 24.1 §:n jonkun muun kuin edellä mainitun (24.1 §:n 1, 2, 5, 7, 8, 9, 10 tai 11) perusteella salassa pidettävä, kuuluu muihin salassa pidettäviin tietoihin tai asiakirjoihin. Esimerkkeinä voidaan mainita salassa pidettävät henkilötiedot sekä liike- ja ammatillisalaisuudet. **Muille salassa pidettäville tiedoille ja asiakirjoille ei toistaiseksi suositella turvaluokittelua**, koska tälle kustannuksia lisäävälle, pääosin nykykäytäntöjen vastaiselle turvaluokittelulle ei ole esitetty tarvetta.

Muu salassa pidettävä tieto tai asiakirja varustetaan ensimmäisen sivun ylälaitaan sijoitettavalla leimalla ”**Salassa pidettävä**” ja sitä saavat käsitellä vain ne henkilöt, jotka tehtävässään tarvitsevat kyseisen asiakirjan tietoja. Leiman väri on punainen. Tällainen asiakirja tulostetaan normaalille paperille. Salassa pidettävän asiakirjan saa lähettää vastaanottajalle sähköisissä tietojärjestelmissä riittävän vahvasti salattuna.

2.2.3 Merkintöjen tekeminen

Salassa pidettävä tieto ja asiakirja tulee varustaa leimalla tai sähköisessä käsittelyssä merkinnällä, josta ilmenee tiedon tai asiakirjan salassa pidettävyys.

JulkL 25 §:n mukaan asianosaiselle annettavaan asiakirjaan on tehtävä merkintä sen salassa pitämisestä, jos asiakirja sisältää yleisen edun tai toisen edun vuoksi salassa pidettäviä tietoja. Myös muuhun asiakirjaan voidaan tehdä merkintä sen salassa pidosta. Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu. Jos salassapito perustuu sellaiseen säännökseen, jossa on vahinkoedellytyslauseke, merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain säännös, johon salassapito perustuu.

Liitteessä 2 on esitetty käytettävien leimojen ja merkintöjen yksityiskohdat. Esimerkiksi JulkL 24 §:n 1 momentin 7 kohdan ollessa salassa pidon peruste leimaan merkintään: "JulkL (621/1999) 24.1 §:n 7 k".

3 LISÄTIETOJEN ANTAMINEN

Lisätietoja tähän ohjeeseen ja sen soveltamiseen liittyvistä asioista antavat tarvittaessa valtiovarainministeriön hallinnon kehittämisosaston neuvottelevat virkamiehet Mikael Kiviniemi (Mikael.Kiviniemi@vm.vn.fi) ja Arja Terho (Arja.Terho@vm.vn.fi).

Ylijohtaja

Jorma Karjalainen

Neuvotteleva virkamies

Mikael Kiviniemi

Liite 1 Asiakirjojen ja tietojen luokittelun käsitteitä

Liite 2 Salassa pidettävien asiakirjojen leimat

Liite 2.1

ASIAKIRJOJEN JA TIETOJEN LUOKITTELUN KÄSITTEITÄ

Julkiset asiakirjat ja harkinnanvaraisesti julkiset asiakirjat

Viranomaisten asiakirjat ovat julkisia, jollei toisin ole säädetty. Tiedon antaminen viranomaisen asiakirjasta ennen JulkL 6 ja 7 §:ssä säädettyjen ajankohtien saavuttamista, on viranomaisen harkinnassa, jollei niihin sisälly salassa pidettäviä tietoja. Harkinnanvaraisesti julkiset asiakirjat ovat joko valmisteilla olevia asiakirjoja tai asiakirjoja, jotka liittyvät keskeneräiseen asiaan.

Salassa pidettävä tieto

Tieto tai asiakirja on salassa pidettävä, jos niin on laissa säädetty (JulkL 22 ja 24 §). Salassa pidettävää tietoa saattaa sisältyä myös sellaiseen asiakirjaan, joka on pääosin julkinen. Jos asiakirjan osa on salassa pidettävä, tieto tulee antaa asiakirjasta muilta osin, jos se käy päinsä salassa pidettävän tiedon paljastumatta (JulkL 10 §).

Erityissuojattava tieto

Tieto voi olla erityissuojattavaa luottamuksellisuuden (salassapito, henkilötietojen suoja), eheyden ja käytettävyyden suhteen. JulkA 2 §:ssä säädetään erityissuojattavan tietoaineiston luokituksesta. Tietoaineistot voidaan luokitella pääsäännön mukaan kolmeen eri turvaluokkaan sen mukaan, minkälaisia tietoturvaluusvaatimuksia on tietoaineistoja käsiteltäessä noudatettava. JulkA 2 §:n mukaan:

- Ensimmäiseen turvaluokkaan kuuluviksi voidaan luokitella tietoaineistot, jos tiedon oikeudeton paljastuminen vaarantaa tiettyjä keskeisiä yleisiä etuja.
- Toiseen turvaluokkaan kuuluviksi voidaan luokitella erityissuojattavat tietoaineistot, jos tiedon oikeudeton paljastuminen ja käyttö loukkaisi merkittävästi niitä etuja, joiden vuoksi rajoitukset on säädetty. Nämä edut voivat olla sekä yleisiä että yksityisiä etuja.
- Kolmanteen turvaluokkaan kuuluviksi voidaan JulkA 2 §:n 4 momentin mukaan luokitella tietoaineistot, jos tiedon oikeudeton paljastuminen ja käyttö vaarantaisi viranomaisen toimintaedellytyksiä taikka liike- ja ammattisalaisuuksia tai henkilötietojen suoja.

Pääosa erityissuojattavista tiedoista on salassa pidettäviä. Ensimmäiseen ja toiseen turvaluokkaan kuuluvat kaikki aineistot ovat salassa pidettäviä. Kaikki salassa pidettävät tiedot ovat erityissuojattavia.

Liite 2.2

SALASSA PIDETTÄVIEN ASIAKIRJOJEN LEIMAT

Salassa pidettävät asiakirjat leimataan asianmukaisella leimalla. Leiman koko on 7 x 1,8 cm. Leiman väri on punainen. Leiman alle voi asiakirjan laatija merkitä asiakirjasalaisuuden lakkaamispäivämäärän.

Alla olevat leimat ovat virallisia perusleimoja. Esitysteknisistä syistä voidaan sisäisissä ja epävirallisissa yhteyksissä käyttää myös muun kokoisia leimoja. Muun muassa ulkoasiain- ja puolustushallinnossa on käytössä myös muita leimoja.

1) TURVALUOKITELLUT ASIAKIRJAT

Turvaluokiteltu I
ERITTÄIN SALAINEN
JulkL (621/1999) 24.1 §:n _____k

Turvaluokiteltu II
SALAINEN
JulkL (621/1999) 24.1 §:n _____k

Turvaluokiteltu III
LUOTTAMUKSELLINEN
JulkL (621/1999) 24.1 §:n _____k

2) MUUT SALASSA PIDETTÄVÄT ASIAKIRJAT

SALASSA PIDETTÄVÄ
JulkL (621/1999) 24.1 §:n _____k
Muun lain (___/___) _____ §:n _____

LIITE 3

OHJEEN RAJAUS

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeeseen ei sisälly

- Virastokohtaisen tietoaineistojen käsittelyvaltuuksien myöntämisen ja niiden valvonnan yksityiskohtaista ohjeistamista. Virastokohtaista ohjeistusta tehtäessä on syytä muistaa riittävä tehtävien eriyttäminen vaarallisten työyhdistelmien välttämiseksi.
- EU-asiakirjojen luokittelun yksityiskohtaista ohjeistusta.
- Salauskäytäntöjen tarkkaa käsittelyä. Näiden ohjeistusta valmistellaan parhaillaan valtionhallinnon tietoturvallisuuden johtoryhmässä.
- HST-kortin tai vastaavat ominaisuudet sisältävän virkamiehen asiointikortin käyttöä salassa pidettävien tietojen käsittelyssä.
- Turvaluokittelun ja salassapidon päättymiseen liittyvien toimenpiteiden tarkkaa määrittelyä.
- Tietoturvaluokittelun määrittelyä, koska näistä on olemassa valtionhallinnon tietoturvallisuuden johtoryhmän tuore julkaisu (VAHTI 1/2000).
- Henkilöiden luotettavuuden varmistusmenettelyiden ohjeistusta, koska henkilöstöturvallisuustoimikunnan valmistelemana, lausuntokierroksella olevassa komiteamietinnössä on käsitelty näitä asioita (OM/komiteamietintö/2000:2).
- Valtionhallinnon asiakirjojen kirjaamiskäytäntöjen ohjeistamista. Arkistolaitos uusi vuoden 2000 aikana ohjeensa 1/06/1995 ”Kirjaaminen valtion virastoissa ja laitoksissa”.
- Turvaluokittelun muuttumiseen asiakirjan pitkän elinkaaren aikana liittyvää menettelytapaohjeistusta.
- Tarpeettomien tietoaineistojen hävittämisen tarkempaa ohjeistusta. VM on antanut asiaa koskevan yleisohjeen 19.4.2000.
- Kannanottoja siihen, milloin sähköinen asiointi on mahdollista viranomaisessa tietoturvaluokittelun näkökulmasta.
- Tarkempaa ohjeistusta tietoteknisten lokien ja varmuuskopioinnin teknisestä järjestämisestä.
- Toimintojen ja tietohallintotoimintojen ulkoistamisen tietoturvaluokittelun vaatimuksia, jotka on ohjeistettu valtionhallinnon tietoturvallisuuden johtoryhmän toimesta (VAHTI 2/1999).
- Yksityiskohtaista henkilötietojen käsittelyn tietoturvallisuuden ohjeistamista.