

**VALTIONHALLINNON  
TIETOJÄRJESTELMÄKEHITYKSEN  
TIETOTURVALLISUUSSUOSITUS**

## SISÄLTÖ

|  |           |
|--|-----------|
| <b>1 Johdanto</b> .....  | <b>3</b>  |
| 1.1 Suosituksen tarkoitus ja rajausta.....   | 3         |
| 1.2 Suosituksen tausta ja laatiminen .....   | 4         |
| <b>2 Yhteenvedo suosituksesta</b> .....  | <b>5</b>  |
| <b>3 Yleistä järjestelmäkehityksestä</b> .....   | <b>8</b>  |
| 3.1 Säädosperusta.....   | 8         |
| 3.2 Perusinfrastruktuuri ja järjestelmäkehityksen tietoturvaluus .....                                 | 9         |
| 3.3 Suosituksessa käytettävä järjestelmäkehitysmalli .....   | 9         |
| <b>4 Järjestelmäkehityksen tietoturvaluusriskeistä</b> .....   | <b>10</b> |
| <b>5 Järjestelmäkehityksen tietoturvaluuden hallinnointi</b> .....                                     | <b>11</b> |
| 5.1 Tietojärjestelmien tietoturvaluusvastuiden työnjako .....  | 11        |
| 5.2 Projektityön tietoturvaluus .....  | 14        |
| 5.3 Järjestelmäkehityksen laadun varmistaminen tietoturvaluusnäkökulmasta.....                         | 16        |
| <b>6 Tietoturvaluusvaatimukset järjestelmän elinkaaren eri vaiheissa</b> .....                         | <b>18</b> |
| 6.1 Järjestelmän esitutkimus .....   | 19        |
| 6.2 Järjestelmän määrittely .....  | 21        |
| 6.3 Järjestelmän suunnittelu.....  | 24        |
| 6.4 Järjestelmän toteutus.....   | 26        |
| 6.5 Järjestelmän käyttöönotto .....  | 27        |
| 6.6 Järjestelmän ylläpito .....  | 30        |
| 6.7 Järjestelmän tuotantoaikainen käyttö .....   | 31        |
| 6.8 Järjestelmän version vaihto.....   | 32        |
| 6.9 Järjestelmän poisto käytöstä (alasajo).....  | 33        |
| 6.10 Testaus ja laadunvarmistus .....  | 34        |
| <b>7 Järjestelmäkehityksen tietoturvaluuden erityiskysymyksiä</b> .....                                | <b>35</b> |
| 7.1 Valmiusvaiheen poikkeusolojen alasajo ja palautus.....   | 35        |
| 7.2 Tietoturvaluus valmisohjelmistojen hankinnoissa .....  | 35        |
| 7.3 Sopimukset.....  | 36        |
| 7.4 Avoimissa tietoverkoissa toteutettavien tietojärjestelmien tietoturvaluuden erityispiirteitä ..... | 38        |
| <b>8 Keskeiset lähteet</b> .....   | <b>40</b> |
| <b>9 Liitteet</b> .....  | <b>41</b> |
| Liite 1: Tietoturvaluutta koskevaa lainsäädäntöä ja ohjeistusta  |           |
| Liite 2: Suosituksessa käytettävä järjestelmäkehitysmalli  |           |
| Liite 3: Tietojärjestelmän elinkaaren eri vaiheiden tietoturvaluustarkistuslistat                      |           |

## 1 Johdanto

Suosituksen sisältöalue on valtionhallinnon tietojärjestelmät. Suosituksen antamisen toimivalta perustuu valtioneuvoston ohjesäännön (VNOS, 1522/1995, muut. 8566/27.8.1999) 19§:n 19 kohtaan. Kohderyhminä ovat ministeriöt, virastot ja laitokset. Suositus tulee voimaan 1.12.2000. Suositus täydentää mm. viranomaisen toiminnan julkisuudesta annetun lain (621/1999) sekä sen perusteella annetun asetuksen (1030/1999) sääntelyä.

### 1.1 Suosituksen tarkoitus ja rajaus

Valtionhallinnon tietojärjestelmäkehityksen tietoturvaluussuosituksen tarkoituksena on:

- parantaa valtionhallinnon tietojärjestelmien tietoturvaluuden tasoa yhtenäistämällä tietoturvaluuden tavoitteiden määrittelyä ja toteuttamista järjestelmäkehityksen eri vaiheissa
- tukea valtion organisaatioita järjestelmäkehityshankkeiden läpivienteihin ja valmisohjelmistojen hankintoihin liittyvissä tietoturvaluustehtävissä.

Suositus on apuväline tietoturvaluusvaatimusten huomioimiseen jo järjestelmän elinkaaren alkuvaiheista (esitutkimus, määrittely, suunnittelu) lähtien.

Suositus määrittelee suositeltavia tietoturvaluusvaatimuksia ja niiden toteutus- ja toimintatapoja järjestelmäkehitys- ja valmisohjelmistohankkeiden läpiviennissä sekä nykyisessä markkina- ja Internet-painotteisessa nopeiden suunnittelumenetelmien tietojärjestelmäkehityksessä. Suositukseen sisältyy hallinnollisia ja teknisiä linjauksia järjestelmäkehityksen laadun varmistamiseen tietoturvaluusnäkökulmasta.

Suositus on suunnattu erityisesti valtionhallinnon järjestelmäkehittäjille, muita kohderyhmiä ovat johto sekä tietohallinto-, tietoturvaluus- ja turvallisuusvastaavat.

Suosituksen avulla valtionhallinnon organisaatiot voivat systemaattisesti nykyistä kiinteämmin liittää tietoturvaluuden varmistamisen osaksi normaalia järjestelmäkehitystoimintaa. Suositus on lisäksi apuväline niiden tietojärjestelmätoimittajien ohjaamisessa, joilta valtionhallinto hankkii järjestelmäkehitystyötä. Suositus voi toimia vaatimusmäärittelyn tukena tietojärjestelmätyötä hankittaessa ja esimerkiksi tarjouspyyntömenettelyissä.

Suosituksen painopiste on tietojärjestelmän elinkaaren alkupäässä, valmistamis-/ hankintavaiheessa, muuta elinkaarta käsitellään karkeammalla tasolla. Painotus on tietojärjestelmien tietoturvaluudessa, infrastruktuurin tietoturvaluutta sivutaan silloin, kun sillä on suoria tai suuria välillisiä vaikutuksia tietojärjestelmien tietoturvaluuteen.

Tietoturvaluusvaatimukset ja -riskit on käsitelty järjestelmäkehityksen eri vaiheissa. Tehtävien ja lopputulosten määrittely sekä tarkistuslistat ja vastuutahojen roolitarkastelut on tehty järjestelmän elinkaaren vaiheiden mukaisesti. Suosituksessa on käsitelty järjestelmäkehityksessä usein esille tulevia hallinnollisen tietoturvaluuden ja infrastruktuurin muutostarpeita.

Kunkin organisaation rakenne ja tekninen infrastruktuuri vaikuttavat tietoturvaluuden (tekniseen) toteutustapaan, eikä se ole yleisesti kuvattavissa eikä ohjeistettavissa. Yleisiä tarjouspyyntöjen liitteitä ei siten ole mahdollista laatia, kunkin organisaation on muodostettava ne tarkistuslistojen avulla oman organisaationsa lähtökohdista.

Tässä suosituksessa ei ole otettu kantaa paperittomaan kirjanpitoon. Asiasta on vireillä Valtiovarainministeriön ja Valtiokonttorin yhteishanke, josta on odotettavissa ohjeita vuonna 2001.

## 1.2 Suosituksen tausta ja laatiminen

Tietoturvaluussuosituksen valmistelutarve koskien tietojärjestelmäkehityksen tietoturvaluutta valtionhallinnossa on tullut esille muun muassa valtionhallinnon tietoturvaluuden johtoryhmässä käydyissä keskusteluissa ajankohtaisista tarpeista koko valtionhallintoa koskeville tietoturvaluusohjeille sekä valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvaluussuosituksen (VAHTI 2/1999) valmistelutyössä. Tarvittavien tietoturvaluusominaisuuksien rakentaminen jälkikäteen jo käyttöön otettuihin järjestelmiin on todettu kalliiksi ja osittain mahdottomaksi. Järjestelmien ja niiden tietojen käytettävyys, eheys ja luottamuksellisuus tulee varmistaa.

Valtiovarainministeriön hallinnon kehittämisosaston 31.3.2000 asettama työryhmä on toiminut valtiovarainministeriön asettaman valtionhallinnon tietoturvaluuden johtoryhmän (VAHTI) alaisuudessa ja ohjauksessa. Työryhmässä ovat toimineet:

*puheenjohtaja:*

**Kiviniemi, Mikael**, neuvotteleva virkamies, valtiovarainministeriö

*jäsenet:*

**Heikkilä, Ville**, ylitarkastaja, oikeusministeriö

**Kupari, Jukka**, järjestelmäintegraattori, väestörekisterikeskus

**Tuomi, Sirkka**, tietohallintovastaava, tielaitos

**Uutinen, Ari**, turvallisuuspäällikkö, valtioneuvoston kanslia

**Vehmas, Keijo**, ylitarkastaja, verohallitus.

Valmistelutyöhön ovat osallistuneet myös tietoturvapäällikkö Risto Alhava väestörekisterikeskuksesta, tietoturvapäällikkö Timo Tuomaila verohallituksesta ja Markku Nousiainen oikeusministeriöstä. Konsulttina on toiminut Aarno Kansikas, ICL:stä.

Tietoturvaluussuosituksen luonnoksesta 9.10.2000 pyydettiin mahdollisia lausuntoja ministeriöiltä, valtion virastoilta ja laitoksilta sekä Tietoturva Ry:ltä. Saatujen 33 lausunnon pohjalta viimeistelty suositus hyväksyttiin valtionhallinnon tietoturvaluuden johtoryhmässä 17.11.2000.

## **2 Yhteenveto suosituksesta**

### **Suosituksen tarve ja reunaehdot**

Tietoturvaluussyö on oleellinen ja kiinteä osa tietojärjestelmien kehittämistehtävistä. Kehittämiseen osallistuvilla tulee olla tietoturvaluuden ja erityisesti järjestelmäkehityksen tietoturvaluuden perustuntemus. Projektin asettajan vastuu tietoturvaluusnäkökulman huomioimisesta korostuu.

Ylin johto määrittelee tietoturvaluuden keskeiset periaatteet esimerkiksi osana toiminta- ja tietohallintostrategiaa sekä päättää merkittävistä hankkeista ja hankinnoista. Johto osallistuu myös liiketoiminnalle kriittisten järjestelmäkehityshankkeiden tavoitteen asetteluun ja valvontaan. Valtion talousarvioasetuksen mukaan viraston ja laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt (sisäinen valvonta).

Useat lait, asetukset sekä suositukset ja ohjeet sisältävät viranomaisia koskevia tietoturvaluusvelvoitteita, jotka on otettava lähtökohdiksi myös tietojärjestelmien tietoturvaluudelle.

Tietojärjestelmien eheysvaatimus (luotettavuus) sisältyy lähes kaikkiin säädöksiin, tietojen luottamuksellisuus- ja suojausvaatimukset yleislakeihin, käytettävyysvaatimukset korostuvat valmiuslaeissa.

Henkilötietojen suojaamiseen osana tietoturvaluutta tulee kiinnittää tarvittava erityishuomio mm. tietoturvariskien hallinnassa, vastuiden määrittelyssä, projektityön tietoturvaluudessa sekä järjestelmäkehityksen elinkaaren eri vaiheissa.

### **Infrastrukturi**

Organisaatiolla tulee olla muun muassa tietoturvaluuspolitiikka, perusturvaluuden tietoturvaluussuunnitelma, tietoturvaluus-arkkitehtuuri, perusinfrastruktuurin tietoturvaluusratkaisut sekä toiminnassa olevat toipumis- ja varmistusmenettelyt. Nämä huomioidaan ja niitä hyödynnetään tietojärjestelmiä kehitettäessä ja käyttöönottaessa. Teknologian kehitys ja järjestelmien kehittämistarpeet voivat edellyttää uusia tietoturvaluusratkaisuja.

Uusi tietojärjestelmä saattaa aiheuttaa tiukempia vaatimuksia nykyisen infrastruktuurin turvaamiselle. Tällöin on tarpeen tarkistaa ja mahdollisesti päivittää perusturvaluuteen liittyvät periaatteet ja ratkaisut sekä suorittaa tarvittavat infrastruktuurin kehittämistoimenpiteet.

## Vastuut

Tietojärjestelmän kehittämisessä on monia osapuolia, joilla on kullakin omat tehtävänsä ja roolinsa kehitysohjelmassa myös tietoturvaluusvastuineen.

Tietoturvaluudesta vastaa johto. Tietojärjestelmän elinkaaren eri vaiheissa johdolla, järjestelmän omistajalla, tietohallintovastaavalla, tietoturvaluusvastaavalla, projekti-päälliköllä, projektiryhmällä, projektin ohjausryhmällä, audittoijalla, järjestelmän ylläpitäjällä ja sisäisellä tarkastuksella on omat erityiset kohdissa 5.1 ja 6 kuvatut tietoturvaluustehtävänsä.

## Tietojärjestelmän elinkaaren eri vaiheiden tietoturvaluus

Suosituksen perustana olevan elinkaarimallin mukaisesti tietojärjestelmän esitutkimusvaiheessa valitaan turvaluusaste ja hahmotetaan tietoturvaluusvaatimukset, lopputuloksina ovat muun muassa järjestelmän tärkeysluokitus, turvaamistarpeet ja turvaamistaso. Tietoturvaluus tulee varmista koko elinkaaren aikana.

Järjestelmän esitutkimusvaiheen tietoturvaluuskartoitus ja -tason valinta on hyvin tärkeä tehtävä, koska siinä luodaan perusta järjestelmän koko elinkaaren tietoturvaluuden varmistamiselle. Tavoiteltava tietoturvaluusaste tulee ottaa huomioon kustannusarvioissa. Määrittelyvaiheessa määritetään tietoturvaluusratkaisut, lopputuloksena ovat muun muassa tietoturvaluusmääritykset ja tarkennetut tietoturvaluusvaatimukset.

Suunnitteluvaiheessa tietoturvaluusratkaisut suunnitellaan ja lopputuloksina ovat muun muassa tietoturvaluusratkaisujen toteutus- ja testausuunnitelmat.

Toteutusvaiheessa kehitysympäristö turvataan ja tietoturvaluusratkaisut toteutetaan sekä testataan, lopputuloksina ovat muun muassa testatut tietoturvaluusratkaisut.

Valmisratkaisujen hankinnan vaatimusmäärittelyjen ja testauksen yhteydessä hyödynnetään elinkaaren eri vaiheiden tarkistuslistoja, soveltamisen tapa on kohdealueriippuvaisista. Edeltävät suunnitteluvaiheet suoritetaan normaalisti päädyttyä valmisratkaisuihin.

Käyttöönottovaiheessa tietoturvaluustoimet hyväksymistestataan ja otetaan käyttöön, lopputuloksena on muun muassa turvattu tietojärjestelmä ja ohjeisto.

Käyttövaiheessa tietoturvaluusjärjestelyjen toimintaa seurataan ja käyttöympäristöä hallitaan, lopputuloksena ovat muun muassa tietoturvaluuden tilanneraportit.

Ylläpitovaiheessa tietoturvaluustoimia ylläpidetään ja käyttöympäristöä hallitaan lopputuloksina ovat muun muassa muutetut tietoturvaluustoimet.

Version vaihdon yhteydessä arvioidaan ja suoritetaan tarvittavat tietoturvaluustoimien muutokset, sekä tietoturvaluustoimien vaihdon turvatoimet, lopputuloksina ovat muun muassa tietoturvaluustoimien muutokset.

Käytöstä poiston yhteydessä turvataan poistotoimet ja järjestelmäliitännöiden muutokset, lopputuloksina ovat muun muassa hallitusti passivoitu järjestelmä ja aineistot. Passivointi dokumentoidaan.

Testaus ja laadunvarmistus ovat osa tietojärjestelmän kehityksen kaikkia vaiheita. Testauksella todetaan, että vaiheen tehtävät on tehty ja tehdyt ratkaisut toimivat ja ovat hyväksyttävissä. Laadunvarmistuksella seurataan, että työ on hyvin ja tehokkaasti tehty ja lopputulokset ovat laadukkaita sekä sisäisesti että ulkoisesti.

Suosituksessa esitettyä elinkaarimalli-lähestymistapaa voidaan soveltaa eri vaihejakoihin sekä esimerkiksi ns. nopeaan järjestelmäkehitysmalliin. Kuvatut tehtävät on suoritettava tässä lähestymistavassa kuvatulla tavalla ryhmiteltiin ne millä tahansa vaihejakomallilla. Lisäksi ylläpito- ja version vaihto –vaiheet poikkeavat muista vaiheista siltä osin, että ne pitävät sisällään toimintoja muista vaiheista. Esimerkiksi ylläpito (pienimuotoiset järjestelmän muutokset) kattaa toimintoja määrittelystä järjestelmän toimitukseen. Version vaihto (laajat järjestelmämuutokset) kattaa toimintoja esitutkimuksesta järjestelmän toimitukseen sekä väistyvän järjestelmän osalta käytöstä poiston.

Yhteiskunnan ja viranomaisen kannalta tärkeillä järjestelmillä on omat menettelynsä jotka on luotu normaalioloissa. Valmiusvaiheen poikkeusolojen alasajo ja palautus tehdään esimerkiksi siten että erillinen suppeampi järjestelmä otetaan käyttöön. Se voi käytännössä olla jopa eri järjestelmä jopa eri organisaation tekemänäkin. Tietoturvallisuudesta huolehditaan soveltaen vastaavien vaiheiden tietoturvaluustehtäviä, -tarkastuslistoja, lopputuloskuvauksia sekä vastuita.

Yhteenvetokaavio tietojärjestelmän elinkaaren eri vaiheiden tietoturvaluustehtävistä ja –tuloksista on esitetty kohdan 6 alussa.

### **Valmisohjelmistojen hankinta**

Myös valmisohjelmistoon perustuvan tietojärjestelmän tietoturvaluus tulee varmistaa elinkaaren kaikissa vaiheissa. Suosituksessa esitetyt tietoturvaluustehtävät ovat pääosin riippumattomia siitä, tehdäänkö kehitystyö viraston omien tietojärjestelmäkehittäjien vaiko sovelluskehitysyrityksen toimesta. Valmisohjelmistojen hankinnan osalta tulevat sovellettavaksi muun muassa esitutkimus-, määrittely- ja käyttövaiheiden tietoturvaluustehtävät. Valmisohjelmistojen pohjalta tehtävään räätälöintiin kannatta myös käyttää hyväksi kohdan 6 suosituksia. Valmisohjelmistojen hankinnan elinkaaren vaiheesta riippumattomia tietoturvaluusvarmistamisen tarkistuslista on esitetty kohdassa 7.2.

### **Suosituksen toimeenpanosta**

Suosituksen esittämää lähestymistapaa suositellaan sovellettavaksi erityisesti organisaation tärkeimpiin tietojärjestelmiin ja merkittäviin tietojärjestelmähankeisiin. Viraston tulee ottaa tämä suositus huomioon muun muassa järjestelmäkehityshankkeisiin osallistuvan henkilöstön koulutussuunnitelmissa.

### 3 Yleistä järjestelmäkehityksestä

#### 3.1 Säädosperusta

Tietoturvaluus on toteutettava ympäristössä, jossa toisaalta on toteutettava julkisuutta (hallinnon julkisuus) ja toisaalta turvattava henkilöiden yksityisyyttä ja valtion turvaluusua. Pääsääntönä on asiakirjan tai sitä vastaavan tietojoukon julkisuus, salassapito on poikkeus ja siitä on säädetty lailla. Ne tiedot, joiden paljastuminen vaarantaisi keskeisten yksityisten tai julkisten etujen toteutumisen, on pidettävä salassa ja niiden suojaamisesta on huolehdittava asianmukaisesti. Päätöksenteossa tarvittavan tiedon tulee myös olla viranomaisen käytettävissä; oikeusturvan kannalta on keskeisintä se, että nämä tiedot ovat samalla oikeita ja asianmukaisia.

Keskeinen julkisuutta ja tietojen suojaamista koskeva säädos on **Laki viranomaisten toiminnan julkisuudesta (JulkL 621/1999) ja vastaava asetus (JulKA 1030/1999)**. Laki asettaa viranomaisille velvoitteen suojata tietojärjestelmät.

Julkisuuslain 3 §:ssä ilmaistaan, että siinä säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien erityisenä tavoitteena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa. Näitä viranomaisille asetettuja hyvän tiedonhallintatavan mukaisia velvoitteita ovat (JulkL 18, 1 §):

- julkisuuden toteutumista palvelevien asialuetteloiden ja tietojärjestelmäkuvausten 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.

Julkisuuslain 18 §:n 1 momentin 1 ja 2 kohdassa tarkoitetut luettelot ja kuvaukset on laadittava vuoden kuluessa lain voimaantulosta - so. 1.12.2000 mennessä. Tietojärjestelmät on suojattava ja niissä olevien tietojen suoja, eheyttä ja laatua turvaavat toimenpiteet toteutettava viiden vuoden kuluessa lain voimaantulosta - so. 1.12.2004 (Laki JulkL 38 §:n muuttamisesta - 636/2000).

Henkilörekistereihin talletettujen tietojen käsittelyä säädelään **Henkilötietolalla (523/1999)**. Sen 32 §:ssä säädetään henkilö tietojen suojaamisesta seuraavasti:

“Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilö tietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämiselta taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta”.

Luettelo keskeisistä tietoturvaluuteen liittyvistä kansallisista normeista on liitteenä 1. Tietoturvaluotteita sisältyy lisäksi kansainvälisiin säädöksiin, kuten EU direktiivit.

Tietojärjestelmien eheysvaatimus (luotettavuus) sisältyy lähes kaikkiin säädöksiin, tietojen luottamuksellisuus- ja suojausvaatimukset yleislakeihin, käytettävyyksivaatimukset korostuvat valmiuslaeissa.

### **3.2 Perusinfrastruktuuri ja järjestelmäkehityksen tietoturvaluus**

Uusia tietojärjestelmiä suunniteltaessa ja käyttöönotettaessa perusinfrastruktuurin tietoturvaluusratkaisut otetaan huomioon ja käytetään valmiina olevia ratkaisuja hyväksi. Ellei näitä ole, on harkittava erillisiä kehittämissuhteita joita voivat olla esimerkiksi:

- tietoturvaluuspolitiikka
- uhka / -riskianalyysi
- tietoturvaluusarkkitehtuuri ja kehittämissuhteita / -ohjelma
- jatkuvuussuunnitelmat, turva-, toipumis-/elpymis- ja valmiuussuunnitelmat
- infrastruktuurin tietoturvaluusratkaisut
- tietoturvaluusohjeistot
- tietoturvaluuskoulutus ja tietoturvaluustietoisuuden kasvattaminen
- tietoturvaluusauditoinnit.

Perusinfrastruktuurin tietoturvaluuden kehittämiseen saattaa vaikuttaa vaatimusnäkökohdan lisäksi tarjontanäkökulma. Alan tuotekehitys tuottaa ratkaisuja, joita ei aikaisemmin ole ollut tai niiden käyttöönotto on ollut liian kallista.

Toisaalta uusi tietojärjestelmä saattaa aiheuttaa uusia tiukempiakin tietoturvaluusvaatimuksia nykyisen infrastruktuurin turvaamiselle. Tällöin saattaa olla tarpeen tarkistaa ja mahdollisesti päivittää olemassa olevia perusturvaluuteen liittyviä periaatteita ja ratkaisuja jopa omina rinnakkaisprojekteinaan. Kehittämiskohteita voivat olla esimerkiksi edellä mainitut kohteet.

Infrastruktuurilinjauksia tehtäessä tietoturvaluuteen tulee kiinnittää erityistä huomiota. Esimerkiksi tietoverkon suorituskykyyn ja laajentamiseen liittyvät ratkaisut voivat oleellisesti vaikuttaa tietojen käytettävyyteen, luottamuksellisuuteen ja eheyteen.

Tietojärjestelmien valmistamisen yhteydessä on selvitettävä perusinfrastruktuurin tietoturvaluusratkaisut etenkin muutostilanteissa. Mikäli olemassa olevat ratkaisut eivät ole riittäviä tulevan tietojärjestelmän tietoturvaluustarpeisiin nähden, on suoritettava tarvittavat infrastruktuurin kehittämistoimenpiteet.

### **3.3 Suosituksessa käytettävä järjestelmäkehitysmalli**

Tässä suosituksessa järjestelmäkehitys ja siihen liittyvä tietoturvaluuden kehittämissuhteita kuvataan perinteisen elinkaarimallin käsitteillä. Elinkaarimallin tulkinnaassa otetaan myös vaikutteita oliopohjaisen työskentelyn iteratiivisesta lähestymistavasta. Painopiste on elinkaaren alkupäässä. Myöhempiä vaiheita käsitellään karkeammalla tasolla. Suosituksessa käytettävä järjestelmäkehitysmalli on liitteenä 2.

## 4 Järjestelmäkehityksen tietoturvaluusriskeistä

### Järjestelmäkehityksen tietoturvaluusriskien hallinta

Kontrollien avulla pyritään edesauttamaan tavoitteiden saavuttamista. Kontrollien avulla pyritään estämään ei-toivottujen tapahtumien esiintymistä, alentamaan niiden todennäköisyyttä tai pienentämään niiden haitallista vaikutusta hyväksyttävälle riskitasolle. Kontrollit voivat olla joko peruskontrolleja, eli koko tietojenkäsittely-ympäristöä suojaavia tai erityiskontrolleja, eli tietylle sovellukselle ominaisia. Tietoturvaluustoimenpiteet ovat kontrolleja, joko perus- tai erityiskontrolleja.

Organisaation tulee selvittää sen hetkiset tietoturvaluusjärjestelynsä ja tarvittaessa parantaa tietoturvaluutta. Tietoturvaluuden kehittämistä päätettäessä on arvioitava:

- miten arvokasta tieto on organisaatiolle ja sen sidosryhmille
- miten paljon resursseja tai rahaa on käytetty tiedon tuottamiseen
- miten helposti tai vaikeasti muut voisivat kopioida tiedon
- minkälaisia seurauksia olisi siitä, että tieto tulisi julki organisaation ulkopuolella.
- mitkä tapahtumat uhkaavat tietoja ja tietojärjestelmiä, kuinka todennäköisiä ne ovat ja mitkä olisivat niiden seuraamukset
- liittymät muihin organisaatioturvaluuden turvaluusalueisiin
- selkeät vastuunjaot tietojärjestelmän koko elinkaaren aikana, tietojärjestelmän ja tietojen omistajuus
- laatujärjestelmäliittymät
- vaaralliset työyhdistelmät
- reagointimenettelyt, raportointimenettelyt, ennalta reagointi
- säädökset, jotka vaikuttavat asiaan
- henkilötietojen suojaaminen
- miten laajalti työhön liittyvä informaatio tunnetaan organisaation ulkopuolella
- miten yleisesti informaatio on organisaation henkilöstön tiedossa.

## **5 Järjestelmäkehityksen tietoturvallisuuden hallinnointi**

### **5.1 Tietojärjestelmien tietoturvaluusvastuiden työnjako**

Tietoturvaluusustyö on oleellinen ja kiinteä osa tietojärjestelmäkehittämisen tehtävistä. Kaikilla tietojärjestelmäkehittämiseen osallistuvilla tulee olla tietoturvaluuden ja erityisesti järjestelmäkehityksen tietoturvaluuden perustuntemus. Myös projektin asettajan vastuuta tietoturvaluusnäkökulman huomioimisesta on korostettava. Esimerkiksi tietoturvaluuskustannusten etukäteisbudjetointi tulee tehdä. Monissa hankkeissa korostuvat henkilötietojen suojaamiseen liittyvät tehtävät osana tietoturvaluusustyötä.

Tietojärjestelmän kehittämisessä on monia osapuolia, joilla on kullakin omat tehtävänsä ja roolinsa kehitysojektissa myös tietoturvaluusvastuineen.

Seuraavassa esitetään suositeltavia tietoturvaluuden vastuunjakoja. Vastuunjakojen tarkka määrittely on organisaatiokohtainen. Tärkeää on, että organisaatiossa on jaettu selkeästi vastuut eri osapuolien kesken.

#### **Johto**

Ylin johto määrittelee tietoturvaluuden keskeiset periaatteet esimerkiksi osana toiminta- ja tietohallintostrategiaa sekä päättää merkittävistä hankkeista ja hankinnoista. Johto osallistuu myös toiminnalle kriittisten järjestelmäkehityshankkeiden tavoitteenasetteluun ja valvontaan. Valtion talousarvioasetuksen mukaan viraston ja laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt (sisäinen valvonta). Johdon sitoutuminen tietoturvaluuskulttuurin ja tietoturvaluushankkeiden edistämiseen on ensiarvoisen tärkeää.

#### **Järjestelmän omistaja**

Järjestelmän omistaja on esimerkiksi sen osaston tai yksikön johtaja, jonka toiminnan tueksi järjestelmä kehitetään. Omistajan rooliin kuuluu vastata määrittelystä tai määrittellä järjestelmälle asetettavat vaatimukset ml. tietoturvaluusvaatimukset, varata käyttäjäorganisaation resurssit projektityöhön, vastata hyväksymisestä tai hyväksytyä vaihekohtaiset tulokset sekä vastata järjestelmän hyväksymistestauksesta ja käyttäjien koulutuksen järjestämisestä.

Järjestelmän omistaja, jos on yksikön/osaston johtaja ei hyväksy esimerkiksi vaihekohtaisia tuloksia useinkaan, vaan nämä tekee ohjausryhmä (jossa johtaja voi olla mukana). Johtaja vastaa että kohdassa mainitut asiat tehdään.

## **Tietohallinto / tietotekniikkavastaava**

Tietotekniikkavastaava varmistaa, että projektilla on käytettävissään ohjelmiston kehitysympäristö ja tarvittavat kehitysvälineet sekä näissä tarvittava tekninen tuki. Rooliin kuuluu myös varmistaa, että järjestelmä on organisaation tietohallintostrategian ja teknisen arkkitehtuurin sekä tietoarkkitehtuurin mukainen. Vastuualueeseen kuuluu myös tuotantoon siirto ja tuotannon aikaisen käyttöympäristön hallinta.

Tietohallintovastaavan tehtävinä ovat myös laadunvarmistus, projektisalkun hallinta, kehittämistyön koordinointi, menetelmäkonsultointi ja niihin liittyvät tietoturvaluusnäkökohdat.

## **Tietoturvaluusvastaava**

Tietoturvaluusvastaavan rooliin kuuluu varmistaa, että kehitettävä järjestelmä vastaa organisaation tietoturvaluusvaatimuksia ja on hyväksytyt tietoturvaluuspolitiikan ja tietoturvaluusarkkitehtuurin mukainen. Tietoturvaluusvastaava tukee tietoturvaluuden suunnittelua ja toteutusta, tarkastaa tietoturvaluustehtävien vaihekohtaiset tulokset sekä varmistaa, että organisaatiolla on järjestelmässä käytettävästä tietoturvaluusustekniikasta riittävä asiantuntemus. Tietoturvaluusvastaava seuraa tietoturvaluuskokonaisuutta projektissa ja esittää tarvittavia kehittämistoimia. Käytön aikainen tietoturvaluuslokien seuranta kuuluu tehtäviin, ellei siitä ole tapauskohtaisesti päätetty muuta käytäntöä.

## **Projektipäällikkö**

Projektipäällikkö vastaa kehitysprojektin hallinnasta, varmistaa projektin vaikutuspiiriin kuuluvien osapuolten edustuksen projektissa, vastaa sovittujen toimintakäytäntöjen ja standardien noudattamisesta ja lopputuloksen laadusta sekä selvittelee ja hakee ratkaisut mahdollisiin ristiriitatilanteisiin. Projektipäällikkö, joka vastaa myös aikataulusta ja kustannuksista, raportoi projektin ohjausryhmälle.

## **Projektiryhmä**

Projektiryhmä toteuttaa projektin tehtävät eli käytännön kehitystyön sovittuja menetelmiä ja standardeja noudattaen, raportoi työn edistymisestä ja tuo välittömästi esiin poikkeamat alkuperäisistä suunnitelmista. Projektiryhmä raportoi projektipäällikölle. Projektiryhmän yksi keskeinen tehtäväalue on usein jatkuvuus suunnittelu.

## **Projektin ohjausryhmä**

Projektin ohjausryhmässä ovat edustettuna projektin lopputulosta hyödyntävät intressiryhmät. Ryhmä toimii projektin valvojana, joka hyväksyy projektisuunnitelmat, päättää suunnitelmien muutoksista, ratkaisee mahdolliset ristiriitatilanteet projektipäällikön tekemien selvitysten perusteella sekä vastaa hankkeen resurssien ohjauksesta. Ohjaus-

ryhmän tulee edellyttää tietoturvallisuuden riittävää huomioimista hankkeen eri tehtävissä hankkeen osapuolilta.

### **Auditoija**

Auditoija tarkastaa tietojärjestelmätyön elinkaaren eri vaiheiden lopputulosten hyväksyttävyyden. Auditoija vertaa saavutettuja tuloksia joko asetettuihin tavoitteisiin, laatumäärittäisiin tai esimerkiksi laatusertifikaatissa esitettyihin kriteereihin (auditointi = tarkastus).

Tietoturvallisuuden auditoija arvioi järjestelmän tietoturvaluusominaisuuksia, kontroleja ja kirjausketjuja, neuvoo tietoturvaluusominaisuuksien ja kontrollien suunnittelussa toteuttamisessa sekä tarkastaa, että eri osapuolet ovat täyttäneet roolinsa ja vastuunsa. Tietoturvallisuuden hallintajärjestelmän sertifiointi edellyttää muun muassa sisäistä auditointia.

### **Järjestelmän ylläpitäjä**

Järjestelmän ylläpitäjä vastaa käytön aikaisista muutoksista. Ylläpitäjä voi kuulua esimerkiksi tietotekniikkavastaavan organisaatioon.

### **Sisäinen tarkastus**

Sisäinen tarkastus arvioi toiminnan riskejä sekä järjestelmän kontroleja ja kirjausketjuja, neuvoo kontrollien suunnittelussa ja toteuttamisessa sekä tarkastaa, että eri osapuolet ovat täyttäneet roolinsa ja vastuunsa. Sisäisellä tarkastuksella ei ole toteutusvastuuta kontroleista. Eri vaiheiden lopputulokset hyväksyy linjajohto eikä sisäinen tarkastus.

### **Tietojärjestelmän pääkäyttäjä**

Tietojärjestelmien pääkäyttäjän tietoturvaluustehtäviä ovat huolehtiminen sovelluksen käytettävyydestä ja kehittämisestä, käyttöoikeuksista, järjestelmän tietoturvaluudesta. Pääkäyttäjän vastuulla saattaa olla myös jatkuvuussuunnittelun tehtäviä.

### **Tietojärjestelmän käyttäjä**

Käyttäjien tehtävinä on järjestelmien käyttäminen työtehtävissä ja siihen liittyvien sallassapitovelvollisuuksien ja muiden tietoturvaluusvelvoitteiden noudattaminen. Käyttöoikeuksien luovuttaminen eteenpäin on kielletty. Organisaatiossa on huolehdittava siitä, että käyttäjät ovat saaneet työyhteisön ja tietojärjestelmän käytön edellyttämän tietoturvaluusosaamisen koulutautumis- ja kehittämistarpeiden perusteella. Järjestelmän käyttäjä arvioi järjestelmän käytettävyyttä ja raportoi ongelmista.

## 5.2 Projektityön tietoturvallisuus

Projektityön tietoturvallisuutta voidaan arvioida tai ottaa siihen kantaa esimerkiksi seuraavien tarkistuslistamallien avulla:

Onko monitoimittajaympäristöissä päävastuullinen toimittaja nimetty riittävän selkeästi ja eri toimijoiden vastuut kuvattu?

Onko kehittämiselle asetettu aikatauluvaatimus epärealistinen?

Onko kehittämisessä tarvittavien resurssien saatavuus varmistettu?

Kenelle organisaatiossa voidaan tiedottaa projektista (tiedotussuunnitelma)?

- Mikäli tiedon saantia ei ole välttämätöntä rajoittaa, on tiedottamisessa käytettävissä organisaation normaalimenettelyt.
- Mikäli tiedon saantia on rajoitettava vain niihin henkilöihin, jotka tarvitsevat sitä tehtävässään, on projektia koskevan tiedon jakamista valvottava.

Miten ulkopuolisille voidaan tiedottaa projektista?

- Tietoa annetaan niille ulkoisille tahoille, joille se on tarpeen antaa yhteistyösuhteiden perusteella.
- Vain välttämätön tieto annetaan. Tehdään salassapito/ tietoturvaluussopimus.

Mitä ovat ehdot / vaatimukset organisaation oman henkilöstön osallistumiselle projektiin?

- Organisaation oman henkilöstön osallistumiselle projektiin ei ole tarpeen asettaa rajoituksia tai erityisiä tietoturvaluusvaatimuksia.
- Oman henkilöstön osallistumiselle määritellään osaamiseen tai turvallisuuteen liittyvät erityisvaatimukset.

Millä periaatteilla projektissa voidaan käyttää ulkopuolista henkilöstöä?

- Ulkopuolista henkilöstöä voidaan käyttää tarvittaessa.
- Ulkopuolisen henkilöstön / organisaation kanssa on tehtävä salassapitosopimus.
- Taustat tarkistetaan mahdollisuuksien mukaan.
- Ulkopuolista henkilöstöä käytetään vain, jos se on projektin kannalta ehdottoman tarpeellista.
- Tehtävät rajataan vain välttämättömään osuuteen.
- Salassapitosopimus ja organisaation käytäntöjen mukainen taustojen tarkistus ovat ehto osallistumiselle.
- Ulkopuoliselle henkilöstölle organisaation antama tietoturvaluusperehdyttäminen.

Jos organisaation päälinjana on ulkoistettu ohjelmistokehitys, millä periaatteilla valitaan organisaation projekteihin osallistuva toimittajan henkilöstö ?

- Toimittaja ilmoittaa organisaatiolle, ketkä osallistuvat organisaation projektiin. Organisaatio voi halutessaan varata itselleen oikeuden hyväksyä tai hylätä toimittajan ehdottamat henkilöt. Salassapitosopimus ja tausta-tarkistukset suositeltavia.
- Projektiin osallistuvat henkilöt on etukäteen hyväksyttävä organisaatiolla. Organisaatio soveltaa toimittajan henkilöstöön oman käytäntönsä mukaisia tausta-tarkistuksia. Salassapitosopimus ja organisaation käytäntöjen mukainen taustojen tarkistus ovat ehto osallistumiselle.

Pääsy toimitiloihin, joissa projektiin liittyvä työ tehdään.

- Organisaation perustietoturvaluustason mukaiset käytännöt.
- Normaalityöaikojen ulkopuolista pääsyä tiloihin valvotaan.
- Pääsyä tiloihin rajoitetaan ja valvotaan kaikkina aikoina.

Paperidokumenttien jakelu.

- Jakelussa organisaation perustietoturvaluustason mukaiset käytännöt.
- Jakelu vain niille, joiden työtehtäviin aineisto liittyy.
- Dokumenteista otetaan vain välttämätön määrä kopioita, jakelu erikseen nimeytyille henkilöille. Mahdollisuuksien mukaan kriittisistä dokumenteista tehdään yksilöllisesti tunnistettavat. Dokumentteja ei saa viedä pois suojatuista tiloista. Dokumenttien käsittely- ja säilytyskäytäntöjä valvotaan.

Dokumenttien sähköinen jakelu

- Jos sovellusta tehtäessä tai sen ylläpidossa käytetään tilaajan ja toimittajan välillä yhteisiä sähköisiä työryhmäohjelmistoja, tulee niiden teknisestä rakenteesta, suojauksesta ja ylläpidosta sekä dokumenttikannan taltioversioinnista sopia tarkasti. Erityisesti monitoimittajaympäristössä tulee dokumenttien tarpeelliseen suojaukseen jo liikesalaisuussyistä kiinnittää huomiota.
- Kun kehitettävä järjestelmä on turvaluustasoltaan vaativa, sen kehittämisen välineistön ja hankkeen viestintämenetelmien on oltava vastaavalla tasolla, tällöin myös toimittajan henkilöstöltä vaaditaan todennettua tietoturvaluuden laatuosaamista.

Projektiin liittyvän työaineiston (paperit, tallenteet ...) säilytys.

- Tietojärjestelmät ja niiden dokumentaatio kuuluvat organisaation arkistoon ja arkistotoimen piiriin kuten muutkin asiakirjat. Ne tulee eritellä arkistolain (831/94) 8 §:n tarkoittamassa viranomaisen arkistonmuodostussuunnitelmassa.
- Organisaation perustietoturvaluustason mukaiset käytännöt.
- Käytävissä oltava erikseen lukittavat säilytystilat, joissa aineisto pidetään työaikojen ulkopuolella. Materiaalin viemistä organisaation tilojen ulkopuolelle ra-

joitetaan. Tärkeimpien aineistojen varmuuskopioille on oltava ulkopuolinen, suojattu ja valvottu säilytyspaikka.

- Säilytetään tiloissa, joihin pääsyä on rajoitettu. Käytettävissä oltava erikseen lukittavat säilytystilat, joissa aineisto pidetään silloin, kun sitä ei käytetä työssä (ns. puhtaan pöydän periaate). Materiaalista viedään suojattujen työskentelytilojen ulkopuolelle vain varmuuskopiot, joiden säilytyspaikan on oltava turvattu.

Järjestelmäkehityksen tietoteknisen ympäristön pääsynvalvontakäytännöt.

- Organisaation perustietoturvaluustason mukaiset käytännöt.
- Pääsynvalvonnalla rajataan projektin aineiston saantioikeudet vain projektista tietoa tarvitseville. Ulkoisia tietoliikenneyhteyksiä kehittämissympäristöön rajoitetaan ja niiden toimintaa valvotaan.
- Kriittisten aineistojen saantikerroista tehdään merkinnät tietoturvaluuslokiin. Ulkoiset tietoliikenneyhteydet (mukaan lukien sähköposti) kehittämissympäristöön estetään mahdollisuuksien mukaan. Samoin rajoitetaan muiden riskialttiiden ohjelmistojen käyttöä. Tarvittaessa harkitaan fax- ja puhelinliikenteen rajoittamista tiloissa, joissa projektin aineistoa käsitellään. Säilytettävän ja siirrettävän tiedon salakirjoitusta käytetään, jos kehittämissympäristöä ei voida riittävän tehokkaasti eristää.

Aineistojen hävittämismenettelyt

- Organisaation perustietoturvaluustason mukaiset käytännöt.
- Tärkeimmät materiaalit hävitetään valvotusti tai käyttäen luotettavaa hävityspalvelua, jonka toiminta aika ajoin tarkastetaan. Magneettisille medioille talletettu aineisto päällekirjoitetaan.
- Materiaali hävitetään valvotusti varmistuen siitä, että hävittämismenettely vastaa aineiston luokitusta (esimerkiksi silppurin riittävän pieni silppukoko). Magneettisille medioille talletettu aineisto hävitetään päällekirjoittamalla riittävän monta kertaa, media demagnetoidaan tai tuhotaan fyysisesti lukukelvottomaksi.

### 5.3 Järjestelmäkehityksen laadun varmistaminen tietoturvaluusnäkökulmasta

Järjestelmäkehitystä ohjeistava laatujärjestelmä/laatuohjeisto menetelmäkuvauksineen, standardeineen yms. työhjeineen on usein oma kokonaisuutensa ja tietoturvaluusohjeisto omansa. Tätä perustellaan esimerkiksi tietoturvaluusasiakirjojen luottamuksellisuudella.

Laadunvarmistus sisältää tietoturvaluusnäkökohtia: ohjelmiston ja kehittämissankkeen laatua arvioidaan toiminnallisuuden, luotettavuuden, käytettävyyden, tehokkuuden, ylläpidettävyyden ja siirrettävyyden näkökulmista.

Järjestelmäkehityksessä tietojärjestelmän kriittisyys arvioidaan ja analysoidaan heti kehitystyön alussa ja kriittisyysluokituksen pohjalta asetetaan laatu- ja tietoturvaluusvaatimukset jotka kirjataan laatu- ja tietoturvaluusuunnitelmaan.

Kehitystyön eri vaiheissa laatu varmistetaan katselmuksilla suunnitelmien mukaisesti. Mikäli tietoturvaluusvaatimukset ovat suuret, on kehitysprojektissa mukana tietoturvaluusasiantuntija. Näin on myös katselmuksissa.

Vähemmän kriittisissä projekteissa on käytäntönä, että tietoturvaluusarkkitehtuuri ja tietoturvaluusohjeisto huomioidaan kehitystyössä. Vastuu tästä on projektilla ja oletetaan että projektin jäsenillä on riittävä tietoturvaluusosaaminen. Laadunvarmistus tehdään ja tietoturvaluus tarkistetaan katselmuksissa.

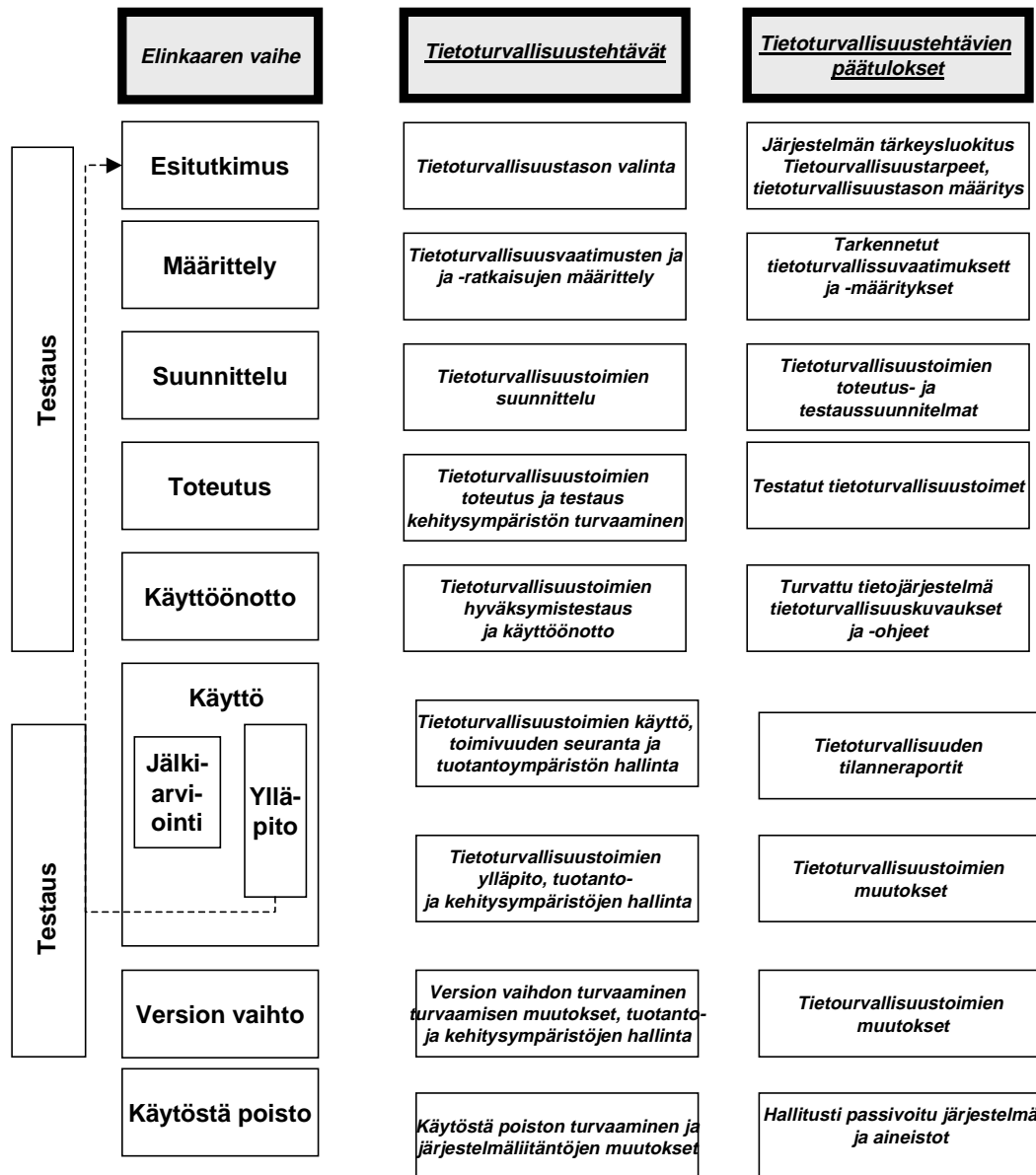
Katselmuksot pohjautuvat suunnitelmiin ja niiden toteutumiseen sekä olemassaolevaan ohjeistukseen, joten tässäkin on erittäin tärkeää, että jo mahdollisimman aikaisessa vaiheessa on kuvattu tietojärjestelmän turvaamiseen liittyvät vaatimukset ja niiden toteuttamistavat.

#### **Standardeista:**

- Järjestelmäkehitykseen muokatut standardit ovat erillisiä (ISO 9000-3 ja BS 7799-1) – laatu ja turvallisuus.
- Uudistuva ISO 9004 - standardi yhdistää organisaation laatujärjestelmään ympäristö- ja tietoturvaluusjärjestelmissä kuvatun “suunnittele ennakolta - toteuta-arvioi- muuta, korjaa, paranna” -ajattelun ja rakenteen. Eri järjestelmistä yhdistyy organisaation toimintajärjestelmä ja siten tietoturvaluudesta tulee osa toimintaprosesseja.

## 6 Tietoturvaluusvaatimukset järjestelmän elinkaaren eri vaiheissa

Seuraavassa mallissa kuvataan järjestelmäkehityksen vaiheet, niihin liittyvät keskeiset tietoturvaluusvaatimukset sekä tehtävien päätulokset.



Mallia voidaan soveltaa eri vaihejakoihin sekä nopeaan järjestelmäkehitysmalliin, tietoturvaluustehtävät suoritetaan tässä mallissa kuvatulla tavalla ryhmiteltiin ne millä tahansa vaihejakomallilla. Mallissa on mahdollista palata tarpeen vaatiessa taaksepäin edelliseen vaiheeseen. Lisäksi ylläpito- ja version vaihto –vaiheet poikkeavat muista vaiheista siltä osin, että ne pitävät sisällään toimintoja muista vaiheista. Esimerkiksi ylläpito (pienimuotoiset järjestelmän muutokset) kattaa toimintoja määrittelystä järjestelmän toimitukseen. Version vaihto (laajat järjestelmämuutokset) kattaa toimintoja esitutkimuksesta järjestelmän toimitukseen sekä väistyvän järjestelmän osalta käytöstä poiston.

Testaus kuuluu olennaisena osana kuhunkin vaiheeseen, korostetusti se on esitetty toteutus- ja käyttöönotto vaiheissa. On myös huomattava, että vaiheiden välillä suoritetaan myös laadunvarmistustehtäviä.

Tietojärjestelmän elinkaaren eri vaiheissa on tehtävä / tarkennettava riskianalyysi tietoturvaluusuhkista ja suunniteltava niiden hallinta.

Jäljempänä esitettävistä yleisistä tarkastuslistoista on muokattava ja sovellettava tapauskohtaiset organisaation tilanteeseen sopivat luettelot esimerkiksi tarjouspyyntöjen liitteiksi. Esitysteknisesti niin tarkistuslistat kuin muukin teksti on kuvattu vaiheittain, todennäköisimmän tulevan käyttötarkoituksen perusteella.

Myös valmisohjelmistojen hankinnassa ja valmisohjelmistojen pohjalta tehtävässä tietojärjestelmäräätälöinnissä tulee soveltaa seuraavassa esitettyjä tietoturvatehtäviä. Erityisesti tulee varmistua esitutkimus- ja määrittelyvaiheiden tietoturvatehtävien hoitamisesta myös valmisohjelmistohankinnoissa.

## **6.1 Järjestelmän esitutkimus**

### **Esitutkimusvaiheen tietoturvaluustehtävät**

Esitutkimusvaiheen tärkein tietoturvaluustehtävä on kartoittaa tietoturvaluuden peittämisestä toiminnalle aiheutuvat menetykset. Esitutkimuksessa kartoitetaan kohteena olevan kehityshankkeen, siihen liittyvien tietoaineistojen ja työtehtävien tärkeys toiminnalle ja sen jatkuvuudelle. Muun muassa näiden perusteella määritellään kehitettävän järjestelmän tärkeysluokitus. Valmiustoiminnan vaatimukset otetaan huomioon tietojärjestelmäkehityksessä tärkeiksi luokiteltujen järjestelmien osalta.

Järjestelmän esitutkimusvaiheen tietoturvaluuskartoitus ja -tason valinta on hyvin tärkeä tehtävä, koska siinä luodaan perusta järjestelmän koko elinkaaren tietoturvaluuden varmistamiselle. Koska tietoturvaluuden tason parantaminen tai riittävän tason luominen edellyttävät voimavaroja, tulee esitutkimusvaiheen tietoturvatehtäviin panostaa riittävästi, jotta hankkeen resurssitarvearvio on tietoturvaluuden varmistamisen osaltakin realistinen.

Tärkeys määrittelee valvonnalle (toiminnan ja tapahtumien seurannalle ja toimenpiteisiin ryhtymiselle) asetettavat vaatimukset. Turvaluokitus koskee asiakirjoja tai tietoja ja tärkeysluokitus järjestelmiä. Tässä yhteydessä on myös päätettävä järjestelmän kehittämisprojektin tietoturvallisuusmenettelyistä.

Tietojärjestelmien tärkeysluokittelu:

Luokka 1: Tietojärjestelmä pyritään pitämään toimintakunnossa kaikissa olosuhteissa siten, että

- tietojärjestelmällä tulee olla atk-varajärjestelmä, korvaava manuaalinen järjestelmä tai suunnitelmat toimenpiteistä vakavia häiriö- ja poikkeustilanteita varten.

Luokka 2: Tietojärjestelmän tukemaa toimintaa ja tietotekniikan käyttöä voidaan supistaa.

Luokka 3: Tietojärjestelmä voidaan korvata tai lopettaa poikkeusoloissa.

Valmiusvaiheen poikkeusolojen alasajo ja palautusvaatimukset auttavat priorisoimaan järjestelmien tärkeimmän ytimen määrittelyssä. Suppean minimijärjestelmän, jonka on toimittava poikkeusoloissakin, hahmottaminen auttaa kokonaisuuden yksinkertaiseen ja edulliseen ratkaisemiseen.

Riskianalyysin ja alustavien tietoturvallisuusvaatimusten avulla arvioidaan vaadittavien tietoturvallisuuteen liittyvien toimintojen kustannus-, hyöty- sekä kuormitusvaikutukset, joiden pohjalta määritetään tärkeimmät tietoturvallisuusvaatimukset.

### **Esitutkimusvaiheen tietoturvallisuustehtävien lopputulokset**

Vaiheen tuloksena syntyy kehitettävän järjestelmän sekä sen kehittämissympäristön tärkeysluokitus, mikä jatkossa ohjaa turvallisuuden kehittämistehtäviä. Nämä tehtävät sisällytetään tietoturvallisuussuunnitelmaan (joka voi olla esimerkiksi esitutkimusraportin osa tai liite) ja niille varataan riittävät resurssit.

- Tietoturvallisuusvaatimukset tietoturvallisuussuunnitelmaan
- Lainsäädännön ja valtion tietoturvaohjeiden tietoturva vaatimusten sekä organisaation tietoturvaperustan (muun muassa valtioneuvoston 11.11.1999 tietoturvallisuuspäätöksen ja VAHTIn ohjeiden mukaisten tietoturvallisuuden 8-osa-alueen toimenpiteiden toteutuksen tarjoamat mahdollisuudet) yleistason läpikäynnin tulokset
- Riskianalyysin tulokset
- Tärkeysluokitus
- Valmiussuunnitteluvaihtoehdot, mahdollinen varautuminen poikkeusoloihin
- Tietoturvallisuuden kustannus-, hyöty- sekä kuormitusvaikutukset.

## **Esitutkimusvaiheen tietoturvallisuusvastuut**

- Järjestelmän omistaja/ohjausryhmä hyväksyy selvitykset
- Tietoturvallisuusvastaava tarkastaa arviot ja varmistaa, että ne ovat organisaation tietoturvallisuuspolitiikan mukaiset
- Kriittisten järjestelmien osalta hankitaan ylimmän johdon hyväksyntä
- Esitutkimuksen perusteella johto määrittelee järjestelmän tärkeysluokituksen ja päättää tietoturvallisuuteen liittyvistä jatkotoimista kun on kyse toiminnalle erityin kriittisestä hankkeesta.

## **6.2 Järjestelmän määrittely**

### **Määrittelyvaiheen tietoturvaluustehtävät**

Valmiusvaiheen poikkeusolojen alasajo ja palautusvaatimukset auttavat priorisoimaan järjestelmien tärkeimmän ytimen määrittelyssä. Suppean minimijärjestelmän, jonka on toimittava poikkeusoloissakin, hahmottaminen auttaa kokonaisuuden yksinkertaiseen ja edulliseen ratkaisemiseen.

Määrittelyvaiheessa tarkennetaan riskianalysia. Järjestelmän toimintojen määrittelyn perusteella tarkennetaan turvallisuudelle asetettavat vaatimukset. Jatkuvuussuunnitelman linjaukset määritellään tässä vaiheessa. Tietoturvallisuusvaatimukset näkyvät turvallisuuden kehittämistehtävinä myöhemmissä vaiheissa.

Määritellään tietojärjestelmän tulevien käyttäjien roolit: miten käyttöoikeudet rajataan työtehtävien mukaisesti, miten hoidetaan valtuuttaminen, miten vältetään vaarallisia työyhdistelmiä, miten hoidetaan syötteiden, muutosten ja tulosteiden valtuutukset.

Määritellään audit trail (eli kirjausketju), joka tarkoittaa muutoshistorian tarkastettavuutta. Mitä tietoja tulee säilyttää virheselvittelyn ja väärinkäytösten tutkimisen mahdollistamiseksi. Myös tietojen kysely on tallennettava mahdollisen salassapitorikkomuksen selvittämiseksi. Taloushallinnon järjestelmissä määritellään, mitä tarvitaan talousarvioasetuksen vaatimusten täyttämiseksi. Asetus edellyttää muun muassa jälkeenpäin todettavissa olevaa tapahtuman hyväksyjän "leimaa", henkilötietoja käsittelevissä järjestelmissä vastaavasti Henkilötietolain vaatimukset täyttävän käsittelyn.

Tietoaineistojen luokittelun periaatteet luodaan kokonaisuudessaan: käytettävyys-, luotamuksellisuus- ja eheysäännöt. Määritellään tietojen eheyden kontrollit tietojen siirrossa paikasta toiseen tai eri järjestelmien välillä. Näitä voidaan hoitaa erilaisilla täsmäytyksillä ja elektronisilla sineteillä. Määritellään tarvittavat tallennuksen eheyskontrollit. Määritellään, miten salassa pidettävien asiakirjojen käsittely ja merkinnät hoidetaan (kts. valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje, VAHTI 2/2000).

Tarkistetaan vastaako nykyinen infrastruktuuri tietoturvuvaatimuksia: salasanojen laatu, murtoyritysten seuranta, järjestelmän ylläpitäjien ja tietokannahoitajien vahvat oikeudet käyttöjärjestelmätasolle ja suoraan tietokantaan, suoja ulkoisia riskejä kohtaan (vi-

rustarkistus, järjestelmään pääsy), fyysiset turvamenettelyt (kulunvalvonta, paloturva yms.)

Määritellään järjestelmän kehityksessä syntyvien dokumenttien tietoturvan taso. Vaaditaan tarvittaessa työhön osallistuvilta konsulteilta salassapitosopimukset.

Tietoliikennettä käytettäessä määritellään, tarvitaanko salausta ja sähköistä tunnistusta. Mikäli tarvitaan, määritellään avainten jakelun ja varmentamisten turvallisuustaso.

Jos päädytään suunnittelu- ja toteutustyön teettämiseen ulkopuolisella taholla, myös turvallisuuteen liittyvät asiat on sisällytettävä tietotekniikkapalvelutoimittajan kanssa tehtävään sopimukseen. Myös määrittely voidaan teettää ulkopuolisten voimin. Näissä tapauksissa on otettava huomioon myös mahdollisen kilpailuttamisen asettamat tietoturvaluusuusvaatimukset. Määrittelyvaiheen yhteistoiminta realististen turvavaatimusten muodostamiseksi on järjestettävä.

Tarkennetaan tietoturvaluusuusvaatimukset:

- riskianalyysi toistetaan tarkemmalla tasolla
- järjestelmään sijoitetut tietoturvaluusuusvaatimukset
- pääsynvalvonta, luottamuksellisuus, eheys, käytettävyyden
- tietoturvaluusuusvaatimusten vaikutus tekniseen arkkitehtuuriin.

Tehdään tai tarkennetaan jatkuvuussuunnitelma toiminnan jatkamiseksi erilaisten häiriöiden aikana ja niiden jälkeen. Määritellään mahdollinen erillinen valmiussuunnitelma ja mahdollinen vaihtoehtoinen toimintatapa kriisitilanteessa.

Toipumissuunnittelussa määritellään:

- Tietojärjestelmälle varajärjestelmävaatimukset, vastuut ja toimet valmiuden luomiseksi sekä annetaan ohjeet toimimisesta poikkeustilanteissa
- Käyttäjätöimintojen suunnitelma
- Manuaalitoiminnot
- Varajärjestelmät.

Jatkuvuussuunnitelma / katastrofeista toipumissuunnitelma tehdään yleensä sellaisiin riskeihin varautumiseksi, jotka uhkaavat organisaation tietojenkäsittelyä infrastruktuuri-tasolla eli tuotantotilojen katastrofitilanteisiin varautumiseksi.

Tärkeyslokiteltujen tietojärjestelmien osalta on lisäksi arvioitava järjestelmän merkitystä toiminnan jatkuvuuden kannalta. Mitä vaikutuksia järjestelmän käytettävyyden vaarantuminen aiheuttaa eri pituisten katkosten seurauksena esimerkiksi taloudellisista näkökulmista, vaikutuksina sidosryhmille tai imago-vaikutuksina. Näin saadaan perusteet varajärjestelmien rakentamiselle, toimintaohjeiden laatimiselle, vaatimukset tietojen, ohjelmistojen ja kuvausten varmistuksille ja säilytykselle.

Määritellään alustava tietoturvaluusuustoimintojen testaussuunnitelma resurssitarpeineen sekä arviointikriteereineen. Tarkennetaan tietoturvaluusuuden testaussuunnitelma (testausympäristö, testauspahtumat, häiriö- ja normaalitilanteet). Varataan alustavasti re-

surssit turvatoimien testaukseen. Tämä tulisi sisältyä testaussuunnitelmakokonaisuuteen. Kehitysympäristön turvaamisen menettelyt määritellään.

Sisällytetään tietoturvaluusuvaatimukset tarjouspyyntöön ja sopimuksiin.

Suunnitellaan alustavasti tietoturvaluusustehtävät:

- tietosisällön suunnittelu
- tiedon eheystarkistukset
- tietokannan eheyden tarkistus
- turvaluokitellun tiedon turvaaminen
- käyttäjätoimintojen määrittely
- käyttäjien käyttövaltuudet (yksilöidyt oikeudet nimettyjen osajärjestelmien tai tietojen saantiin, esimerkiksi luku-, kirjoitus, poistovaltuus)
- käyttäjien tehtäviin liittyvät valvonnat
- virhetilanteiden hallinnan suunnittelu
- muutostilanteiden hallinnan suunnittelu.

### **Määrittelyvaiheen tietoturvaluusustehtävien lopputulokset**

Tietoturvaluusuvaatimukset on kuvattu täsmällisesti ja vaatimukset toteuttavat ratkaisut on määritelty. Jatkuvuussuunnitelman alustava versio on laadittu. Järjestelmän toimintaan liittyvät riskit on tunnistettu ja ne on otettu huomioon turvaamisen määrittelyssä. Turvaamisen testaussuunnitelman alustava versio on laadittu ja testausresurssit varattu. Tietoturvaluusuvaatimukset on sisällytetty ohjelmiston toimitussopimukseen, jos ohjelmistokehitys on päätetty teettää muilla kuin organisaation omilla resursseilla. Kehitysympäristön turvaamisen menettelyt on määritelty ja niitä sovelletaan määrittelyvaiheen työn tulosten turvaamiseen.

- Tietoturvan erityisvaatimusten kirjaaminen esimerkiksi tietoturvaluisuuden 8-osa-alueen vaatimusten pohjalta uhkien hallitsemiseksi esimerkiksi tarvittavat käyttäjäryhmittelyt/roolit, tunnistaminen, tarkkuustaso ja rajaukset, tarkennetut tietoturvavaatimukset
  - Vaikutukset arkkitehtuuriin
  - Riskianalyysi
  - Toimintokohtaiset vaatimukset
- Tietoaineistojen luokittelun vaatimukset
- Lainsäädännön ja valtion tietoturvaohjeiden tietoturvavaatimusten sekä organisaation tietoturvaperustan (muun muassa valtioneuvoston 11.11.1999 tietoturvaluusupäätöksen ja VAHTIn ohjeiden mukaisten tietoturvaluisuuden 8-osa-alueen toimenpiteiden toteutuksen tarjoamat mahdollisuudet) tarkempi läpikäynti, jotta saadaan määriteltyä mitkä tietoturvaluusuvaatimukset järjestelmän on toteutettava (ja mitkä piirteet saadaan infrastruktuurista)
- Tietoturvaluusuvaatimusten ja järjestelmän toimintaa koskevien riskien kuvaus
  - Koko järjestelmästä ja sen ulkoisista liittymistä
  - Järjestelmän päätoiminnoista
  - Tietoturvaluuskriittisistä yksittäisistä kohteista
  - Käyttäjistä ja käyttöympäristöstä aiheutuvat riskit?

- Peruskontrollien ja sovittujen pelisääntöjen soveltaminen järjestelmään
- Toteutettavat lisäkontrollit ja turvaaminen
- Järjestelmäliittymien turvaaminen
- Kustannusarvio perusteluineen
- Jäännösriskin kuvaus yleisesti, arvio tietoturvallisuuskriittisten kohteiden jäännösriskeistä
- Turvaamisen alustava testaussuunnitelma resurssivarauksineen.
- Projektin tietoturvallisuusmenettelyjä koskevat poikkeamaraportit
- Jatkuvuussuunnitelman alustava versio
  1. Toipumissuunnitelma
  2. Varajärjestelmä
- Tietoturvallisuustehtävien suunnitelmat
  1. järjestelmät ja liittymät
  2. ohjelmat, tietokannat
- Alustava testaussuunnitelma, päivitetty tietoturvaamisen testaussuunnitelma normaalitoiminnassa ja häiriötilanteissa.

### **Määrittelyvaiheen tietoturvavastuut**

- Järjestelmän omistaja hyväksyy määritykset
- Tietoturvallisuusvastaava tarkastaa arviot ja varmistaa, että ne ovat organisaation tietoturvallisuuspolitiikan mukaiset
- Kriittisten järjestelmien osalta organisaation ylimmän johdon hyväksyntä.

### **6.3 Järjestelmän suunnittelu**

#### **Suunnitteluvaiheen tietoturvallisuustehtävät**

Suunnitteluvaiheen tietoturvallisuustehtäviin vaikuttaa olennaisesti se, onko aiemmassa vaiheessa esiin tulleille tietoturvallisuusvaatimuksille olemassa valmiita teknisiä ratkaisuja. Jos näitä ei löydy, on turvaamisen tekniset ratkaisutavat suunniteltava. Myös kehitettävän järjestelmän käyttövaltuudet eri käyttäjäryhmille on suunniteltava.

Tärkeä tietoturvallisuustehtävä on myös testaussuunnitelman tarkentaminen. Testaussuunnitelmassa kuvataan testattavat kohteet, testausympäristö ja testitapahtumat sekä varataan testauksessa tarvittavat resurssit. Testaussuunnitelmaan tulee sisällyttää sekä normaalien tilanteiden että poikkeuksellisten tapahtumien käsittelyt. Kehitysympäristön turvaamisen menettelyt täsmennetään. Kehitys- ja testiympäristöt eriytetään (pitäisi koko ajan olla eri ympäristöt).

Suunnitellaan, miten toteutetaan tulevien käyttäjien käyttöoikeudet määrittelyssä asetettujen vaatimusten mukaisesti. Selvitetään palveleeko jo olemassa oleva infrastruktuuri ratkaisuja vai tarvitaanko järjestelmäkohtaisia toimenpiteitä.

Suunnitellaan, miten kirjausketju (audit trail) toteutetaan (mm. hoidetaanko tietojen historiointi sovelluksessa vai infrastruktuurin yleisillä, esimerkiksi tietokannan toimesta? Osa kirjausketjuista hälytyksenä reaaliaikaisesti). Suunnitellaan eheyskontrollien toteutus, miten ja kuka seuraa virheilmoituksia ja mahdollisia huomautuslokeja. Suunnitellaan järjestelmän käyttäjäorganisaatioiden (jolloin johtokin on mukana, jos näin on tarpeen) ja järjestelmän käytön valvojen koulutus myös tietoturvallisuuden osalta.

Tarkistetaan, vastaako yleinen varmuuskopiointi ja niiden säilytys järjestelmälle asetettua tietoturvaluustasoa kaikilta osin sekä määrittelyvaiheessa asetettuja palautumistavoitteita. Jos ei, niin suunnitellaan lisävarmistukset ja palauttamismenettelyt. Palauttamismenettelyt tulee suunnitella sekä tietokannalle, tietojärjestelmälle että liittymille/tiedonsiirroille/ajojonoille (uudelleenaloitukset jne).

Lisävarmistuksia voidaan tarvita myös ennen suuria massatallennuksia, konversioiden yhteydessä tai kauden vaihtuessa.

Tarvittaessa suunnitellaan salausmenettelyt, avainten jakelu ja kirjanpito sekä varmentamismenettelyt.

Suunnitellaan testiaineistot niin, että tietojen luottamuksellisuus ei vaarannu.

Tietojärjestelmän suunnittelun lähtökohtana ovat modulaarinen rakenne ja selvät osien väliset työnjaot. Tämä helpottaa virheiden paikallistamista ja niiden vaikutusten rajaamista.

Suunnitellaan myös manuaalimateriaalin säilytys ja arkistointi turvallisella tavalla. Ne tulee eritellä arkistolain (831/94) 8 §:n tarkoittamassa viranomaisen arkistonmuodostussuunnitelmassa.

### **Suunnitteluvaiheen tietoturvaluustehtävien lopputulokset**

Järjestelmään sisällytettävät uudet tietoturvaluusratkaisut tai jo käytössä olevien tietoturvaluusratkaisujen soveltaminen kehitettävään järjestelmään on suunniteltu.

Käyttäjäroolit ja niiden valtuudet, vältettävät vaaralliset työyhdistelmät, tapahtumien hyväksymisvaltuudet sekä kirjausketjun toteutus on suunniteltu. Turvaamisen testaussuunnitelma on tarkennettu ja se kattaa sekä normaalitoiminnan että poikkeustilanteet.

Kehitysympäristön tietoturvaluussuunnitelma on tarkennettu. Suunniteltua turvaamista sovelletaan suunnitteluvaiheen työn tulosten turvaamiseen.

- Tietoturvaluusratkaisujen suunnittelu määriteltyjen vaatimusten pohjalta luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseksi
- Järjestelmän skaalautumisen varmistaminen käyttäjä- ja tapahtumamäärien kasvun varalle

- Alustava näkemys asioiden toteuttamisesta järjestelmässä ottaen huomioon infrastruktuurin tarjoamat tietoturvaluusuosminaisuudet
- Kuvaus peruskontrollien soveltamisesta järjestelmässä ja sen liittymissä
- Kuvaus keskeisten osien lisäkontrolleista
- Kuvaus yksittäisten tietoturvaluuskriittisten kohteiden lisäkontrolleista
- Suunniteltujen kontrollien vertailu tietoturvaluusvaatimuksiin
- Kontrollien testaussuunnitelma tietoturvaluusustason vaatimalla tarkkuudella
- Kuvaus käyttäjäryhmistä ja käyttövaltuuksista
- Projektin tietoturvaluusumenettelyjä koskevat poikkeamaraportit.

#### **Suunnitteluvaiheen tietoturvaluustuut**

- Järjestelmän omistaja hyväksyy suunnitelmat
- Tietoturvaluusuvastaava tarkastaa kontrollien toteutussuunnitelmat
- Testaussuunnitelmalle erillinen järjestelmän omistajan ja tietoturvaluusuvastaavan hyväksyntä.

#### **6.4 Järjestelmän toteutus**

##### **Toteutusvaiheen tietoturvaluusustehtävät**

Suunnitellut turvaamiset toteutetaan järjestelmään osana muuta järjestelmäkehitystä. Ohjelmiin sisältyvät turvaamiset ja käyttöympäristön hallintamenettelyt testataan testaussuunnitelman mukaisesti, ja testauksista tehdään testauspöytäkirjat. Testaukseen tulee sisällyttää sekä normaalitoimintojen että poikkeustilanteiden käsittelyt. Turvaaminen dokumentoidaan tietoturvaluuskuvauksiin. Käyttäjille näkyvä turvaaminen sisällytetään järjestelmän käyttöohjeisiin.

Kehittäisympäristön turvaamisesta huolehditaan kehitysympäristön ja kehitettävän järjestelmän turvaluokituksen edellyttämällä tavalla. Samoin toteutetaan ja testataan käytön aikaisen kehitysympäristön turvaaminen.

Muita toteutusvaiheen tietoturvaluustehtäviä ovat

- Riskianalyysi toteutuksen näkökulmasta
- Tietoturvaluusustoimintojen toteutus sisältyy muun muassa ohjelmiin, käyttöohjeisiin, käytön ohjeisiin, järjestelmän käyttövaltuuksien ja käyttäjäryhmien ja -roolien määrittelyyn.
- Tietoturvaluusustoimintojen testaus
- Tietojärjestelmän kuvausten tarkentaminen myös tietoturvaluisuuden osalta
- Tietojärjestelmän tietojen luokittelun viimeistely
- Tietojärjestelmän tietojen säilyttäminen ja säilytysaikojen päivittäminen - arkistonmuodostussuunnitelmiin.

## **Toteutusvaiheen tietoturvaluustehtävien lopputulokset**

Järjestelmään sisällytetyt tietoturvaluusominaisuudet on testattu ja ne ovat sovittujen vaatimusten mukaiset. Turvaamisen testauspöytäkirjoista ja syntyneistä testausympäristön lokeista voidaan todentaa testauksen riittävyys ja tulosten oikeellisuus. Turvaaminen on dokumentoitu ja käyttäjille näkyvät osuudet turvaamisesta sisällytetty käyttöohjeisiin.

- Suunnitellut tietoturvaluusvaatimukset toteutettu
- Vaatimusten mukaiset kontrollit toteutettu
- Testaustulokset ja testausraportit
- Vaiheen tuotosten perusteella tarkennettu tietoturvaluuskuvaus.
- Kuvaus käytön aikaisen kehitys- ja testausympäristön turvaamisesta (sisältyy turvakuvaukseen)
- Riippumattoman tarkastajan lausunto toteutuksesta
- Projektin tietoturvaluusmenettelyjä koskevat poikkeamaraportit
- Käyttäjille näkyvä turvaaminen sisällytetty käyttöohjeisiin ja koulutussuunnitelmaan.

## **Toteutusvaiheen tietoturvaluusvastuut**

- Järjestelmän omistajan hyväksyntä testausaineistoille.
- Tietoturvaluusvastaavan hyväksyntä testausaineistoille ja testausmenettelyille.
- Projektipäällikkö ja projektin ohjausryhmä hyväksyvät toteutuksen.
- Tietoturvaluusvastaava hyväksyy kontrollien toteutuksen.
- Toteutuksen hyväksymisessä kannattaa etenkin merkittävässä hankkeissa käyttää riippumatonta tarkastajaa
- Projektipäällikkö hyväksyy käyttäjien toimintoihin liittyvien kontrollien toteutuksen ja koulutussuunnitelmat.
- Projektin valvontaryhmä hyväksyy käyttäjien toimintoihin liittyvien kontrollien toteutuksen ja koulutussuunnitelmat
- Järjestelmän omistaja hyväksyy käyttäjien toimintoihin liittyvien kontrollien toteutuksen ja koulutussuunnitelmat.
- Tietoturvaluusvastaava hyväksyy käyttäjien toimintoihin liittyvien kontrollien toteutuksen ja koulutussuunnitelmat.

## **6.5 Järjestelmän käyttöönotto**

### **Käyttöönottovaiheen tietoturvaluustehtävät**

Turvaamisen hyväksymistestaus ja tuotantoon siirto valmistellaan nimeämällä niille vastuuhenkilöt, joille annetaan testaustehtävän kannalta riittävät käyttövaltuudet. Käyttäjille ja tukiorganisaatiolle annetaan turvaamista koskeva koulutus.

Turvaaminen testataan sekä teknisen toteutuksen että hallinnollisten menettelyjen osalta. Hyväksymistestauksen yhteydessä viimeistellään järjestelmän turvakuvaukset ja turvaamisen käyttöohjeet.

Mahdollisuuksien mukaan ohjelmakoodi tarkistetaan siten, ettei sinne ole tehty / jäänyt ns. takaportteja, joiden kautta suunnittelijat pääsisivät käyttämään järjestelmää tai se muutoin toimisi määrittelyjen vastaisesti.

Vastuuhenkilö hyväksyy valmiin ohjelmiston. Lähdekoodi tallennetaan turvalliseen paikkaan. Vastuuhenkilö siirtää käännetyn ohjelman tuotantoon. Ohjelman ja sen versioiden tuotantoonsiirrossa on automaattinen kirjanpito. Tuotantoympäristö tietokantoi-  
neen luodaan ja todetaan toimivaksi.

Käyttöönottovaiheen tehtäviä tehdään rinnan kehitysprojektin kanssa erillisessä käyttöönottoprojektissa.

Testauksen aikaiset käyttövaltuudet poistetaan. Testauksen aikainen tietokanta tyhjenetään.

Projektin aineiston säilyttämisestä huolehditaan. Järjestelmän käyttövaltuudet annetaan työtehtävien ja vastuun edellyttämässä laajuudessa.

Järjestelmän hallinta ja valvonta siirretään käyttöpalvelutoimittajan vastuulle käytössä olevan auditointimenettelyn mukaisesti varmistaen ohjeiston mukainen toiminta.

### **Käyttöönottovaiheen päätulos**

Käyttöönottovaiheen päätuloksena on hyväksytty, tuotantokäyttöön siirretty toimiva tietojärjestelmä, jonka tietoturvallisuus täyttää asetetut vaatimukset.

- Tuotantoympäristön käyttövaltuudet asetettava sovittujen määritysten mukaisesti.
- Järjestelmän kehittäjille ei saa ”periytyä” tuotantoympäristöön käyttövaltuuksia kehittämisympäristöstä.
- Kontrollien ohittamisen tai muuttamisen mahdollistavia kehittämis- ja testaustyökaluja ei saa siirtää tuotantoympäristöön.
- Tuotantoympäristön on oltava kehittämis- ja testausympäristöstä erillinen välittömästi järjestelmän käyttöönoton jälkeen – kontrollien ohittamisen tai muuttamisen mahdollistava ”siirtymäaika” ei ole hyväksyttävä toimintakäytäntö.
- Vaikka järjestelmässä havaittaisiinkin tuotantokäytön alkuvaiheessa tavallista enemmän ylläpitoa vaativia toiminnallisia puutteita ja virheitä, ylläpidossa on syytä noudattaa sovittuja tuotantoonsiirtomenettelytapoja. Mikäli alkuvaiheen ylläpito vaatii järjestelmän kehittäjien osallistumista virheiden selvittelyyn tuotantoympäristössä, järjestelmän käytöstä vastaavan organisaation tulee huolehtia kehittäjien suorittamien selvittelyjen valvonnasta ja kirjaamisesta. Järjestelmän omistajan hyväksyntä vaaditaan poikkeuksellisille toimintamenettelyille.

Tietojen siirto vanhasta järjestelmästä uuteen

- Tarkistetaan tietojen eheys siirron jälkeen: tietokantarivien lukumäärät ovat samat, summat, tiedon arvoalueen rajat, valitut tietokannan rivit yms. vastaavat toisiaan
- Huolehditaan tietojen luottamuksellisuudesta: siirtomenettelyt tietoturvaluusvaatimusten mukaisiksi.

### **Käyttöönottovaiheen tietoturvaluustehtävien lopputulokset**

Kehitetty tietojärjestelmä on hyväksytty ja otettu tuotantokäyttöön. Järjestelmään toteutetut turvaamiset ovat sovitun tietoturvaluustason vaatimusten mukaiset. Turvaaminen on dokumentoitu ja sitä koskevat käyttöohjeet on jaettu käyttäjille. Käyttäjät ovat saaneet turvaamisen käytössä tarvittavan koulutuksen ja toimintaohjeet erilaisten poikkeustilanteiden varalle. Tuotannon aikaisten järjestelmämuutosten kehittämis- ja testausympäristö turvaamisineen on ylläpidosta vastaavan henkilöstön käytettävissä. Tuotantoonsiirtomenettely on tarkastettu ja dokumentoitu. Käytön ja ylläpidon tietoturvaluusjärjestelyistä on selkeät vastuut, toimintatavat ja ohjeet.

- Testitulokset, jotka osoittavat vaatimusten mukaisen tietoturvaluustason toteutumisen järjestelmässä
- Toteutus- ja testaussuunnitelma hyväksymistestissä löydetyille puutteille ja virheille, jotka on korjattava ennen tuotantoon siirtoa
- Ylläpitosuunnitelma, joka sisältää hyväksymistestissä löydettyjen puutteiden ja virheiden korjaukset
- Vaatimusten mukainen tietoturvaluustaso tuotantoympäristössä
- Vaatimusten mukaiset, dokumentoidut ylläpito- ja tuotantoonsiirtokäytännöt
- Kontrollien käyttöön koulutetut käyttäjät sekä käyttö- ja ylläpitohenkilöstö
- Projektin tietoturvaluusmenettelyjä koskevat poikkeamaraportit ja niiden jakeilu
- Toimiva, testattu järjestelmä, joka toimii myös tietoturvaluusvaatimusten mukaisesti
- Tietoturvaamisen dokumentaatio
- Tietojärjestelmäseloste
- Testauspöytäkirjat
- Tietoturvaluuteen liittyvä koulutus
- Tietoturvaluusohjeisto.

### **Käyttöönottovaiheen tietoturvaluusvastuut**

- Järjestelmän omistaja hyväksyy testitulokset ja antaa luvan järjestelmän tuotantoon siirrolle
- Järjestelmän omistajan hyväksyntään sisällytetään lausuma vaatimusten mukaisen tietoturvaluustason toteutumisesta
- Järjestelmän omistaja hyväksyy puutteiden / virheiden korjaus- ja/tai ylläpitosuunnitelman
- Tietoturvaluusvastaava hyväksyy testitulokset ja tuotantoonsiirtosuunnitelman
- Käyttäjä raportoi tietoturvaongelmista jotka liittyvät eheyteen, käytettävyyteen ja luottamuksellisuuteen.

- Organisaation johto antaa luvan kriittisen järjestelmän tuotantoon siirrolle
- Omistaja ja käyttöorganisaatio hyväksyvät järjestelmän tuotantokäyttöön
- Ylläpitovastaava ottaa vastaan kontrollien ylläpitovastuun
- Tietoturvaluusvastaava hyväksyy tuotantoympäristön kontrollien toteutuksen ja ylläpitomenetelmät.

## 6.6 Järjestelmän ylläpito

### Ylläpitovaiheen tietoturvaluustehtävät

Hallittu muutosprosessi, johon kuuluu erillisten tuotanto- ja kehitysympäristöjen hallinta, on tärkeä tietoturvaluustoiminto. Ylläpidossa on myös pidettävä huolta siitä, että muutoksia tehtäessä otetaan huomioon järjestelmän kehittämisen perustana olevat kriteerit sekä toiminnallisuuden että turvallisuuden suhteen. Ylläpito versioidaan, versiohallinta toimii ja on dokumentoitu.

Järjestelmän toiminnallisten muutosten vaikutukset turvaamiseen analysoidaan, ja niitä vastaavat turvaamisen muutokset suunnitellaan ja toteutetaan. Muutosprosessi voi käynnistyä myös tarpeesta tehdä muutos turvaamiseen, ja tällä muutoksella voi olla vaikutusta järjestelmän yleisiin ratkaisuihin.

Jos turvaamisen muutos näkyy järjestelmän käyttäjille, on käyttöohjeisiin tehtävä tarvittavat muutokset ja käyttäjille järjestettävä muutoksia koskeva koulutus. Jatkuvuussuunnitelmien muutostarve on tarkistettava ja suunnitelmiin tehtävä tarvittavat muutokset.

### Ylläpitovaiheen tietoturvaluustehtävien lopputulokset

Järjestelmän turvaamiseen tarvittavat muutokset on tehty, testattu ja otettu käyttöön tuotantoympäristössä. Jatkuvuussuunnitelma on päivitetty muuttuneen tilanteen tasalle ja keskeiset muutokset on testattu. Käyttäjille näkyvistä turvaamisen muutoksista on tehty ohjeet ja käyttäjille on annettu muutosta koskeva koulutus.

- Tietoturvaluusvelvoitteet esimerkiksi julkisuuslaki koskee myös vanhoja järjestelmiä
- Lakimuutosten edellyttämä ylläpito
- Yleiskuvaus muutoksen vaikutuksesta turvaamiseen.
- Kuvaus muutoksen vaikutuksesta järjestelmän keskeisten osien turvaamiseen.
- Kuvaus muutoksen vaikutuksesta yksittäisten kriittisten osien turvaamiseen
- Turvaamisen toteutus- ja testaussuunnitelma
- Turvaamisen muutosten testauspöytäkirjat ja testiaineistot
- Jatkuvuussuunnitelman dokumentoidut muutokset.
- Jatkuvuussuunnitelman testauspöytäkirjat.
- Ylläpidon tietoturvaluusmenettelyjä koskevat poikkeamaraportit

## **Ylläpitovaiheen tietoturvallisuusvastuut**

- Päätös kriittisen järjestelmän ylläpitotoimesta: järjestelmän omistaja
- Päätös ylläpitotoimesta: järjestelmän omistaja
- Päätös ylläpitotoimesta: myös tietoturvallisuusvastaava
- Muutoksen käyttöönotto: omistaja / pääkäyttäjä
- Muutoksen käyttöönotto: myös tietoturvallisuusvastaava

## **6.7 Järjestelmän tuotantoaikainen käyttö**

### **Käytön aikaiset tietoturvaluustehtävät**

Turvaamista käytetään osana toimivaa järjestelmää. Järjestelmän ja sen turvaamisen käyttöä seurataan asetettujen vaatimusten mukaisesti ja mahdollisista poikkeamista raportoidaan sovitulla tavalla säännöllisesti. Järjestelmän käyttövaltuuksien hallinnassa noudatetaan sovittuja menettelytapoja. Käyttöympäristön muutokset sekä laitteiden vaihdot ja käyttöönotot tehdään toiminnan tietoturvaluusvaatimukset huomioon ottaen.

Tietoaineistojen varmistuksista huolehditaan tietoaineistojen tietoturvaluusluokitusten edellyttämällä tavalla. Järjestelmille tehdään sovituin välien tietoturvaluusstarkastus.

Tuotantokäytössä olevaan järjestelmään tehdyt muutokset ja versiopäivitykset tehdään huomioiden tietoturvaluus.

Noudatetaan sovittuja varmistus- ja arkistointimenettelyitä. Varmuuskopioinneista ja niiden käytöstä sekä säilytyksestä pidetään kirjaa. Varmistusten luettavuutta ja palauttamista testataan säännöllisesti, varmistusten toimivuus on säännöllisesti testattava palautustoimenpitein.

Pidetään erillään järjestelmän hyväksikäyttö, tuotantotehtävät, sovellussuunnittelu ja tiedon hoito.

Valvotaan käyttöoikeuksien myöntämistä. Seurataan, etteivät oikeudet kasaannu, ei muodostu vaarallisia työyhdistelmiä ja oikeuksia muutetaan tarvittaessa henkilön tehtävien muuttuessa. Poislähteneen työntekijän oikeudet poistetaan.

Käyttöönotosta 6-12 kuukauden kuluttua on hyödyllistä tehdä jälkiarviointi, jonka tyyppisiä tietoturvaluustehtäviä ovat muun muassa varmistuminen pääsykontrollien riittävydestä, tietojärjestelmien kontrollien toimivuudesta ja operoinnin tapahtumien tarkastaminen turvalokeista.

### **Käytön aikaisten tietoturvaluustehtävien lopputulokset**

Käytössä noudatetaan sovittuja toimintakäytäntöjä, joista näyttönä syntyvät vaatimusten mukaiset lokitiedostot ja raportit. Turvallisuuden valvonnan avulla käytön aikaisiin poikkeamiin reagoidaan siten, että vahingon vaikutukset ja mahdollinen epäkäytettä-

vyys saadaan rajatuksi mahdollisimman tehokkaasti. Ongelmaraportit johtavat tarvittaessa turvaamisen muutosprosessin käynnistymiseen.

- Raportoinnissa teknisten mittarien lisäksi myös käyttäjien kokema mittaristo
- Palvelevuus ja havainnot tietoturvallisuuskista yms.
- Lyhyt lausunto valvonnassa / tarkastuksessa tehdyistä löydöksistä ja mahdollinen suositus tietoturvallisuusluokan muutoksesta
- Yhteenvetona arvio kontrollien toimivuudesta ja suositus kontrollien muutoksiksi.
- Tietoturvallisuuspoikkeamien analyysi, selvitys poikkeamien syistä ja ehdotus kontrollien muutoksiksi.
- Toipumissuunnitelman testaustulokset ja testiin perustuen suositukset toipumisjärjestelyjen muutoksiksi.

### **Käyttövaiheen tietoturvallisuusvastuut**

- Järjestelmän omistaja hyväksyy johtopäätökset ja toimenpide-suositukset.
- Tietoturvallisuusvastaava hyväksyy kontrollien muutosehdotukset
- Johto valvoo tietoturvakokonaisuutta apunaan tietoturvallisuusvastaava sekä edellyttää raportointia tietoturvaongelmista

## **6.8 Järjestelmän version vaihto**

### **Version vaihdon tietoturvaluustehtävät**

Keskeinen tietoturvaluustehtävä on varmistaa, että kaikki vanhasta järjestelmästä uuteen ympäristöön siirrettävät tiedot säilyvät merkitykseltään muuttumattomana. Siirron aikainen luottamuksellisuus on myös varmistettava. Erityishuomiota vaativat tietojen siirrossa mahdollisesti käytettävät väliaikaiset tietorakenteet, joiden suojaustaso ei oletusarvoisesti vastaa normaalitilanteen suojauksia.

Toinen tärkeä tehtävä on jatkuvuussuunnitelmien muutostarpeen kartoitus ja tämän perusteella tehtävät jatkuvuussuunnitelmien ja tietoturvaluusvaatimusten muutokset.

### **Version vaihdon tietoturvaluustehtävien lopputulokset**

Järjestelmän turvaamiseen on tehty tarvittavat muutokset ja tietojen siirrossa uuteen ympäristöön on varmistettu tietojen eheys ja luottamuksellisuus. Uutta järjestelmäversiota kehitettäessä on huolehdittu turvaamisen kehittämisestä aiemmin kuvatun mukaisesti. Vanhan version poiston turvaaminen on hoidettu myöhemmin kuvatulla tavalla. Jatkuvuussuunnitelma on päivitetty muuttuneen tilanteen tasalle ja keskeiset muutokset on testattu.

- Siirtosuunnitelman turvaamisen kuvaus
- Tiedonsiirron testipöytäkirjat
- Tietojen siirron pöytäkirja ja lokit
- Jatkuvuussuunnitelman testatut muutokset
- Projektin tietoturvaluusmenettelyjä koskevat poikkeamaraportit

## **Versionvaihtovaiheen tietoturvaluusuvastuut**

- Siirtosuunnitelma: järjestelmän omistaja
- Siirtosuunnitelma: tietoturvaluusuvastaava
- Jatkuvuussuunnitelma: järjestelmän omistaja
- Jatkuvuussuunnitelma: tietoturvaluusuvastaava

## **6.9 Järjestelmän poisto käytöstä (alasajo)**

### **Käytöstä poiston tietoturvaluustehtävät**

On tärkeää varmistaa, ettei järjestelmän passivointi häiritse jäljelle jääviä toimintoja. Aktiivikäytöstä poistettavien aineistojen (sekä ohjelmat että tiedot) mahdollinen arkistointi hoidetaan tietoturvaluusuluokitus ja arkistonmuodostussuunnitelma huomioon ottaen. Poiston yhteydessä hävitettävät tietoaineistot käsitellään nekin tietoturvaluusuluokan ja arkistonmuodostussuunnitelman vaatimusten mukaisesti.

Käytöstä poistettavien laitteistojen kiintolevyt ovat osa poistettavaa aineistoa. Jos levyt sisältävät salassa pidettävää tietoaineistoa, tietojen poistaminen levyiltä on tehtävä tietoturvaluusuluokituksen ja säädösten edellyttämällä tavalla.

Jatkuvuussuunnitelmien muutostarve on tarkistettava ja suunnitelmiin tehtävä tarvittavat muutokset.

Huolehditaan poistettavan järjestelmän dokumentaation ja muiden ohjeiden säilyttämisestä/hävittämisestä määritellyn säilytysarvon mukaisesti noudattaen tietojen hävittämisestä annettuja ohjeita. Ohjeistetaan käyttäjillä olevan ohjeistuksen poistaminen. Huolehditaan käyttöoikeuksien poistamisesta sekä järjestelmän vaatimien tietoliikenneyhteyksien sulkemisesta.

### **Käytöstä poiston tietoturvaluustehtävien lopputulokset**

Vaiheen tuloksena käytöstä poistettava järjestelmä on passivoitu hallitusti. Tarvittavat ohjelmistot ja tietoaineistot on arkistoitu turvaluokituksen ja arkistonmuodostussuunnitelman vaatimusten mukaisesti, ja aineistojen käytössä tarvittavien laitteistojen saatuus on varmistettu. Poistotoimet on dokumentoitu jäljitettävyyden mahdollistavalla tavalla. Jäljelle jäävien järjestelmien toiminnot on sopeutettu uuteen tilanteeseen ja jatkuvuussuunnitelmaan on tehty vaadittavat muutokset.

- Turvaamisen ylläpitosuunnitelma jäljelle jääville järjestelmille, joihin poistolla on vaikutusta
- Vaadittavat aineistot arkistoitu ja niiden käytettävyyden (myös tarvittavien laitteistojen osalta) varmistettu
- Aineistot on hävitetty tietoturvaluusuluokituksen ja sen edellyttämien tietoturvaluusuvaatimusten (VAHTI 2/2000) sekä arkistonmuodostussuunnitelman vaatimusten mukaisesti

- Laitteistojen uudelleen sijoituksessa on varmistettu, ettei salassa pidettäviä tietoja ole siirtynyt valtuuttamattomien tahojen käyttöön.
- Pöytäkirja poisto- ja arkistointitoimenpiteistä.
- Poistamistoimenpiteiden tietoturvaluusmenettelyjä koskevat poikkeamaraportit.

### **Käytöstä poistovaiheen tietoturvaluusvastaat**

- Jäljelle jäävien järjestelmien ylläpitosuunnitelma hyväksytään ko. järjestelmälle sovittujen ylläpitokäytäntöjen mukaisesti.
- Poistosuunnitelma sisältäen arkistoinnin ja laitteistojen uudelleen sijoituksen: järjestelmän omistaja
- Poistosuunnitelma: tietoturvaluusvastaava

### **6.10 Testaus ja laadunvarmistus**

Testaus ja laadunvarmistus ovat osa tietojärjestelmän kehityksen kaikkia vaiheita. Kaikissa vaiheissa tulee testauksella todeta, että vaiheen tehtävät on tehty ja tehdyt ratkaisut toimivat ja ovat hyväksyttäviä. Laadunvarmistuksella seurataan kaikissa vaiheissa, että lopputulokset ovat laadukkaita sekä sisäisesti että ulkoisesti:

- Sisäinen laatu: kehitysvaiheen lopputulokset on tehty sovittujen pelisääntöjen mukaisesti, ne on testattu, dokumentoitu, ohjelmat ovat modulaarisia ja kommentoituja
- Ulkoinen laatu: kehitysvaiheen lopputulokset palvelevat tarkoitustaan, vastaavat edellisessä vaiheessa asetettuja tavoitteita ja ovat käyttäjiä palvelevia.

Tietoturvaluuden osalta testauksella ja laadunvarmistuksella varmistetaan, että eri vaiheissa tarkoituksenmukaiset tietoturvatehtävät on tehty ja ne toimivat tarkoituksenmukaisesti. Esimerkiksi testataan, että esitutkimusvaiheessa on tehty järjestelmän riskikartoitus ja asetettu tietoturvavaatimukset, määrittelyvaiheessa on määritelty, mitä tarvitaan tietoturvavaatimusten täyttämiseksi, suunnitteluvaiheessa on suunniteltu turvatehtävien toteutus, toteutusvaiheessa on toteutettu kaikki suunnitellut turvatehtävät, käyttöönottovaiheessa kaikki järjestelmän osat toimivat yhdessä turvavaatimukset täyttävällä tavalla. Mikäli testaukset osoittavat puutteita turvatehtävien toiminnassa, palataan takaisin joko kyseiseen vaiheeseen tai tarvittaessa edellisiin vaiheisiin.

Testauksessa on huolehdittava myös testauksen tietoturvaluudesta. Testaus on suoritettava erillään tuotantoympäristöstä. On pidettävä huoli, että testaus ei vahingossakaan muuta tuotannossa olevia tietoja. Testiaineiston osalta on huolehdittava salassapidosta, testiaineistoa koskevat samat vaatimukset kuin tuotantotietoja. Mikäli testaukseen osallistuu organisaation ulkopuolisia kehittäjiä on heiltä vaadittava salassapitositoumukset ja/tai testiaineisto laadittava niin, että salassapidettävät tiedot eivät paljastu.

Laatuohjeistossa tulisi olla linkit niihin turvallisuusohjeistoihin, joita kulloinkin tulisi käyttää.

## **7 Järjestelmäkehityksen tietoturvallisuuden erityiskysymyksiä**

### **7.1 Valmiusvaiheen poikkeusolojen alasajo ja palautus**

Yhteiskunnan kannalta ja viranomaisen kannalta tärkeillä järjestelmillä on omat menettelynsä, jotka on jo luotu normaalioloissa.

Valmiusvaiheen poikkeusolojen alasajo ja palautus tehdään esimerkiksi siten että eri minimijärjestelmä otetaan käyttöön. Se voi käytännössä olla jopa eri järjestelmä jopa eri organisaation tekemänäkin.

Tietoturvallisuudesta huolehditaan soveltaen edellä kuvattuja vastaavien vaiheiden tietoturvaluustehtäviä, -tarkastuslistoja, lopputuloskuvauksia sekä vastuita.

### **7.2 Tietoturvaluus valmisohjelmistojen hankinnoissa**

Valmisohjelmistoja hankittaessa (valmiina pakettina tai räätälöitävänä työnä) tulee tietoturvaluuden varmistamisen tukena käyttää kohdassa 6 esitettyjä toimenpiteitä: ohjelmistohankintaa edeltää kappaleessa kuusi kuvatut esitutkimus ja määrittelyvaiheet. Näissä vaiheissa tulee määrittellä hankittavalta järjestelmältä vaadittavat tietoturvaominaisuudet. Järjestelmän käyttöönotossa tulee varmistua, että turvaominaisuudet on myös toteutettu määritellyllä tavalla ja ne toimivat asianmukaisesti.

Seuraavaa valmisohjelmistojen hankinnan erityiskysymyksiä käsittelevää tarkistuslistaa voidaan käyttää em. tarkistuslistoja täydentävänä:

- 1) Mikä on toimittajan henkilöstömäärä?
- 2) Onko toimittajan taloudellinen tilanne hyvä?
- 3) Onko toimittajan avainhenkilöiden taustat tarkistettu?
- 4) Onko toimittajalla aiempia referenssejä vastaavan kaltaisista hankkeista?
- 5) Onko organisaatiolla tai sen henkilöstöllä entuudestaan kokemuksia yhteistyöstä toimittajan kanssa?
- 6) Onko toimittajan henkilöstöllä hankkeessa tarvittavaa ammatillista osaamista?
- 7) Onko toimittajalla organisaation sidosryhmien kanssa yhteistyötä, joka voisi olla organisaatiolle tietoturvariski?
- 8) Onko toimittajalla sertifioitu laatu-järjestelmä tai muuta riippumatonta näyttöä toiminnan laadukkuudesta?
- 9) Miten toimittajan organisaatituruvaluus ja tietoturvaluus on organisoitu?
- 10) Onko toimittajan tietoturvaluuden hallintajärjestelmä sertifioitu?
- 11) Onko toimittajalla ajan tasalla olevat tärkeimmät osa-alueet kattavat tietoturvaluusohjeet ja onko ohjeet koulutettu henkilöstölle?
- 12) Onko toimittajan toimitilojen tietoturvaluustaso hyvä?
- 13) Onko toimittajan järjestelmäkehitysmalli organisaation käytäntöjen kanssa yhteensopiva?

- 14) Onko toimittajan järjestelmäkehitysmallissa otettu huomioon tietoturvallisuusnäkökohdat?
- 15) Käyttääkö toimittaja ohjelmistokehityksessä välineitä, jotka ovat yhteensopivia organisaation käyttämien kehitystyökalujen kanssa?
- 16) Estääkö toimittajan kehittämissympäristön pääsynvalvonta asiaankuulumattomien pääsyn projektin aineistoon?
- 17) Onko toimittajan kehittämissympäristöstä tietoturvariskin sisältäviä ulkoisia tietoliikenneyhteyksiä?
- 18) Onko toimittajalla ajan tasalla oleva, testattu jatkuvuussuunnitelma?
- 19) Onko tarpeen ja mahdollista tehdä escrow-sopimus hankittavasta ohjelmistosta?
- 20) Onko toimittajan kehittämissympäristön tietoturvaluusjärjestelyt mahdollista tarkastaa?
- 21) Onko hankittavan ohjelmistopakettien kehittämisen tietoturvaluusmenettelyistä saatavissa tietoa ja ovatko nämä menettelyt riittävät?
- 22) Onko hankittavasta ohjelmistosta saatavissa turvakuvaus?
- 23) Onko hankittavan ohjelmiston tietoturvaluusaste riittävä?
- 24) Valmisohjelmistoaluekohtaiset erityisvaatimukset.
- 25) Onko hankittavaan ohjelmistoon julkistettu säännöllisesti korjaus-/ylläpitopaketteja?

### 7.3 Sopimukset

Organisaation tekemillä sopimuksilla on monia liittymäkohtia tietoturvaluuteen. Näin on myös tietojärjestelmien kehittämiseen / ostamiseen liittyvien sopimusten osalta. Sopimusten laatimisessa on pitkälti kysymys hankintaan liittyvien riskien hallinnasta sopimusjuridiikan avulla.

Suurin osa sopimusehdoista koskettaa yleensä tavalla tai toisella osapuolten velvollisuuksia ja vastuita (esimerkiksi takuu-, force majeure-, sopimussakko-, purku-, määritysten tarkentaminen-, sopimuksen muutokset- ja laatulausekkeet).

Tietotekniikan asiantuntijoilla ei yleensä ole riittäviä taustatietoja sopimustekniikkaan (ml. sopimustekstin ulkopuolelle jäävät asiat ja erilaisten sanktioehtojen etusijajärjestys) liittyvistä menettelytavoista. Tästä syystä etenkin isojen hankintojen yhteydessä ns. sopimusjuridiset asiat on käsiteltävä omana kokonaisuutenaan tämän osa-alueen asiantuntijoiden toimesta.

Valtionhallinnon tietotekniikkahankinnoissa käytetään sopimisen perustana valtion yleisiä tietotekniikkahankintojen sopimusehtoja. Valtionhallinnon käyttöön tarkoitetut tietotekniikkahankintojen sopimusehdot koostuvat yleisistä sopimusehdoista (VYSE) sekä niitä täydentävistä hankintakohteen mukaisista erityisehdoista. Ne on esitetty osoitteessa: <http://www.vn.fi/vm/kehittaminen/tietohallinto/vati/paasivu.htm>

Yksittäiset teknistä/ tietojärjestelmien kehittämisen työnjakoa ja siihen liittyviä tietoturvaluusvastuita koskevat asiat liitetään sopimukseen liite- / projektisuunnitelmatasolla. Tässä suosituksessa esitetyillä tarkistuslistoilla ja vaiheiden tuloksilla on organisointita-

pa huomioiden merkitystä myös silloin kun tietojärjestelmän kehittäminen ostetaan ulkopuolelta.

Toimittajien yleiset sopimusehdot ovat yleensä palveluntarjoajan edun mukaisia, yksityiskohtien tarkennettuun ja (valtio)asiakkaan edun huomioon ottavaan sopimiseen kannattaa kiinnittää huomiota sopimusjuristin avustuksella tapauskohtaisesti esimerkiksi seuraavan kaltaisissa kohdissa:

#### Välttämättömät periaatteet

- Toimittaja ei vastaa ajon keskeytyksen tai tietokoneen toiminnan aiheuttamasta vahingosta.
- Laitteistohäiriöistä tai toimittajan henkilökunnan virheellisestä käyttötoiminnasta toimittaja vastaa vain tilaajan hukkaan menneen työajan verran.
- Ohjelmistovirheiden tai muiden virheiden seurauksena syntyneiden vahinkojen osalta toimittaja vain korjaa virheet. Toimituksen myöhästymisen tai viivästyksen osalta on sovittava menettelytavat.
- Tiedon katoamisen tai saamatta jääneen voiton osalta ei mitään korvausta tai vastuuta.
- Jos taas asiakkaan rike johtaa sopimuksen purkuun, toimittajalle tulee täysi korvaus palveluista sekä vahingonkorvaus.
- Pääsynvalvonta, hallinta ja sopimukset olisi saatava asianmukaisesti hallintaan.
- Hankkeesta päätettäessä olisi oheisasiakirjoissa oltava riittävät selvitykset ulkoistamisen vaikutuksista ennen kuin ulkoistamiseen mennään.
- Sopimuksessa olisi sovittava toimittajan avainhenkilöiden vaihtuvuudesta/pysyvyydestä, varahenkilöjärjestelyistä, taustojen tarkistuksesta, koulutuksesta ja osaamisen ylläpidosta, salassapitosopimuksista, käyttöoikeuksista ja niiden valvonnasta, henkilöstön lukumäärästä.
- Käyttäjän vahva tunnistaminen
- Varmistuskopiointimenettelyt
- Tietoturvaluusnäkökohdat on otettava riittävästi huomioon.
- Vaatimusten on oltava niin yksikäsitteisiä, että niillä on käytännön vaikutusta.
- Toimittajan velvollisuus ilmoittaa huomatuista tietoturvahingoista: millaisista, millä aikataululla, kenelle.
- Asiakkaan oikeus lähdekoodiin, omistusoikeus, VYSE:ssä huolehditaan asiakkaan oikeudesta sekä lähdekoodiin että kuvauksiin.
- Toimittajan laatujärjestelmän tai tietoturvallisuuden hallintajärjestelmän sertifikaatti, sopimusten katselmointi, valvonta, asiakkaan auditointioikeus, raportointi.
- Toimittajan atk -tilojen fyysinen turvallisuus: kulunvalvonta, paloturvallisuus, vesivahinkovaara, ilmastointi.
- Sopimuskumppanin on noudatettava asiakkaan tai organisaation tietoturvaluusohjeita ja –käytäntöjä esimerkiksi tietoturvaluuspolitiikkaa järjestelmien suunnittelussa käytettäviä ohjeita, projektiohjeita, hallinnon hyvän tiedonhallintatavan, vaitiolositoumusten ja sopimusten noudattamisen jne.
- Asiakkaalla oikeus tarkastaa toimittajan tietoturvamenettelyt.

Perusperiaatteiden lisäksi huomioitavia

- Noudatetaanko toimittajan vai asiakkaan turvaperiaatteita?
- Hankkijan ja alihankkijan turvamenettelyjen, teknisten turvamekanismien ja väärinkäytöksiä ehkäisevien valvontamekanismien määrittelyt
- Kenen vastuulla on ulkoistettu verkko?
- Mitkä osat on ulkoistettu?
- Millaiset sopimukset on tehty?
- Mikä on ulkoistetun osuuden turvataso?
- Ulkoistettujen tietokantojen turvallisuuteen on kiinnitettävä huomiota

Toimittajat eivät yleensä ota sellaista vahingonkorvausvastuuta, mikä voisi vaarantaa yrityksen toiminnan tai aiheuttaa suuria taloudellisia ongelmia. Tästä syystä kaikki viivästys ja virhesanktiot mitoitetaan sellaiselle tasolle mikä riittää pelotteeksi ehkäisemään suurimmat huolimattomuusvirheet mutta ei pelasta tilaajaa, jos se ei huolehdi siitä että a) määritykset tehdään huolella b) toimituksen valvonnasta huolehditaan (hyväksymistarkastus, työn edistymisen ja laadun seuranta yms.). Tämän vuoksi sopimuksen aikainen yhteistyö on hoidettava huolella.

Tilaaja ei yleensä määrittele toimittajan sisäisiä menettelytapoja pitkäaikaisia ulkoistamissopimuksia lukuun ottamatta. Tilaajan on tutkittava toimittajan taloudelliset, tekniset ja toiminnalliset edellytykset myös tietoturvaluusnäkökulmasta tarjous- ja sopimusneuvotteluvaiheissa.

Vastuusiin vaikuttaa useimmiten onko kyseessä tuottamuksellinen, törkeällä tuottamuksella tai tahallisesti aiheutettu virhe tai viivästys vai onko kyseessä täydellinen vahinko, tämän sopimusoikeudellisen lähtökohdan kumoavat sopimusehdot saattavat olla kohutuuttomia. Lisäksi sovellettavat säännöt vaihtelevat sen mukaan ostetaanko järjestelmä ns. räätälöintityönä vai valmiina järjestelmänä. Kriittinen piste on järjestelmän vastaanotto tai hyväksymistarkastus.

Ulkoistettujen palveluiden osalta on syytä kehittää sopimuksia ja valvontaa. Tästä on valtiovarainministeriö antanut myös oman suosituksen (VM 30/01/1999, 11.11.1999 Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus <http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/vahti21999.pdf> ).

#### **7.4 Avoimissa tietoverkoissa toteutettavien tietojärjestelmien tietoturvaluuden erityispiirteitä**

Tässä kappaleessa käsitellään sellaisia tietojärjestelmiä, joissa asiakkaat tai muut sidosryhmät asioivat hallintoon avointen tietoverkkojen (lähinnä internet) kautta. Järjestelmä voi olla joko kaikille käyttäjille avoin tai se voi perustua kahdenvälisiin sopimuksiin. Tässä ei tarkoiteta kaikille avointa tietopalvelua vaan nimenomaan tietojen vaihtoa, asiointia asiakkaan ja hallinnon välillä. Avoimissa tietoverkoissa toteutettavilta tietojärjestelmiltä edellytetään kappaleen 6 suositusten noudattamista. Lisäksi tällaisilta järjestelmiltä edellytetään tiettyjä erityispiirteitä.

Valtiovarainministeriö on antanut internetin käyttö- ja turvallisuussuosituksen , VAHTI 1/1998. Siinä on kuvattu internetin käytön turvallisuusedellytyksiä. Rakennettaessa avoimiin verkkoihin perustuvia tietojärjestelmiä tulee ottaa huomioon suosituksen ohjeet verkkojen eristämisestä palomuurilla, yhteyden salaus, vastapuolen tunnistus, viestin todennettavuus ja kiistämättömyys, salausavainten hallinta ja järjestelmän käytettävyys.

Valtiovarainministeriö on marraskuussa 2000 muodostanut VAHTIn ohjaaman valmisteluryhmän laatimaan sähköisen asioinnin edellyttämää tietoturvallisuuden yleisohjeistusta. Työn viiteryhmä on valtiovarainministeriön perustama sähköisen asioinnin yhteistyöfoorumi.

## 8 Keskeiset lähteet

- 8.1. Valtion Internetin käyttö- ja tietoturvaluussuositus (Valtionhallinnon tietoturvallisuuden johtoryhmän julkaisu 1/1998)
- 8.2. Ohje salassa pidettävien tietojen ja asiakirjojen turvaluokitteluista ja merkinnöistä (VM 5/01/2000).
- 8.3. Valtionhallinnon tietoturvallisuuden johtoryhmän alaisuudessa toimiva Tietojen luokittelu- ja käsittelyohjeita määrittelevä työryhmä
- 8.4. Tietoturvasanasto  
<http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/sanasto/sisallys.htm>
- 8.5. Tietojärjestelmäkehityksen tietoturvaluusmalli, Tietoturvallisuuden varmistaminen tietojärjestelmän elinkaaren eri vaiheissa, Helvi Salminen, Tutkielma, Teknillinen korkeakoulu Koulutuskeskus Dipoli, 5. Turvaluusjohdon kurssi, Otaniemi 2000
- 8.6. Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus, VM 30/01/1999, 11.11.1999  
<http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/vahti21999.pdf>
- 8.7. Valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje (VM 23/01/2000, 18.8.2000)  
<http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/vahti2.htm>
- 8.8. Tietoriskien arviointi, Juha E. Miettinen ja Jorma Kajava, Oulun yliopisto 1994
- 8.9. Control Objectives for Information and Related Technology, Information Systems Audit and Control Foundation, 1998
- 8.10. Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja, Tietojärjestelmien tarkastus ja valvonta ry, 1997
- 8.11. [www.qualitas-fennica.fi/artikkelit/iso9004yhdistajana.html](http://www.qualitas-fennica.fi/artikkelit/iso9004yhdistajana.html)

## **9 Liitteet**

Liite 1. Tietoturvaluutta koskevaa lainsäädäntöä ja ohjeistusta

Liite 2. Suosituksessa käytettävä järjestelmäkehitysmalli

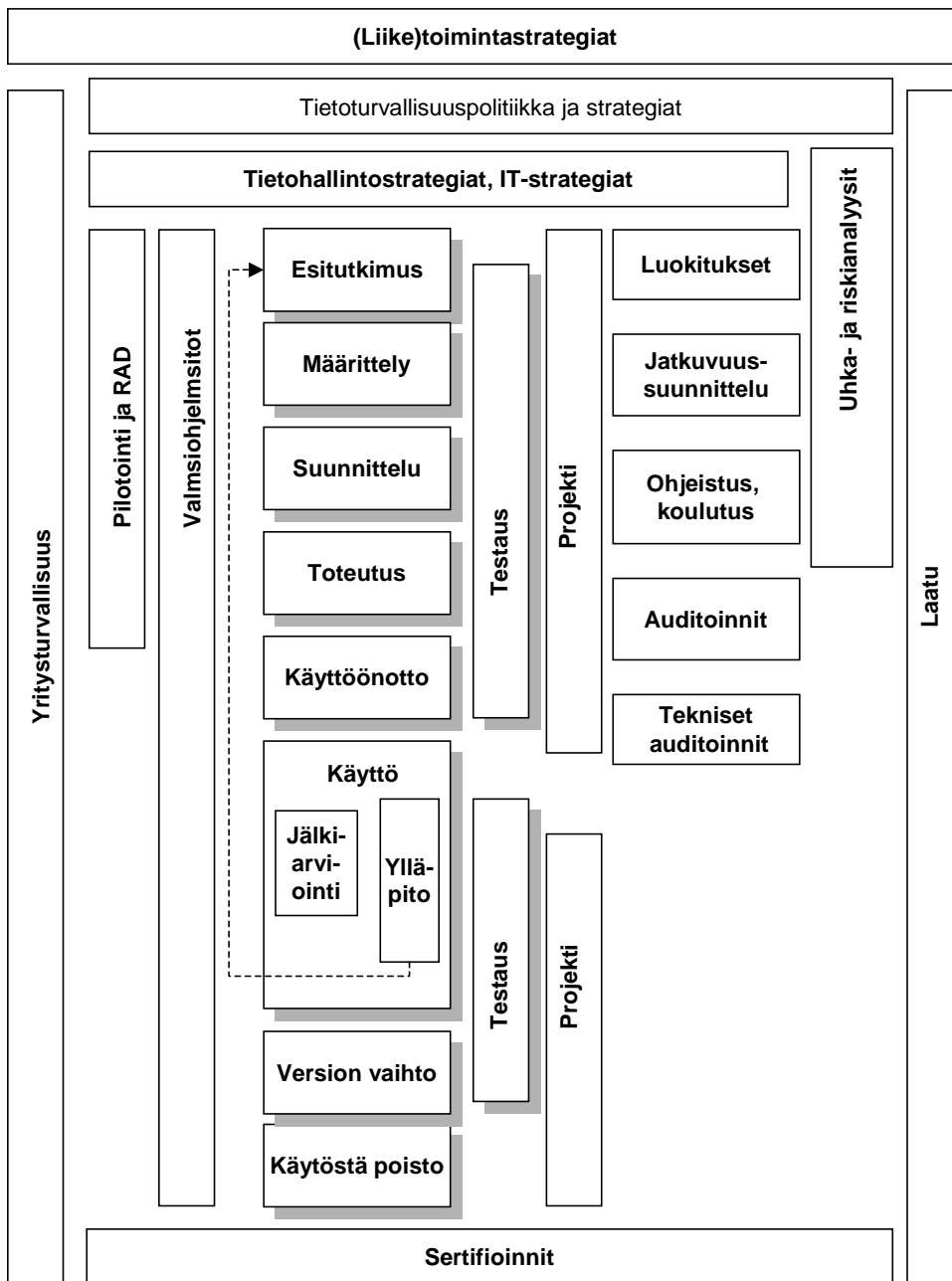
Liite 3. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvaluustarkistuslistat

- Suomen perustuslaki (731/1999) - 10 § ja 12 §
- Laki viranomaisten toiminnan julkisuudesta (621/1999) ja 38 §:n muutos (636/2000)
- Asetus viranomaisten toiminnan julkisuudesta (1030/1999)
- 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) ja muutokset (600/1997 ja 263/2000)
- Henkilötietolaki (523/1999)
- Henkilökorttilaki (829/1999)
- Väestötietolain muutos (527/1999)
- Laki yksityisyyden suojasta televiestinnässä ja teletoinnin tietoturvasta (565/1999) ja asetus (723/1999)
- Telemarkkinalaki (396/1997)
- Laki sähköisestä viestinnästä oikeudenkäyntiasioissa (594/1993)
- Valtion virkamieslaki (750/1994)
- Valmiuslaki (1080/1991)
- Laki ja asetus puolustustaloudellisesta suunnittelukunnasta (238/1960, 239/1960)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta 11.11.1999
- Valtioneuvoston periaatepäätös valtion tietohallinnon kehittämisestä 2.3.2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VM 23/01/2000, 18.8.2000, VAHTI 2/2000)
- Tarpeettomaksi tulleiden tietoaineistojen hävittämisohje VM 21/01/2000, 19.4.2000
- Valtionhallinnon tietoturvallisuuskäsitteistö, 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 tietoturvallisuussuositus, VAHTI 2/1999
- Valtion etätyön tietoturvallisuussuositus, VAHTI 1/1999
- Internetin käyttö - ja tietoturvallisuussuositus, VAHTI 1/1998
- Tietoturvallisuuden tulosohtaus 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
- Erityissäädöksiä kuten Poliisin henkilörekisterilaki, Laki oikeudenkäynnin julkisuudesta ym.

Tässä suosituksessa järjestelmäkehitys ja siihen liittyvä tietoturvallisuuden kehittämismalli kuvataan perinteisen elinkaarimallin käsitteillä. Elinkaarimallin tulkinnessa otetaan myös vaikutteita oliopohjaisen työskentelyn iteratiivisesta lähestymistavasta. Painopiste on elinkaaren alkupäässä. Myöhempiä vaiheita käsitellään karkeammalla tasolla.

Järjestelmäkehityksen elinkaarimalli viitekehyyksineen ja perusinfrastruktuuriiliittymineen on esitetty oheisessa kuvassa

SYSTEEMITYÖ, VAIHEJAKO JA YMPÄRISTÖ



Tarkistuslistojen numerointi (suluissa otsikoiden jälkeen) vastaa luvun 6 numerointia.

### **Esitutkimusvaiheen tietoturvaluustarkistuslista (6.1)**

- Onko toiminta, johon kehitettävä järjestelmä liittyy, todennäköinen ulkopuolisen/asiaankuulumattomien kiinnostuksen kohde? Onko kehitettävä Voidaanko järjestelmää käyttää väärinkäytösten apuvälineenä?
- Miten varsinainen toiminta aiotaan hoitaa erilaisissa yhteiskunnan kriisitilanteissa, esimerkiksi silloin kun valtakunnalliset tietoliikennepalvelut eivät toimi?
- Tunnettaanko järjestelmän kehittämisessä käytettyjen tekniikoiden ja työvälineiden tietoturvaluusominaisuudet?
- Tunnettaanko järjestelmän käyttöympäristön (tietoliikenneverkko, palvelimet,...) tietoturvaluusominaisuudet ja vastaavatko ne vaatimuksia?
- Onko järjestelmällä liittymiä matalamman tietoturvaluustason järjestelmiin?
- Onko järjestelmällä liittymiä esimerkiksi sidosryhmien järjestelmiin, joiden tietoturvaluustasosta ei ole tarkkaa tietoa tai tietoturvaluustaso ei ole järjestelmän vaatimusten mukainen?
- Rakennetaanko järjestelmää valmiista komponenteista, joiden tietoturvaluusominaisuuksia ei tunneta?
- Onko organisaatiolla käytössään tietoturvaluustekniikoita, jotka soveltuvat käytettäväksi kehitettävässä järjestelmässä?
- Onko järjestelmän vaatimuksia vastaavan tietoturvaluustekniikan käytölle lainsäädäntöön tms. syyhyn perustuvia rajoituksia?
- Onko organisaatiolla johdon vahvistamat tietoturvaluusperiaatteet ja täyttääkö suunniteltu järjestelmä sen vaatimukset?
- Onko selvitetty kaikki järjestelmään liittyvä tietoturvalainsäädäntö?

### **Määrittelyvaiheen tietoturvaluustarkistuslista (6.2)**

- Esitutkimusvaiheessa tehdyn tietoturvaluusluokituksen toteaminen kehittämisen perustaksi
- Järjestelmän ulkoisia liittymiä koskeva riskianalyysi
- Järjestelmän päätoimintojen riskianalyysi
- Yksittäisten tietoturvaluuskriittisten kohteiden tarkempi riskianalyysi
- Ulkoisten liittymien tietoturvaluusvaatimusten määrittely
- Järjestelmän päätoimintojen tietoturvaluusvaatimusten määrittely
- Yksittäisten tietoturvaluuskriittisten kohteiden tietoturvaluusvaatimusten määrittely
- Tietoturvaluusvaatimusten kartoitus järjestelmän käyttäjien näkökulmasta
- Jatkuvuussuunnitelmalle asetettavat vaatimukset tarkennetaan
- Turvaamisen testaukselle asetettavat vaatimukset määritellään
- Tietoturvaluusosaamisen varaaminen projektin käyttöön
- Selvitetään turvaratkaisun valintaa rajoittavat tekijät
- Arvioidaan organisaatiossa sovellettavien peruskontrollien soveltuvuus ja riittävyys
- Määritellään lisäkontrollien tarve
- Kartoitetaan mahdolliset tietoturvaluusratkaisut
- Arvioidaan, miten vaihtoehtoiset ratkaisut täyttävät asetut vaatimukset

- Arvioidaan lisäturvaamisen kustannukset ja vertaillaan niitä riskien taloudellisiin vaikutuksiin yleisesti
- Turvaamisen kustannusvaikutusten tarkempi arviointi
- Arvioidaan jäännösriski yleisesti
- Arvioidaan tietoturvaluokituksen kohtien jäännösriski
- Varmistetaan sovittujen tietoturvaluokitusmenettelyjen noudattaminen projektityössä
- Laaditaan turvaamisen alustava testaussuunnitelma
- Laaditaan jatkuvuussuunnitelman alustava versio
- Arvioidaan käytettäviin ohjelmistokehitysvälineisiin liittyvät riippuvuusriskit
- Arvioidaan ohjelmistokehitysvälineiden tietoturvaluokitusominaisuudet, määrittely pitäisi tehdä yleensä välineistä vielä välittämättä. Tietoturvaluokitusvaatimusten pohjalta voi kuitenkin tulla vaatimuksia organisaation käytössä oleviin välineisiin
- Käyttäjäroolien ja niiden rajausten määrittely huomioiden vaaralliset työyhdistelmät
- Kirjausketju -tarpeiden määrittely. Alustava suunnitelma tarpeiden toteuttamistavasta
- Eheyssääntöjen määrittely
- Alustava suunnitelma tietojen eheyden säilyttämisen menettelytavoista
- Kehityksen aikaisten turvaratkaisujen määrittely.

### **Suunnitteluvaiheen tietoturvaluokitustarkastuslista (6.3)**

- Kuvataan peruskontrollien soveltamistapa järjestelmän toiminnoissa
- Kuvataan järjestelmäliittymien peruskontrollit
- Selvitetään ja kuvataan järjestelmän keskeisiin toimintaprosesseihin tarvittavat lisäkontrollit
- Selvitetään ja kuvataan tarkasti järjestelmän tietoturvaluokituskriittisiin yksittäisiin toimintoihin tarvittavat lisäkontrollit
- Verrataan kontrolleja ja niiden toteutuksen vaikutusta tietoturvaluokitusvaatimukseen
- Suunnitellaan peruskontrollien testausmenettely
- Suunnitellaan järjestelmän keskeisiin toimintoihin liittyvien lisäkontrollien testaus
- Suunnitellaan yksittäisten tietoturvaluokituskriittisten kohteiden kontrollien testaus ja määrittää testausvastuut
- Suunnitellaan käyttäjäryhmät ja käyttövaltuudet
- Varmistetaan, että tietoturvaluokitustehtävät sisältyvät seuraaviin vaiheisiin
- Varmistetaan sovittujen tietoturvaluokitusmenettelyjen noudattaminen projektityössä
- Määrittää mitä kontrollimekanismeja sovelletaan perustietoturvaluokitustason järjestelmissä peruskontrolleiksi ja mitkä ovat korkeamman tietoturvaluokitustason järjestelmissä sovellettavia lisäkontrolleja (esimerkkejä liitteenä)
- Suunnitellaan kirjausketjun (audit trail) toteutus
- Suunnitellaan eheyskontrollien toteutus
- Suunnitellaan järjestelmän käyttäjien, johdon ja järjestelmän käytön valvojien koulutus myös tietoturvaluokituksen osalta
- Suunnitellaan varmuuskopiointimenettelyt ja palautukset
- Tarvittaessa suunnitellaan salausmenettelyt, avainten jakelu ja kirjanpito sekä varmentamismenettelyt
- Suunnitellaan testiaineistot huomioiden tietojen luottamuksellisuus.

#### **Toteutusvaiheen tietoturvatarkastuslista (6.4)**

- Tarkistetaan peruskontrollien toteutus pistokokeina
- Tarkistetaan, että järjestelmän keskeisiin toimintoihin liittyvien kontrollien toteutus on määritysten mukainen.
- Tarkistetaan, että järjestelmän yksittäisiin tietoturvallisuuskriittisiin kohteisiin liittyvät kontrollit vastaavat määrityksiä.
- Määritellään, voidaanko testeissä käyttää lainkaan tuotantoaineistoja
- Varmistetaan, että testauksessa poikkeuksellisesti käytettävä tuotantoaineisto ei sekaannu aidon aineiston kanssa.
- Varmistetaan, että em. aineistoon sisältyvät henkilötiedot ja tietoturvallisuuskriittiset osat tiedoista muutetaan tai että ne pysyvät vain tietojen käyttöön valtuutettujen tiedossa.
- Varmistetaan, ettei mahdollinen poikkeuksellinen tuotantotietojen testikäyttö aiheuta väärinkäytösmahdollisuutta
- Varmistetaan, että testiaineisto ja testaus kattavat kaikki turvallisuuden kannalta merkittävät tapaukset.
- Tarkistetaan ohjelmiston kriittisten osien lähdekoodi tekijästä riippumattomasti.
- Estetään hyväksytyjen ohjelmamodulien muutokset
- Tehdään toteutuksen ja testauksen riippumaton tarkastus
- Toteutetaan ja testataan käytön aikaisen kehitys- ja testausympäristön sekä tuotanto-ympäristön turvaaminen
- Tarkennetaan tietoturvallisuuskuvaukset, rakenteellisuus ja dokumentointi
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Tarkistetaan käyttäjien toimintoihin liittyvien peruskontrollien toteutus
- Tarkistetaan käyttäjien toimintoihin liittyvien kontrollien kokonaisuus sekä keskeisiin prosesseihin liittyvät kontrollit
- Varmistetaan, että yksittäisiin tietoturvallisuuskriittisiin käyttäjien toimintoihin liittyvien kontrollien toteutus vastaa asetettuja vaatimuksia.
- Varmistetaan, että käyttäjien koulutussuunnitelmaan sisältyy peruskontrollien käyttökoulutus.
- Varmistetaan, että käyttäjien koulutussuunnitelmaan sisältyy lisäkontrollien käyttökoulutus.
- Tarkistetaan tarvittaessa koulutussuunnitelma yksityiskohtaisesti kontrolleihin liittyvän koulutuksen osalta.
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Luetteloidaan toiminnalliset puutteet ja virheet, jotka on korjattava ennen järjestelmän siirtoa tuotantoon. Laaditaan korjausten toteutus- ja testaussuunnitelma

#### **Käyttöönottovaiheen tietoturvaluustarkastuslista (6.5)**

- Rinnakkaisajon tulosten vertaaminen kontrollien osalta
- Tarkistetaan lisäkontrollien testaussuunnitelma
- Varmistetaan, että testaussuunnitelma kattaa kaikki järjestelmän määrityksiin sisältyvät kontrollit
- Tarkistetaan peruskontrollien testitulokset
- Tarkistetaan lisäkontrollien testitulokset
- Valvotaan kriittisiin toimintoihin liittyvien kontrollien testausta
- Tuotantoaineiston mahdollisen poikkeuksellisen testauskäytön osalta noudatetaan toteutusvaiheessa kuvattuja menettelytapoja

- Luetteloidaan toiminnalliset puutteet ja virheet, jotka voidaan korjata tuotantoon siirron jälkeen ylläpitotyönä. Tehdään ylläpitosuunnitelma
- Varmistetaan sovittujen tietoturvaluokkien noudattaminen projektityössä
- Varmistetaan, että järjestelmän perustietojen latauksessa noudatetaan peruskontrolleja
- Valvotaan perustietojen latauksen kontrollien toimivuutta
- Tarkistetaan toistuvasti kaikki turvallisuuden kannalta merkittävät kontrollit perustietojen latauksessa
- Varmistetaan tuotanto-organisaatiolta, että uuden ohjelmiston asennuksessa noudatetaan peruskontrolleja
- Tarkistetaan pistokokeina ohjelmiston asennuksen kontrollit
- Tarkistetaan, että ohjelmistoasennuksen kontrollit ovat asetettujen vaatimusten mukaiset
- Varmistetaan, että käyttäjien koulutus kontrolleihin liittyen on tehty hyväksytyyn koulutussuunnitelman mukaisesti
- Varmistetaan, että kaikki käyttäjät ovat saaneet kontrolleja koskevan koulutuksen
- Varmistetaan käyttäjäorganisaatiolta, että käyttäjien toimintoihin liittyvät kontrollit vastaavat vaatimuksia
- Tarkistetaan pistokokeina käyttäjien toimintoihin liittyvät tuotantoympäristön kontrollit
- Tarkistetaan, että käyttäjien toimintoihin liittyvät kontrollit tuotantoympäristössä ovat vaatimusten mukaiset
- Varmistetaan järjestelmän ylläpidosta vastaavilta, että kontrollien ylläpitovastuu sisältyy määriteltyihin ylläpitokäytäntöihin
- Tarkistetaan pistokokeina ylläpitäjien järjestelmädokumentaatio
- Tarkistetaan, että ylläpitäjien dokumentaatioon sisältyy kattava kontrollien kuvaus ja että ylläpitomenetelmät varmistavat vaatimusten mukaisen tietoturvaluokkustason säilymisen
- Varmistetaan sovittujen tietoturvaluokkien noudattamisesta
- Varmistetaan, että hyväksymistestaus kattaa muun muassa seuraavat kokonaisuudet:
  - Pääsynvalvontamenettelyjen toimivuus
  - Järjestelmän toiminta normaalissa kuormitusolotilanteessa ja huippukuormituksella
  - Järjestelmän ”kaatuminen” ja vakavat laitehäiriöt
  - Vakavasta virheestä toipuminen (sekä tekniset asiat että käyttäjien toimenpiteet)
  - Järjestelmän perustietojen lataus
  - Tuotannon aikaisen kehitys- ja testausympäristön hallinta
  - Käyttäjien toimintoihin liittyvät kontrollit
  - Järjestelmän teknisessä toteutuksessa
  - Käyttäjien toiminnoissa
  - Käyttöhenkilöstön toimintoihin liittyvät kontrollit
- Varmistetaan onko tietoturvaluokkusuunnitelma tehty?
- Varmistetaan onko tietoturvaluokkusuunnitelma tehty?
- Varmistetaan onko tärkeysluokka määritelty?
- Varmistetaan onko jatkuvuussuunnitelma tehty?
- Varmistetaan sisältyykö jatkuvuussuunnitelmaan toipumissuunnitelma?
  - tiedotussuunnitelma?
  - yhteyshenkilöt?
- Varmistetaan onko varajärjestelmää, onko varajärjestelmä testattu?
- Varmistetaan onko käyttöoikeusmenettelyt kuvattu ja ohjeistettu?
- Varmistetaan onko järjestelmäseloste tehty ohjeiden mukaisesti?
- Tarkistetaan henkilötietojen suojaaminen

## **Ylläpitovaiheen tietoturvatarkastuslista (6.6)**

- Lainsäädännön velvoitteiden läpikäynti ja huomiointi
- Varmistetaan, että muutos on perusteltu ja päätös sen tekemisestä on asianmukaisesti hyväksytty.
- Varmistetaan, että muutoksessa otetaan huomioon järjestelmän alkuperäiset suunnittelukriteerit turvallisuuden kannalta. Poikkeamat perusteltava.
- Selvitetään muutoksen vaikutukset muihin kuin muutettavaan kohteeseen epätoivotujen sivuvaikutusten välttämiseksi.
- Selvitetään järjestelmämuutoksen aiheuttamat turvaamisen muutostarpeet yleisellä tasolla
- Selvitetään muutoksen vaikutus järjestelmän keskeisten osien turvaamiseen
- Selvitetään muutoksen vaikutus järjestelmän yksittäisten kriittisten osien turvaamiseen
- Selvitetään tietokannan rakenteen muutosten tietoturvallisuusvaikutukset
- Selvitetään muutoksen vaikutus käyttäjille näkyviin turvaamisiin ja tehdään muutokset käyttöohjeisiin
- Selvitetään vaikutukset tietoturvallisuuden huomioimisesta kehitysympäristön versioinnissa, muutosten dokumentoinnissa sekä koulutusympäristössä
- Laaditaan turvaamisen toteutus- ja testaussuunnitelma resurssivarauksineen
- Varmistetaan, että muutostoimenpiteen hallinnassa noudatetaan tietoturvallisuusluokituksen mukaisia menettelytapoja (soveltaen ensikehitysprojektin toimintamalleja ja muutoksen laajuutta vastaavasti)
- Varmistetaan, että muutos on testattu kattavasti erillisessä turvallisessa testiympäristössä ennen sen siirtoa tuotantoon
- Tehdään tarvittaessa muutokset jatkuvuussuunnitelmaan
- Testataan jatkuvuussuunnitelman muutokset.

## **Käyttövaiheen tietoturvaluustarkastuslista (6.7)**

### **Järjestelmän käyttöön liittyvät toiminnot**

Hoidetaan osana järjestelmän käyttötoimintaa turvallisuuteen liittyvät tehtävät, joihin sisältyvät muun muassa

- 1) Varmistukset ja arkistointi
- 2) Käyttövaltuuksien hallinta
- 3) Laitteiden poistot ja vaihdot.

Käsitellään osana jatkuvaa päivittäistä toimintaa järjestelmän toimintaan liittyvät tietoturvaluushälytykset ja –poikkeamat.

### **Toipumissuunnitelmien testit**

Varmistetaan, että järjestelmän toipumissuunnitelma testataan sovituin määrävälein sovitussa laajuudessa.

## Järjestelmän tarkastus määrävälein

- Tehdään tietoturvaluustarkastus tarvittaessa.
- Tarkistetaan tietoturvaluuslokit ja analysoidaan havaitut poikkeamat ja ”läheltä piti” –tilanteet.
- Tarkistetaan peruskontrollien toimivuus.
- Selvitetään kontrollien merkittävimmät heikkoudet.
- Selvitetään syyt kontrollien pettämiselle.
- Määritellään tarkastuksen perusteella, ovatko käytettävyys-, eheys- ja luottamuksellisuusvaatimukset muuttuneet alkuperäisistä.

## Havaintojen / analyysin perusteella tehtävät toiminnot

- Tehdään tarvittaessa suositus järjestelmän tärkeysluokan tai tietoaineiston luokituksen ja kontrollien muutoksista (esitutkimus-kohta 6.1).
- Tehdään suositus kontrollien muutoksista.
- Tehdään perusteltu ehdotus kontrollien muutoksista. Sisällytetään ehdotukseen arvio kontrollien muutosten toiminnallisista ja kustannusvaikutuksista.

## Versionvaihtovaiheen tietoturvaluustarkastuslista (6.8)

Tietojen siirto vanhasta järjestelmästä uuteen

- 1) Varmistetaan, että tiedon siirron suunnitelma sisältyy version vaihdon projekti-suunnitelmaan
- 2) Varmistetaan, että siirtosuunnitelmassa on kuvattu toimenpiteet, joilla varmistetaan tiedon siirron täydellisyys sekä siirrettävien tietojen eheys
- 3) Varmistetaan, että siirtotoimenpiteet testataan testiaineistolla ennen tuotantoaineistojen siirtoa. Tarkistetaan testitulokset.
- 4) Varmistetaan, että siirrosta tehtävät välitallennukset eivät vaaranna tiedon luotamuksellisuutta
- 5) Tarkistetaan, että tiedon siirto uuteen järjestelmään on tehty hyväksytyyn suunnitelman mukaisesti.

Tehdään jatkuvuussuunnitelmiin tarvittavat muutokset. Testataan suunnitelman toimivuus mahdollisuuksien mukaan.

Varmistetaan sovittujen tietoturvaluusmenettelyjen noudattaminen projektityössä.

## Käytöstä poistovaiheen tietoturvaluustarkastuslista (6.9)

- Tehdään turvaamisen ylläpitosuunnitelma niille järjestelmille, joiden toimintaan poistettavalla järjestelmällä on vaikutusta
- Selvitetään poistettavan järjestelmän aineistoja koskevat arkistointivelvoitteet arkistomuodostussuunnitelmasta
- Laaditaan hävittämissuunnitelma niille tietoaineistoille, joita ei ole tarpeen arkistoida
- Suunnitellaan poistettavan järjestelmän laitteistojen uudelleenkäyttökohteet tai hävittämismenettelyt
- Tehdään muutokset jatkuvuussuunnitelmiin.
- Toteutetaan poisto sekä mahdolliset arkistoinnit ja laitteistojen sijoittaminen uuteen käyttökohteeseen suunnitelmien mukaisesti pitäen kirjaa tehdyistä toimenpiteistä
- Varmistetaan sovittujen tietoturvaluusmenettelyjen noudattaminen poistamistoimenpiteissä.

**Valtionhallinnon tietoturvallisuuden johtoryhmän vuonna 2000 aiemmin ilmestyneet julkaisut**

- 1/2000 Valtionhallinnon tietoturvaluuskäsitteistö
- 2/2000 Valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje
- 3/2000 Valtionhallinnon tietojärjestelmäkehityksen tietoturvaluussuositus