11.1 § kohta 1 Tietojärjestelmien erottelu

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikenne-järjestelyt on toteutettava siten, että:
1) ne erotetaan niissä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän luotettavasti alemman turvallisuustason tietojärjestelmistä ja tietoliikennejärjestelyistä;

Turvallisuusluokan IV tietojärjestelmien ja tietoliikennejärjestelyjen erottelu eri turvallisuusluokan ympäristöistä voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla turvallisuuskriittisten alemman turvallisuusluokan palvelujen (web-selailu, sähköposti, ja vastaavat) liikenne kulkemaan erillisten sisältöä suodattavien välityspalvelinten kautta. Turvallisuusluokan IV tietojärjestelmiä ja tietoliikennejärjestelyjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, kunhan turvallisuusluokan muut vaatimukset täyttyvät. Tyypillinen käyttötapa turvallisuusluokan IV käsittely-ympäristölle on organisaation "toimistoverkon" tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi työasemista ja asianhallintajärjestelmistä sekä niiden suojaamiseen liittyvistä järjestelyistä (palomuuraus, käyttöoikeushallinto, jne.). Vastaava erottelu soveltuu myös turvallisuusluokittelemattoman salassa pidettävän tiedon suojaamiseen, kuten myös julkisen tiedon eheyden ja käytettävyyden suojaamiseen.

Turvallisuusluokasta III lähtien erottelu eri turvallisuusluokkien ympäristöihin voidaan toteuttaa riittävän turvallisilla yhdyskäytäväratkaisuilla. Tällaisia ovat esimerkiksi vain yhdensuuntaisen liikennöinnin mahdollistavat datadiodiratkaisut. Turvallisuusluokan II tietojärjestelmien ja tietoliikennejärjestelyjen erottelu voidaan toteuttaa lähtökohtaisesti vain korkean luotettavuuden tarjoavilla datadiodiratkaisuilla. Turvallisuusluokan I tietojärjestelmien ja tietoliikennejärjestelyjen erottelussa tulee lisäksi huomioida, että erottelu tulee toteuttaa lähtökohtaisesti täydellisellä fyysisellä eristämisellä, ja vain poikkeustapauksissa datadiodiratkaisuilla.

Tietojärjestelmien ja tietoliikennejärjestelyjen liittämisessä on otettava huomioon myös kansainväliset tietoturvavelvoitteet, joissa liittäminen voi olla kokonaan kielletty. Valtionhallinnon viranomainen voi myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) mukaan pyytää Liikenne- ja viestintävirastolta tietojärjestelmän tai tietoliikennejärjestelyjen vaatimustenmukaisuuden arviointia. Arvioinnin pyytäminen erityisesti turvallisuusluokkien I ja II tietojärjestelmien ja tietoliikennejärjestelyjen liittämisestä matalamman turvallisuusluokan tietojärjestelmiin tai tietoliikennejärjestelyihin on suositeltavaa, jotta tietojärjestelmän tai tietoliikennejärjestelyn turvallisuudesta vastuussa olevalla viranomaisella on riskienhallintapäätöstensä tueksi käytettävissään myös Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntija-arvio liittämiseen mahdollisesti liittyvistä jäännösriskeistä.

Turvallisten yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä ratkaisumalleja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ohjeessa.

Kyberturvallisuuskeskuksen Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista
(www.ncsa.fi > Yhdyskäytäväratkaisuohje).

Kyberturvallisuuskeskuksen Ohje Liikenne- ja viestintävirasto Traficomin suorittamista tietojärjestelmien arviointi- ja hyväksyntäprosesseista.