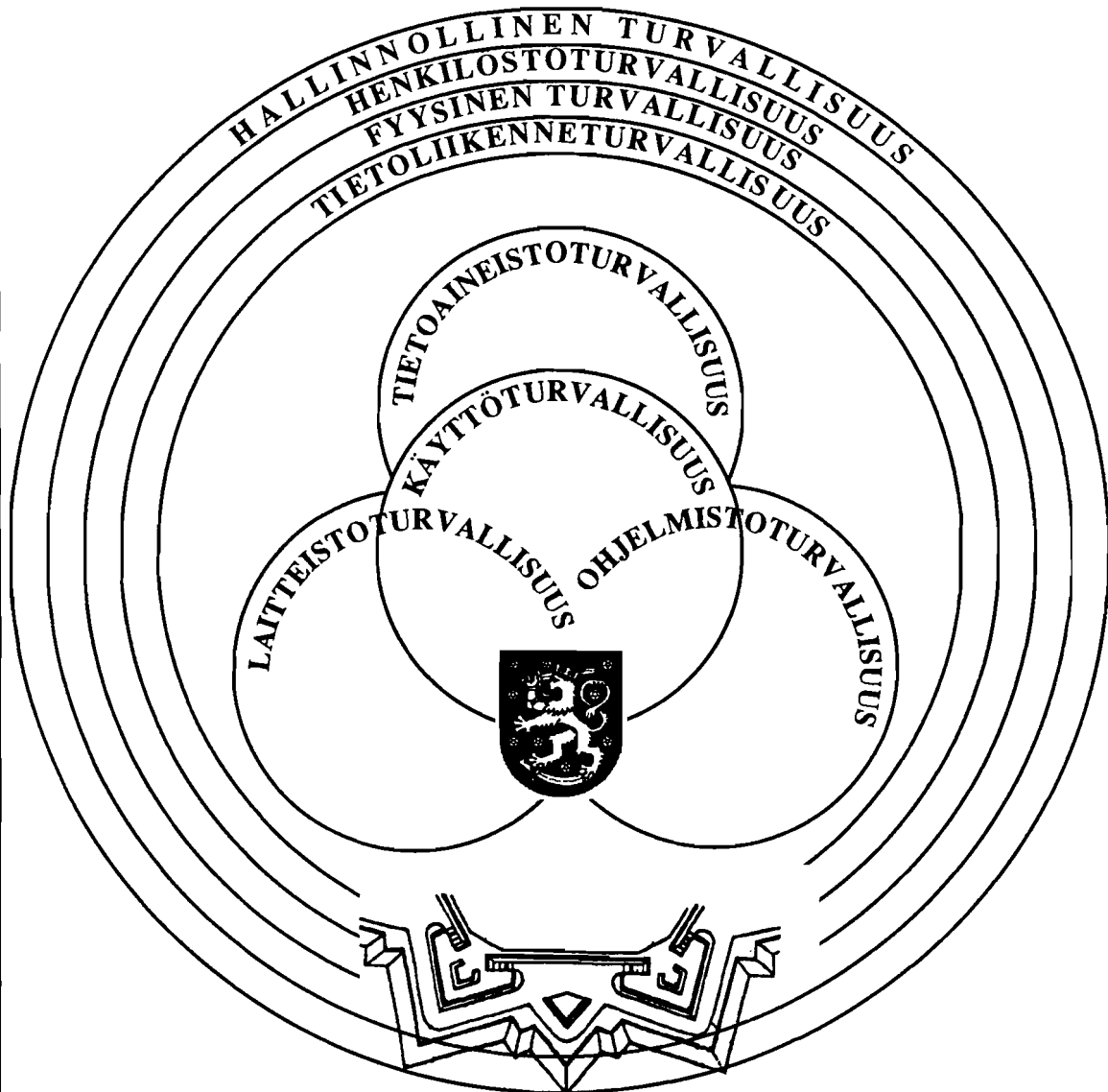


MATTI TENHUNEN:
JULKISHALLINNON JÄRJESTELMIEN
TIETOTURVALLISUUSVAATIMUKSET
1990-LUVULLA



TERVEYDENHUOLLON
ATK-PÄIVÄT

TERVEYS + TEKNIikka

Kongressi- ja messutapahtuma Tampere-talossa

4. - 6. 5. 1993



4.2.1993

VM 1/73/93

**Valtioneuvoston kanslialle,
ministeriöille sekä niiden alaisille
virastoille ja laitoksille**

**VALTIONEUVOSTON
PERIAATEPÄÄTÖS
TIETOTURVALLISUUDEN
KEHITTÄMISESTÄ
VALTIONHALLINNOSSA**

Valtioneuvosto on tänään tehnyt seuraavan periaatepäätöksen valtionhallinnon tietohallinnossa noudatettavista periaatteista tietoturvallisuuden kehittämiseksi.

Tietoturvallisuuden kehittämistavoitteet

Valtionhallinto on suurin yksittäinen tietotekniikan käyttäjä maassamme. Kansalaisille tarjottavien palvelujen ja hallinnon viranomais-tehtävien sujuvuuden kannalta tietojärjestelmien suojaus ja häiriötön toiminta sekä talletettujen tietojen oikeellisuus, luotettavuus ja ajantasaisuus on tärkeää.

Yleisen turvallisuustarpeen lisäksi lähinnä valtionhallinnon tietohallinnosta annettu asetus ja henkilökisterilainsäädäntö sekä eräät hallinnolliset ohjeet sisältävät tietoturvallisuusvelvoitteen. Näiden lisäksi velvoite voi perustua myös sellaisiin kansainvälisiin sopimuksiin, joita Suomi on erikseen sitoutunut noudattamaan.

Tämän valtioneuvoston periaatepäätöksen tarkoituksena on yhtenäistää ja kehittää valtionhallinnon tietoturvallisuuspolitiikkaa sekä siitä annettavia ohjeita ja suosituksia.



4.2.1993

FM 1/73/93

**Till statsrådets kansli,
ministerierna samt de ämbetsverk
och inrättningar som lyder under dem**

**STATSRÅDETS PRINCIPBESLUT
OM UTVECKLANDE
AV
INFORMATIONSSÄKERHETEN
INOM STATSFÖRVALTNINGEN**

Statsrådet har i dag fattat följande principbeslut om vilka principer som skall iakttas inom statsförvaltningens informationsförvaltning i syfte att utveckla informationssäkerheten.

**Målen för utvecklandet av
informationssäkerheten**

Statsförvaltningen är den största enskilda användaren av datateknik i Finland. När det gäller de tjänster som erbjuds medborgarna och flexibiliteten hos förvaltningens myndighetsuppgifter är det viktigt att datasystemen skyddas och fungerar störningsfritt samt att lagrad information är korrekt, tillförlitlig och aktuell.

Utom det allmänna behovet av säkerhet ingår ett krav på informationssäkerhet främst i förordningen om statsförvaltningens informationsförvaltning och lagstiftningen om personregister samt i vissa administrativa anvisningar. Dessutom kan kravet även basera sig på sådana internationella konventioner som Finland särskilt har förbundit sig att iakta.

Avsikten med detta principbeslut av statsrådet är att informationssäkerhetspolitiken inom statsförvaltningen samt de anvisningar och rekommendationer som ges om den skall förenhetligas och utvecklas.

Tietoturvallisuuden kehittäminen tehostaa osaltaan valtionhallinnossa noudatettavien julkisuus- ja avoimuusperiaatteiden mukaista kansalaisten oikeuksien ja etujen turvaamista.

Kansallisesti tietoturvallisuus on takeena valtion, erilaisten yhteisöjen ja kansalaisten perusoikeuksien toteutumiselle.

Kansainvälisesti tietoturvallisuuspolitiikka on asia, jota muut valtiot, ulkomaiset yritykset ja kansainväliset järjestöt yhä useammin edellyttävät yhteistyösapuoliltaan.

Tietoturvallisuuden kehittämisen päätavoite on hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuustason luominen. Hyvään tietojenkäsittelytapaan kuuluu erottamattomasti tietoturvallisuus. Asianmukaista perusturvallisuustasoa tarvitaan, koska valtionhallinnon tiedot, järjestelmät ja palvelut muodostavat taloudellisesti arvokkaan ja valtakunnan turvallisuuden kannalta tärkeän omaisuuden.

Soveltamisala

Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa, josta myöhemmin käytetään nimeä tietoturvallisuuden kehittämisspätös, koskee ministeriöitä, virastoja ja laitoksia sekä näiden ulkopuolisilta hankkimia tietohallintopalveluja.

Kunkin ministeriön, viraston tai laitoksen tulee huolehtia tietoturvallisuudestaan myös hankkiessaan palveluita oman organisaationsa ulkopuolelta. Toimeksianto ei vapauta käyttäjää velvoitteestaan huolehtia tietoturvallisuudesta eikä vastuuta voi siirtää yksinomaan toimeksisaajalle.

Päätöksen periaatteita suositellaan noudatettavaksi myös valtionhallinnon ja muiden organisaatioiden (mm. kunnallishallinnon yksiköt, yritykset ja yhteisöt) välisessä tietoteknisessä yhteistyössä ja tiedonsiirrossa sekä valtion uusimuotoisten liikelaitosten ja valtionyhtiöiden tietoturvallisuustyössä.

Utvecklandet av informationssäkerheten innebär att medborgarnas rättigheter och intressen kan tryggas effektivare enligt de principer om offentlighet och öppenhet som iakttas inom statsförvaltningen.

Nationellt är informationssäkerhet en garanti för statens, olika samfunds och medborgarnas grundläggande rättigheter.

Internationellt är informationssäkerhetspolitik något som andra stater, utländska företag och internationella organisationer allt oftare kräver av sina samarbetspartners.

Det huvudsakliga målet för utvecklandet av informationssäkerheten är att skapa en god databehandlingssed och en behörig grundsäkerhetsnivå. Informationssäkerhet hör oskiljaktigt samman med god databehandlingssed. En behörig grundsäkerhetsnivå behövs, eftersom informationen, systemen och tjänsterna inom statsförvaltningen utgör en ekonomiskt sett värdefull och med avseende på rikets säkerhet viktig egendom.

Tillämpningsområde

Statsrådets principbeslut om utvecklande av informationssäkerheten inom statsförvaltningen, nedan beslutet om utvecklande av informationssäkerheten, gäller ministerier, ämbetsverk och inrättningar och sådana informationsförvaltningstjänster som dessa skaffar hos utomstående.

Varje ministerium, ämbetsverk eller inrättning skall även när tjänster skaffas utanför den egna organisationen sörja för informationssäkerheten. Ett uppdrag befriar inte användaren från skyldigheten att sörja för informationssäkerheten och ansvaret kan inte helt överföras på uppdragstagaren.

Enligt rekommendationer skall principerna i beslutet även iakttas i datatekniskt samarbete och dataöverföring mellan statsförvaltningen och andra organisationer (bl.a. enheter inom kommunalförvaltningen, företag och samfund) samt i informationssäkerhetsarbetet vid statliga affärsverk och statsbolag av ny typ.

Tietoturvallisuuden perusosat

Tässä periaatepäätöksessä tietoturvallisuudella tarkoitetaan asiaintilaa, jossa tiedot, järjestelmät ja palvelut ovat asianmukaisesti suojattuja sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuus perustuu tiedon kolmeen eri ominaisuuteen; luottamuksellisuuteen, eheyteen ja käytettävyyteen.

1) *Luottamuksellisuus*; tiedot ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.

2) *Eheys*; tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ne ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

3) *Käytettävyys*; järjestelmien tiedot ja muodostamat palvelut ovat tarvittaessa niihin oikeutettujen käytettävissä.

Tietoturvallisuus jaetaan suunnittelun, toteutuksen ja valvonnan kannalta seuraaviin kahdeksaan osa-alueeseen:

- 1) Hallinnollinen tietoturvallisuus,
- 2) Henkilöstöturvallisuus,
- 3) Fyysinen turvallisuus,
- 4) Tietoliikenneturvallisuus,
- 5) Laitteistoturvallisuus,
- 6) Ohjelmistoturvallisuus,
- 7) Tietoaineistoturvallisuus ja
- 8) Käyttöturvallisuus.

Tietoturvallisuuden osa-alueiden tarkempaa sisältöä käsitellään tietoturvallisuuden kehittämissä päätöksen jälkeen annettavassa valtiovarainministeriön ohjeessa.

Informationssäkerhetens grundbegrepp

I detta principbeslut avses med informationssäkerhet ett tillstånd där information, system och tjänster både under normala förhållanden och vid undantagsförhållanden på ett behörigt sätt är skyddade med hjälp av administrativa, tekniska och andra åtgärder. Uppgifternas konfidentiella karaktär, integritet och tillgänglighet skyddas mot fel i maskin- eller programvara, naturföreteelser och sådana hot och skador som människor genom sina handlingar uppsåtligen, av vållande eller genom olycksfall förorsakar.

Informationssäkerheten baserar sig på tre olika egenskaper hos informationen: dess konfidentiella karaktär, integritet och tillgänglighet.

1) *Konfidentiell karaktär*; informationen är tillgänglig endast för dem som är berättigade att använda den, den röjs inte för utomstående och den ställs inte heller i övrigt till deras förfogande.

2) *Integritet*; informationen och systemen är tillförlitliga, korrekta och aktuella och har varken förändrats eller förstörts på grund av fel i maskin- eller programvara, naturföreteelser eller oberättigade mänskliga handlingar.

3) *Tillgänglighet*; informationen i systemen och den service de erbjuder är vid behov tillgänglig för sådana som är berättigade till den.

Informationssäkerheten omfattar följande åtta delområden med avseende på planering, genomförande och övervakning:

- 1) Administrativ informationssäkerhet,
- 2) Personalsäkerhet,
- 3) Fysisk säkerhet,
- 4) Datakommunikationssäkerhet,
- 5) Maskinvarusäkerhet,
- 6) Programvarusäkerhet,
- 7) Informationsmaterialsäkerhet och
- 8) Användarsäkerhet.

Innehållet i informationssäkerhetens delområden behandlas närmare i anvisningar som finansministeriet meddelar efter beslutet om utvecklande av informationssäkerheten.

Tietoturvallisuusriskien hallinta

Tietoturvallisuuden luomiseksi on ministeriöiden sekä virastojen ja laitosten johdon kyettävä pääpiirteittäin tunnistamaan, arvioimaan ja hallitsemaan riippuvuutensa tietojenkäsittelytoiminnasta sekä erityisesti tietotekniikan käyttöön liittyvät uhkatekijät ja riskit.

Turvallisuustoimenpiteiden tavoitteena on hyvän tietojenkäsittelytavan ja asianmukaisen tietoturvallisuuden perustason luominen.

Turvallisuustoimenpiteitä koskevien päätösten pohjaksi tarvittavan tietoturvallisuusanalyysin kukin organisaatio laatii itse. Tarkastelun kohteena ovat tällöin:

- 1) Organisaation tietojenkäsittelyn kokonaisuus, tietojärjestelmät sekä niiden tietosisällön kuvaukset,
- 2) Uhkien selvitys ja riskien arviointi sekä
- 3) Tarvittavien toimenpiteiden määrittely.

Tietoturvallisuusanalyysi ja sen mukaan tehdyt päätökset muodostavat yhdessä kehittämistyön kannalta tärkeän tietoturvallisuussuunnitelman.

Organisointi ja tehtävät

Kunkin valtion viraston tai laitoksen tehtävänä on huolehtia oman organisaationsa ja hankkimiansa palvelujen tietoturvallisuudesta sekä laatia tarvittaessa tarkemmat lisäohjeet.

Viraston tai laitoksen kuuluu myös huolehtia tietojenkäsittelyn valmiussuunnittelusta ja varautumisesta poikkeusoloihin sekä tietoturvallisuuskoulutuksen antamisesta henkilöstölleen.

Kunkin ministeriön tehtävänä on lisäksi hallinnonalansa tietoturvallisuustoiminnan yleisohjaus ja valvonta sekä tarvittaessa tarkempien ohjeiden antaminen. Valvontaan tulisi sisältyä myös tietoturvallisuustoimenpiteisiin liittyviä tarkastuksia.

Hantering av informationssäkerhetsrisker

Ledningen för ministerierna samt för ämbetsverken och inrättningarna skall i syfte att skapa informationssäkerhet i huvuddrag kunna identifiera, bedöma och hantera sitt beroende av databehandling samt i synnerhet riskfaktorer i samband med användningen av datateknik.

Målet för säkerhetsåtgärderna är att en god databehandlingssed och en behörig grundnivå för informationssäkerheten skall skapas.

Den informationssäkerhetsanalys som behövs som grund för beslut som fattas om säkerhetsåtgärder utför varje organisation själv. Föremål för granskning är då

- 1) Databehandlingen inom organisationen i sin helhet, datasystemen och beskrivningar av datainnehållet i dem,
- 2) Klarläggandet och bedömningen av risker samt
- 3) Preciseringen av behövliga åtgärder.

Informationssäkerhetsanalysen och beslut som fattas i enlighet med den utgör tillsammans en informationssäkerhetsplan som är viktig för utvecklingsarbetet.

Organisering och uppgifter

Varje statligt ämbetsverk eller statlig inrättning har till uppgift att sörja för informationssäkerheten inom den egna organisationen och i fråga om den service som anskaffas samt att vid behov utarbeta detaljerade anvisningar.

Ämbetsverken eller inrättningarna skall dessutom sörja för beredskapsplanering och förberedelser för undantagsförhållanden i fråga om databehandling samt för att deras personal utbildas i informationssäkerhet.

Varje ministerium skall dessutom sörja för den allmänna ledningen och övervakningen av informationssäkerheten inom sitt förvaltningsområde samt vid behov meddela närmare anvisningar. Övervakningen bör även omfatta kontroller i anslutning till informationssäkerhetsåtgärderna.

Viraston tai laitoksen ylin johto hyväksyy ja vahvistaa tietoturvallisuustyön tavoitteet ja menettelytavat sekä määrittelee tarvittavan organisaation, tehtävät ja vastuut. Tietoturvallisuustehtävät ulottuvat organisaation johdosta ja sovellusten vastuuhenkilöistä aina peruskäyttäjiin asti viraston tai laitoksen päättämällä tavalla sekä voimassa olevien säännösten mukaisesti.

Tietoturvallisuustoimenpiteiden aiheuttamat kustannukset ovat normaaleja toimintamenoja ja ne otetaan huomioon toimintaa suunniteltaessa sekä laadittaessa aikatauluja, talousarvioita ja -esityksiä.

Tietoturvallisuuden ohjaus

Tietoturvallisuustyön ohjaukseen osallistuvat jäljempänä mainitut organisaatiot, joiden tietoturvallisuustehtävät ovat seuraavat:

Valtiovarainministeriö ohjaa ja yhteensovittaa valtion tietohallinnon kehittämistä valtionhallinnon tietohallinnosta annetun asetuksen (155/88) mukaan. Siten se ohjaa ja yhteensovittaa myös normaaliolojen tietotekniikkatoimintaan kuuluvaa turvallisuustyötä antamalla valtionhallinnon tietoturvallisuuden yleislinjaukseen liittyviä ohjeita ja suosituksia.

Valtiovarainministeriötä avustaa näissä tehtävissä ministeriön asettama *valtiorhallinnon tietoturvallisuuden johtoryhmä*.

Valtioneuvosto voi asettaa poikkeusoloissa valmiuslain (1080/91) perusteella valtiovarainministeriön alaisuuteen *säännöstely-yksikön*. Sen tehtävänä on toimia koko maan tietotekniikka-toimintojen toimintaedellytysten varmistamiseksi tarvittavan ohjauksen ja säännöstelyn toimeenpanoon ja valmisteluun liittyviä tehtäviä hoitavana viranomaisena.

Den högsta ledningen för ett ämbetsverk eller en inrättning skall godkänna och fastställa målen för och procedureerna i informationssäkerhetsarbetet samt definiera vilken organisation som behövs samt uppgifter och ansvar. Informationssäkerhetsuppgifterna sträcker sig från organisationens ledning och de personer som ansvarar för tillämpningarna till primäranvändarna enligt vad ämbetsverket eller inrättningen bestämmer samt enligt gällande stadganden.

De kostnader som informationssäkerhetsåtgärderna ger upphov till är normala omkostnader och beaktas när verksamheten planeras och tidtabeller, budgeter och budgetförslag utarbetas.

Styrningen av informationssäkerheten

I styrningen av informationssäkerhetsarbetet deltar nedan nämnda organisationer, som har följande informationssäkerhetsuppgifter:

Finansministeriet leder och samordnar utvecklandet av statens informationsförvaltning enligt förordningen om statsförvaltningens informationsförvaltning (155/88). Ministeriet leder och samordnar sålunda även säkerhetsarbetet inom datateknikens område under normala förhållanden genom att ge anvisningar och rekommendationer om den allmänna linjedragningen beträffande informationssäkerheten inom statsförvaltningen.

Finansministeriet biträds i dessa uppgifter av *ledningsgruppen för informationssäkerheten inom statsförvaltningen*, som tillsatts av ministeriet.

Statsrådet kan vid undantagsförhållanden på basis av beredskapslagen (1080/91) tillsätta en *regleringsenhet*, som lyder under finansministeriet. Dess uppgift är att vara en myndighet som sköter uppgifter i anslutning till verkställigheten och beredningen av sådan styrning och reglering som behövs för att trygga verksamhetsförutsättningarna för datatekniken i hela Finland.

Valtioneuvoston kanslian ja kunkin ministeriön tehtävänä on valtionhallinnon tietohallinnosta annetun asetuksen mukaisesti kehittää ja ohjata tietohallintoa omalla hallinnonalallaan

Valtioneuvoston kanslian tehtävänä on valtioneuvoston tietoverkon ja sen sovellusten turvallisuuteen liittyvä ohjaus ja ohjeistus valtioneuvoston runkoverkon osalta.

Sisäasiainministeriön tehtävänä ovat lääni- ja kunnallishallintoon liittyvät yleiset tietoturvasuustehtävät ja yleisohjeistus silloin, kun valtion ja kuntien tietojärjestelmillä on välittömiä liittyviä toisiinsa.

Liikenneministeriö ohjaa ja yhteensovittaa tietoliikenneverkkojen ja -palveluiden turvaamiseen liittyviä toimenpiteitä.

Liikenneministeriön alaisella *Telehallintokeskuksella* on tietoliikennejärjestelmien tekniseen turvaamiseen liittyviä ohjaustehtäviä. Lisäksi ministeriötä avustavat *Sähköisen viestinnän varautumisen neuvottelukunta* sekä lääninhallitusten alaisina toimivat *sähköisen viestinnän valmiusrhytmät* suunnittelemalla ja valmistelemalla teletoiminnan turvaamiseen liittyviä asioita.

Tietosuojavaltuutettu antaa henkilörekisterilain ja asetuksen (471/87, 476/87) perusteella tarkempia ohjeita henkilörekisterien tietosuojasta ja valvoo rekisteritoiminnan turvallisuutta sekä suorittaa siihen liittyviä tarkastuksia.

Valtionarkisto antaa arkistolain ja -asetuksen (L 184/81 ja A 1012/82, muutettu 1290/87) perusteella asiakirjahallintoon liittyviä ohjeita tietoaineistojen säilytyksestä, säilyvyydestä ja hävittämisestä.

Statsrådets kansli och varje ministerium skall i enlighet med förordningen om statsförvaltningens informationsförvaltning utveckla och styra informationsförvaltningen inom sitt förvaltningsområde

Statsrådets kansli skall i fråga om statsrådets nätverk, som förenar ministerierna, sörja för meddelandet av anvisningar om och styrningen av säkerheten i statsrådets datanät och dess tillämpningar.

Inrikesministeriet skall sörja för allmänna informationssäkerhetsuppgifter inom läns- och kommunalförvaltningen och meddelandet av allmänna anvisningar i det fall att det finns direktförbindelser mellan statens och kommunernas data-system.

Trafikministeriet leder och samordnar åtgärder i anslutning till säkerställandet av datakommunikationsnät och datakommunikationsservice.

Teleförvaltningscentralen, som lyder under trafikministeriet, har styrningsuppgifter i samband med det tekniska säkerställandet av datakommunikationsnät. Dessutom biträds ministeriet av *delegationen för beredskap för elektronisk kommunikation* samt *beredskapsgrupper för elektronisk kommunikation*, som lyder under länsstyrelserna, genom att dessa planerar och bereder ärenden i anslutning till tryggheten av televerksamheten.

Dataombudsmannen meddelar på basis av personregisterlagen och personregisterförordningen (471/87, 476/87) närmare anvisningar om datasekretessen i personregistren och övervakar säkerheten i registerverksamheten samt utför inspektioner i anslutning därtill.

Riksarkivet meddelar på basis av arkivlagen och arkivförordningen (lag 184/81 och förordning 1012/82, ändrad 1290/87) anvisningar om dokumentförvaltningen i fråga om förvaring och utgallring av samt beständighet hos informationsmaterial.

Valtiontalouden tarkastusvirasto (L 967/47) suorittaa valtionhallinnon tietojenkäsittelyn ja tietohallinnon ohjaukseen sekä virastojen ja laitosten tietoturvallisuuteen liittyviä tarkastuksia ja valvontaa.

Poliisiviranomaiset ja erityisesti *keskusrikospoliisi* ja *suojelupoliisi* suorittavat tietoturvallisuuden loukkauksien ja tietotekniikkarikosten ennaltaehkäisemistä, selvittämistä ja syyteharkintaan saattamista.

Puolustustaloudellisen suunnittelukunnan (L 238/60) *atk-toimikunta* ohjaa ja kehittää virastojen, laitosten ja elinkeinoelämän tietojenkäsittelyn valmiussuunnittelua ja varautumista poikkeusoloihin. Tässä tehtävässä sitä avustaa valtionhallinnon tietoturvallisuuden johtoryhmä.

Valtion hankintakeskus (L 265/41 ja A 741/74) varastoi keskeisimpiä atk-tarvikkeita valtionhallinnon tietojenkäsittelyn jatkuvuuden turvaamiseksi poikkeusoloissa.

Statens revisionsverk (Lag 967/47) kontrollerar och övervakar styrningen av statsförvaltningens databehandling och informationsförvaltning samt ämbetsverkens och inrättningarnas informationssäkerhet.

Kränkningar av informationssäkerheten och datateknikbrott förebyggs, utreds och anmäls till åtalsprövning av polismyndigheterna och i synnerhet av *centralkriminalpolis* och *skyddspolis*.

Försvarsekonomiska planeringskommissionens ADB-kommitté (lag 238/60) leder och utvecklar beredningsplaneringen och förberedelserna för undantagsförhållanden inom databehandlingen vid ämbetsverk och inrättningar samt inom näringslivet. I denna uppgift biträds kommittén av ledningsgruppen för informationssäkerheten inom statsförvaltningen.

Statens upphandlingscentral (lag 265/41 och förordning 741/74) upplagar de viktigaste ADB-förnödenheterna för att trygga en kontinuerlig databehandling inom statsförvaltningen vid undantagsförhållanden.

Tietoturvallisuustoimenpiteet

Tietoturvallisuuden kehittämiseksi tarvittavat toimenpiteet voidaan jakaa kahteen osaan:

- 1) Perusturvallisuuden takaavat toimenpiteet ja
- 2) Lisäturvallisuustoimenpiteet.

Perusturvallisuustoimenpiteet muodostavat virastojen ja laitosten tietoturvallisuuden kehittämisen rungon.

Lisäturvallisuustoimenpiteet ovat suositeltavia ja niiden käytöstä voidaan päättää virasto- ja laitostyökohtaisesti. Perus- ja lisäturvallisuustoimenpiteitä käsitellään laajemmin annettavassa valtiovaraministeriön ohjeessa.

Informationssäkerhetsåtgärder

De åtgärder som behövs för att utveckla informationssäkerheten omfattar

- 1) Åtgärder som garanterar grundsäkerheten och
- 2) Ytterligare säkerhetsåtgärder.

Grundsäkerhetsåtgärderna utgör stommen i utvecklandet av informationssäkerheten vid ämbetsverk och inrättningar.

Ytterligare säkerhetsåtgärder kan rekommenderas. Om tillämpningen av dem kan varje ämbetsverk och inrättning besluta särskilt. Grundsäkerhetsåtgärder och ytterligare säkerhetsåtgärder behandlas mera ingående i anvisningar från finansministeriet.

Virastojen ja laitosten on tarpeen organisaatio-kohtaisesti selvittää tietojärjestelmiensä ja niiden tietojen merkitys toiminnalle, arvioida kysymykseen tulevat uhat sekä valita ja toteuttaa perusturvallisuustoimenpiteiden lisäksi tarvittavat lisäturvallisuustoimenpiteet.

Toteuttaminen

Tietoturvallisuuden kehittämiseksi on virastojen ja laitosten sekä päätöksen mukaisia ohjaustehtäviä suorittavien organisaatioiden tarpeen selvittää ne puutteet, joita esiintyy tietoturvallisuuden kehittämispäätöksessä määriteltyyn verrattuna sekä päättää tarvittavista toimenpiteistä ja niiden toteuttamisaikataulusta.

Tietoturvallisuuden kehittämispäätöksen mukaisesti tarkastus- ja valvontatehtäviä suorittavat organisaatiot sekä kukin organisaatio itse seuraa periaatepäätöksen toteutumista ja tietoturvallisuuden kehitystä.

Valtiovarainministeriö antaa tämän valtionhallinnon tietoturvallisuutta koskevan periaatepäätöksen osalta tarkentavia yleisohjeita.

Ministeri

Ilkka Kanerva

Neuvotteleva virkamies

Kaarlo Korvola

Det är nödvändigt att ämbetsverken och i-rättingarna för varje organisation särskilt klarlägger vilken betydelse datasystemen och den informationen de innehåller har för verksamheten, bedömer aktuella risker samt väljer och vidtar sådana ytterligare säkerhetsåtgärder som behövs utöver grundsäkerhetsåtgärder.

Genomförande

För att informationssäkerheten skall utvecklas är det nödvändigt att ämbetsverken och inrättingarna samt organisationer som utför styrningsuppgifter i enlighet med beslutet klarlägger de brister som förekommer jämfört med den nivå som definieras i beslutet om utvecklande av informationssäkerheten samt beslutar om vilka åtgärder som behövs och inom vilken tidtabell de skall vidtas.

Organisationer som utför kontroll- och övervakningsuppgifter enligt beslutet om utvecklande av informationssäkerheten samt varje enskild organisation iakttar hur principbeslutet verkställs och hur informationssäkerheten utvecklas.

Finansministeriet meddelar allmänna preciserande anvisningar beträffande detta principbeslut om informationssäkerheten inom statsförvaltningen.

Minister

Ilkka Kanerva

Konsultativ tjänsteman

Kaarlo Korvola