KOMISSION PÄÄTÖS,

annettu 4 päivänä toukokuuta 2010,

SIS II:n keskusjärjestelmään ja viestintäinfrastruktuuriin liittyvästä turvasuunnitelmasta

(2010/261/EU)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä 20 päivänä joulukuuta 2006 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1987/2006 [1] ja erityisesti sen 16 artiklan,

ottaa huomioon toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä 12 päivänä kesäkuuta 2007 tehdyn neuvoston päätöksen 2007/533/YOS [2] ja erityisesti sen 16 artiklan,

sekä katsoo seuraavaa:

(1) Asetuksen (EY) N:o 1987/2006 16 artiklassa ja päätöksen 2007/533/YOS 16 artiklassa säädetään, että tietokantaa hallinnoivan viranomaisen on toteutettava SIS II:n keskusjärjestelmän osalta ja komission on toteutettava viestintäinfrastruktuurin osalta tarvittavat toimenpiteet, turvasuunnitelma mukaan lukien.

(2) Asetuksen (EY) N:o 1987/2006 15 artiklan 4 kohdan ja päätöksen 2007/533/YOS 15 artiklan 4 kohdan mukaan komissio vastaa SIS II:n keskusjärjestelmän operatiivisesta hallinnoinnista siirtymäkautena, ennen kuin tietokantaa hallinnoiva viranomainen ottaa tehtävänsä vastaan.

(3) Koska tietokantaa hallinnoivaa viranomaista ei ole vielä perustettu, komission laatimaa turvasuunnitelmaa olisi sovellettava siirtymäkautena myös SIS II:n keskusjärjestelmään.

(4) Komission suorittamaan henkilötietojen käsittelyyn, joka liittyy sen velvollisuuteen huolehtia SIS II:n operatiivisesta hallinnoinnista, sovelletaan Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001 [3].

(5) Asetuksen (EY) N:o 1987/2006 15 artiklan 7 kohdassa ja päätöksen 2007/533/YOS 15 artiklan 7 kohdassa säädetään, että mikäli komissio siirtää vastuualaansa kuuluvia tehtäviä siirtymäkautena ennen kuin tietokantaa hallinnoiva viranomainen ottaa tehtävänsä vastaan, sen on varmistettava, ettei tehtävien siirto vaikuta haitallisesti unionin lainsäädännön nojalla toimivien valvontajärjestelmien tehokkuuteen unionin tuomioistuimen, tilintarkastustuomioistuimen tai Euroopan tietosuojavaltuutetun osalta.

(6) Tietokantaa hallinnoivan viranomaisen olisi laadittava oma SIS II:n keskusjärjestelmää koskeva turvasuunnitelmansa heti kun se on ottanut tehtävänsä vastaan. Tämän turvasuunnitelman voimassaolon olisi sen vuoksi päätyttävä SIS II:n keskusjärjestelmän osalta heti kun tietokantaa hallinnoiva viranomainen ottaa tehtävänsä vastaan.

(7) Asetuksen (EY) N:o 1987/2006 4 artiklan 3 kohdan ja päätöksen 2007/533/YOS 4 artiklan 3 kohdan mukaan CS-SIS, joka huolehtii teknisistä valvonta- ja hallintotehtävistä, sijaitsee Strasbourgissa (Ranska), ja CS-SIS:n varakeskus, joka voi huolehtia kaikista CS-SIS:n pääkeskuksen toiminnoista, jos järjestelmään tulee vika, sijaitsee Sankt Johann im Pongaussa (Itävalta).

(8) Turvasuunnitelmassa olisi määrättävä, että nimetään yksi järjestelmän turvallisuusvastaava, jonka vastuulla ovat SIS II:n keskusjärjestelmän ja viestintäinfrastruktuurin turvallisuuteen liittyvät tehtävät, sekä kaksi paikallista turvallisuusvastaavaa, joista toisen vastuulla ovat SIS II:n keskusjärjestelmän turvallisuuteen liittyvät ja toisen vastuulla viestintäinfrastruktuurin turvallisuuteen liittyvät tehtävät. Jotta voidaan varmistaa tietoturvaloukkausten tehokas ja ripeä käsittely ja niistä raportointi, olisi määritettävä turvallisuusvastaavien tehtävät.

(9) Olisi laadittava turvapolitiikka, jossa kuvataan yksityiskohtaisesti kaikki tekniikkaa ja organisaatiota koskevat tiedot tämän päätöksen säännösten mukaisesti.

(10) Olisi määritettävä toimenpiteet, joilla voidaan varmistaa SIS II:n keskusjärjestelmän ja viestintäinfrastruktuurin toiminnan riittävä turvallisuus,

[1] EUVL L 381, 28.12.2006, s. 4.
[2] EUVL L 205, 7.8.2007, s. 63.
[3] EYVL L 8, 12.1.2001, s. 1.

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

1. Tässä päätöksessä vahvistetaan turvaorganisaatio ja toimet (turvasuunnitelma), joilla suojataan SIS II:n keskusjärjestelmä ja siinä käsiteltävät tiedot niiden saatavuuteen, eheyteen ja luottamuksellisuuteen kohdistuvilta uhkilta asetuksen (EY) N:o 1987/2006 16 artiklan 1 kohdassa ja toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä tehdyn päätöksen 2007/533/YOS 16 artiklan 1 kohdassa tarkoitetulla tavalla siirtymäkautena, kunnes tietokantaa hallinnoiva viranomainen ottaa tehtävänsä vastaan.

2. Tässä päätöksessä vahvistetaan turvaorganisaatio ja toimet (turvasuunnitelma), joilla suojataan viestintäinfrastruktuuri sen saatavuuteen, eheyteen ja luottamuksellisuuteen kohdistuvilta uhkilta asetuksen (EY) N:o 1987/2006 16 artiklassa ja toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä tehdyn päätöksen 2007/533/YOS 16 artiklassa tarkoitetulla tavalla.

II LUKU

ORGANISAATIO, VASTUUALUEET JA TIETOTURVALOUKKAUSTEN HALLINTA

2 artikla

Komission tehtävät

1. Komissio huolehtii tässä päätöksessä tarkoitettujen, SIS II:n keskusjärjestelmää koskevien turvatoimien tehokkaasta täytäntöönpanosta ja seurannasta.

2. Komissio huolehtii tässä päätöksessä tarkoitettujen, viestintäinfrastruktuuria koskevien turvatoimien tehokkaasta täytäntöönpanosta ja seurannasta.

3. Komissio nimeää yhden virkamiehistään järjestelmän turvallisuusvastaavaksi. Järjestelmän turvallisuusvastaavan nimittää komission oikeus-, vapaus- ja turvallisuusasioiden pääosaston pääjohtaja. Järjestelmän turvallisuusvastaavan tehtävänä on erityisesti:

a) valmistella turvapolitiikka tämän päätöksen 7 artiklassa kuvatun mukaisesti;

b) valvoa SIS II:n keskusjärjestelmän turvamenettelyjen tehokasta täytäntöönpanoa;

c) valvoa viestintäinfrastruktuurin turvamenettelyjen tehokasta täytäntöönpanoa;

d) osallistua asetuksen (EY) N:o 1987/2006 50 artiklassa ja päätöksen 2007/533/YOS 66 artiklassa tarkoitettujen turvallisuutta koskevien kertomusten valmisteluun;

e) antaa koordinointitukea ja muuta apua Euroopan tietosuojavaltuutetulle asetuksen (EY) N:o 1987/2006 45 artiklassa ja päätöksen 2007/533/YOS 61 artiklassa tarkoitettujen tarkastusten ja valvonnan suorittamisessa sekä tämän päätöksen 5 artiklan 2 kohdassa tarkoitettujen turvaloukkauksia koskevien ilmoitusten toimittamisessa komission tietosuojavastaavalle;

f) valvoa, että kaikki SIS II:n keskusjärjestelmän hallinnointiin osallistuvat hankkijat ja alihankkijat noudattavat tätä päätöstä ja turvapolitiikkaa asianmukaisesti ja kokonaisuudessaan;

g) valvoa, että kaikki viestintäinfrastruktuurin hallinnointiin osallistuvat hankkijat ja alihankkijat noudattavat tätä päätöstä ja turvapolitiikkaa asianmukaisesti ja kokonaisuudessaan;

h) pitää yllä luetteloa SIS II:n turvallisuudesta vastaavista kansallisista yhteyspisteistä ja toimittaa luettelo viestintäinfrastruktuurin paikalliselle turvallisuusvastaavalle;

i) toimittaa h kohdassa tarkoitettu luettelo SIS II:n keskusjärjestelmän paikalliselle turvallisuusvastaavalle.

3 artikla

SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava

1. Komissio nimeää yhden virkamiehistään SIS II:n keskusjärjestelmän paikalliseksi turvallisuusvastaavaksi, sanotun kuitenkaan rajoittamatta 8 artiklan soveltamista. On huolehdittava siitä, että paikallisen turvallisuusvastaavan tehtävä ei ole ristiriidassa henkilön muiden tehtävien kanssa. SIS II:n keskusjärjestelmän paikallisen turvallisuusvastaavan nimittää komission oikeus-, vapaus- ja turvallisuusasioiden pääosaston pääjohtaja.

2. SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava huolehtii siitä, että tässä päätöksessä tarkoitetut turvatoimet pannaan täytäntöön ja että CS-SIS:n pääkeskuksessa noudatetaan turvamenettelyjä. SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava huolehtii myös CS-SIS:n varakeskuksen osalta siitä, että tässä päätöksessä tarkoitetut turvatoimet, lukuun ottamatta 9 artiklassa tarkoitettuja toimenpiteitä, pannaan täytäntöön ja että turvamenettelyjä noudatetaan.

3. SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava voi siirtää osan tehtävistään alaisilleen. On huolehdittava siitä, että näiden tehtävien suorittaminen ei ole ristiriidassa muiden tehtävien kanssa. Paikallinen turvallisuusvastaava tai hänen kulloinkin työvuorossa oleva alaisensa on milloin tahansa tavoitettavissa yhdestä puhelinnumerosta ja osoitteesta.

4. SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava suorittaa CS-SIS:n pääkeskuksen ja varakeskuksen sijaintipaikoissa toteutettaviin turvatoimiin liittyvät tehtävät 1 kohdassa asetetut rajoitukset huomioon ottaen, ja erityisesti:

a) huolehtii paikallisten toimintojen turvallisuuteen liittyvistä tehtävistä, kuten palomuurien testauksesta, säännöllisestä turvatestauksesta, tarkastuksista ja turva-asioista raportoinnista;

b) valvoo toiminnan jatkuvuussuunnitelman tehokuutta ja huolehtii säännöllisten harjoitusten toteuttamisesta;

c) turvaa kaikkia SIS II:n keskusjärjestelmän tai viestintäinfrastruktuurin turvallisuuteen mahdollisesti vaikuttavia SIS II:n keskusjärjestelmän tapahtuvia koskevan todistusaineiston ja raportoi tapahtumista järjestelmän turvallisuusvastaavalle;

d) ilmoittaa järjestelmän turvallisuusvastaavalle, jos turvapolitiikkaa on muutettava;

e) valvoo, että kaikki SIS II:n keskusjärjestelmän hallinnointiin osallistuvat hankkijat ja alihankkijat noudattavat tätä päätöstä ja turvapolitiikkaa;

f) varmistaa, että henkilöstö on tietoinen velvollisuuksistaan, ja valvoo turvapolitiikan noudattamista;

g) valvoo tietoturvan kehitystä ja varmistaa, että henkilöstö saa asianmukaista koulutusta;

h) hankkii turvapolitiikan laatimisessa, päivittämisessä ja tarkistamisessa tarvittavat tiedot ja valmistelee eri toimintavaihtoehdot 7 artiklan mukaisesti.

4 artikla

Viestintäinfrastruktuurin paikallinen turvallisuusvastaava

1. Komissio nimeää yhden virkamiehistään viestintäinfrastruktuurin paikalliseksi turvallisuusvastaavaksi, sanotun kuitenkaan rajoittamatta 8 artiklan soveltamista. On huolehdittava siitä, että paikallisen turvallisuusvastaavan tehtävä ei ole ristiriidassa henkilön muiden tehtävien kanssa. Viestintäinfrastruktuurin paikallisen turvallisuusvastaavan nimittää komission oikeus-, vapaus- ja turvallisuusasioiden pääosaston pääjohtaja.

2. Viestintäinfrastruktuurin paikallinen turvallisuusvastaava valvoo viestintäinfrastruktuurin toimintaa ja varmistaa, että turvatoimet pannaan täytäntöön ja turvamenettelyjä noudatetaan.

3. Viestintäinfrastruktuurin paikallinen turvallisuusvastaava voi siirtää osan tehtävistään alaisilleen. On huolehdittava siitä, että näiden tehtävien suorittaminen ei ole ristiriidassa muiden tehtävien kanssa. Paikallinen turvallisuusvastaava tai hänen kulloinkin työvuorossa oleva alaisensa on milloin tahansa tavoitettavissa yhdestä puhelinnumerosta ja osoitteesta.

4. Viestintäinfrastruktuurin paikallinen turvallisuusvastaava toteuttaa viestintäinfrastruktuuria koskeviin turvatoimiin liittyvät tehtävät ja erityisesti:

a) huolehtii kaikista viestintäinfrastruktuurin toiminnan turvallisuuteen liittyvistä toimista, kuten palomuurien testauksesta, säännöllisestä turvatestauksesta, tarkastuksista ja turva-asioista raportoinnista;

b) valvoo toiminnan jatkuvuussuunnitelman tehokkuutta ja huolehtii säännöllisten harjoitusten toteuttamisesta;

c) turvaa kaikkia SIS II:n keskusjärjestelmän tai viestintäinfrastruktuurin turvallisuuteen mahdollisesti vaikuttavia viestintäinfrastruktuurin tapahtumia koskevan todistusaineiston ja raportoi tapahtumista järjestelmän turvallisuusvastaavalle;

d) ilmoittaa järjestelmän turvallisuusvastaavalle, jos turvapolitiikkaa on muutettava;

e) valvoo, että kaikki viestintäinfrastruktuurin hallinnointiin osallistuvat hankkijat ja alihankkijat noudattavat tätä päätöstä ja turvapolitiikkaa;

f) varmistaa, että henkilöstö on tietoinen velvollisuuksistaan, ja valvoo turvapolitiikan noudattamista;

g) valvoo tietoturvan kehitystä ja varmistaa, että henkilöstö saa asianmukaista koulutusta;

h) hankkii turvapolitiikan laatimisessa, päivittämisessä ja tarkistamisessa tarvittavat tiedot ja valmistelee eri toimintavaihtoehdot 7 artiklan mukaisesti.

5 artikla

Tietoturvaloukkaukset

1. Kaikki tapahtumat, joilla on tai saattaa olla vaikutusta SIS II:n turvallisuuteen ja jotka voivat aiheuttaa vahinkoa SIS II:lle tai johtaa tietojen häviämiseen, katsotaan tietoturvaloukkauksiksi, erityisesti jos tietoihin on mahdollisesti päästy käsiksi tai jos tietojen saatavuus, eheys tai luottamuksellisuus on vaarantunut tai saattanut vaarantua.

2. Tietoturvaloukkauksiin vastataan nopeasti, tehokkaasti ja asianmukaisesti turvapolitiikkaa noudattaen. Laaditaan menettelyt, joita noudatetaan tietoturvaloukkausten jälkeen.

3. Tietoturvaloukkauksesta, jolla on tai saattaa olla vaikutusta SIS II:n toimintaan jäsenvaltiossa tai jäsenvaltion syöttämien tai lähettämien tietojen saatavuuteen, eheyteen tai luottamuksellisuuteen, ilmoitetaan kyseiselle jäsenvaltiolle. Lisäksi tietoturvaloukkauksista ilmoitetaan komission tietosuojavastaavalle.

6 artikla

Tietoturvaloukkausten hallinta

1. Kaikki SIS II:n kehittämiseen, hallinnointiin ja toimintaan osallistuvat henkilöstön jäsenet sekä hankkijat velvoitetaan kirjaamaan muistiin viestintäinfrastruktuurin turvallisuudessa havaitsemansa tai epäilemänsä puutteet ja ilmoittamaan niistä järjestelmän turvallisuusvastaavalle tai viestintäinfrastruktuurin paikalliselle turvallisuusvastaavalle.

2. Kun havaitaan mikä tahansa tapahtuma, jolla on tai saattaa olla vaikutusta SIS II:n turvallisuuteen, viestintäinfrastruktuurin paikallinen turvallisuusvastaava ilmoittaa asiasta mahdollisimman nopeasti järjestelmän turvallisuusvastaavalle ja tarvittaessa SIS II:n turvallisuudesta vastaavalle kansalliselle yhteyspisteelle, jos kyseisessä jäsenvaltiossa on tällainen yhteyspiste, kirjallisesti tai jos asia on erityisen kiireellinen, muita viestintäkanavia käyttäen. Raportissa kuvaillaan kyseinen tietoturvaloukkaus, riskin suuruus, mahdolliset seuraukset ja toimenpiteet, jotka on toteutettu tai olisi toteutettava riskin pienentämiseksi.

3. Viestintäinfrastruktuurin paikallinen turvallisuusvastaava turvaa välittömästi kaiken tietoturvaloukkaukseen liittyvän todistusaineiston. Todistusaineisto toimitetaan järjestelmän turvallisuusvastaavalle tämän pyynnöstä, jos se on sovellettavien tietoturvasäännösten puitteissa mahdollista.

4. Turvapolitiikassa määritellään palauteprosessi sen varmistamiseksi, että tieto turvaloukkauksen laadusta, käsittelystä ja lopputuloksesta toimitetaan järjestelmän turvallisuusvastaavalle ja viestintäinfrastruktuurin paikalliselle turvallisuusvastaavalle heti kun tietoturvaloukkaus on käsitelty loppuun.

5. Edellä olevia 1–4 kohtaa sovelletaan tarvittavin muutoksin SIS II:n keskusjärjestelmää koskeviin tietoturvaloukkauksiin. Sen vuoksi kaikki 1–4 kohdassa olevat viittaukset viestintäinfrastruktuurin paikalliseen turvallisuusvastaavaan on ymmärrettävä viittauksiksi SIS II:n keskusjärjestelmän paikalliseen turvallisuusvastaavaan.

III LUKU

TURVATOIMET

7 artikla

Turvapolitiikka

1. Oikeus-, vapaus- ja turvallisuusasioiden pääosaston pääjohtaja laatii sitovan turvapolitiikan ja päivittää ja tarkistaa sitä säännöllisesti tämän päätöksen mukaisesti. Turvapolitiikassa kuvataan yksityiskohtaisesti menettelyt ja toimet, joilla suojaudutaan viestintäinfrastruktuurin saatavuuteen, eheyteen ja luottamuksellisuuteen kohdistuvilta uhkilta, sekä varasuunnitelmat, jotta voidaan varmistaa riittävä turvallisuuden taso tässä päätöksessä kuvatulla tavalla. Turvapolitiikan on oltava tämän päätöksen mukainen.

2. Turvapolitiikka perustuu riskinarviointiin. Turvapolitiikassa kuvattujen toimien on oltava oikeassa suhteessa havaittuihin riskeihin.

3. Riskinarviointia ja turvapolitiikkaa päivitetään, jos se on tarpeen teknisen kehityksen, havaittujen uusien uhkien tai muiden seikkojen johdosta. Turvapolitiikkaa tarkistetaan joka tapauksessa vuosittain sen varmistamiseksi, että se vastaa edelleen asianmukaisesti viimeisintä riskinarviointia tai mitä tahansa uutta teknistä kehitysaskelta, uhkaa tai muuta keskeistä seikkaa.

4. Turvapolitiikan laatii järjestelmän turvallisuusvastaava yhteistyössä SIS II:n keskusjärjestelmän paikallisen turvallisuusvastaavan ja viestintäinfrastruktuurin paikallisen turvallisuusvastaavan kanssa.

5. Edellä olevia 1–4 kohtaa sovelletaan tarvittavin muutoksin SIS II:n keskusjärjestelmää koskevaan turvapolitiikkaan. Sen vuoksi kaikki 1–4 kohdassa olevat viittaukset viestintäinfrastruktuurin paikalliseen turvallisuusvastaavaan on ymmärrettävä viittauksiksi SIS II:n keskusjärjestelmän paikalliseen turvallisuusvastaavaan.

8 artikla

Turvatoimien täytäntöönpano

1. Tässä päätöksessä ja turvapolitiikassa tarkoitettujen tehtävien ja vaatimusten toteuttaminen, paikallisen turvallisuusvastaavan nimeäminen mukaan luettuna, voidaan ulkoistaa tai antaa tehtäväksi yksityiselle tai julkiselle elimelle.

2. Siinä tapauksessa komissio varmistaa oikeudellisesti sitovan sopimuksen avulla, että tässä päätöksessä ja turvapolitiikassa asetettuja vaatimuksia noudatetaan. Jos paikallisen turvallisuusvastaavan nimeäminen annetaan tehtäväksi jollekin muulle taholle tai ulkoistetaan, komissio varmistaa oikeudellisesti sitovan sopimuksen avulla, että sitä kuullaan paikallisen turvallisuusvastaavan tehtävään nimettävän henkilön valinnasta.

9 artikla

Laitteisiin pääsyn valvonta

1. Alueet, joilla tietojenkäsittelylaitteet sijaitsevat, suojataan asianmukaisilla esteillä ja pääsynvalvontajärjestelyillä, ja niiden ympärille rajataan turva-alueet.

2. Turva-alueen sisälle luodaan suojattuja alueita, joiden tarkoituksena on suojella fyysisiä komponentteja, esimerkiksi laitteistoja, tietovälineitä ja konsoleja, SIS II:ta koskevia suunnitelmia ja muita asiakirjoja sekä SIS II:n toimintaan osallistuvan henkilöstön toimistoja ja työpisteitä. Suojatut alueet varustetaan asianmukaisilla pääsynvalvontajärjestelyillä, jotta vain valtuutetut henkilöt pääsevät alueelle. Suojatuilla alueilla työskentelyyn sovelletaan turvapolitiikassa yksityiskohtaisesti määritettyjä turvallisuussääntöjä.

3. Toimistojen, huoneiden ja laitteiden fyysisestä turvallisuudesta huolehditaan. Esimerkiksi toimitus- ja lastausalueita ja muita alueita, joiden kautta sivulliset voivat päästä tiloihin, valvotaan, ja jos mahdollista, ne eristetään tietojenkäsittelylaitteista luvattoman käytön estämiseksi.

4. Laaditaan suunnitelma turva-alueiden suojaamiseksi fyysisesti luonnonkatastrofeilta ja ihmisen aiheuttamilta katastrofeilta ja sovelletaan sitä oikeassa suhteessa riskeihin.

5. Laitteet suojataan fyysisiltä ja ympäristöuhkilta sekä luvattomalta käytöltä.

6. Komissio lisää 2 artiklan 3 kohdan h alakohdassa tarkoitettuun luetteloon sen yhteyspisteen, joka vastaa tämän artiklan säännösten täytäntöönpanon valvonnasta CS-SIS:n varakeskuksen sijaintipaikassa, edellyttäen että sillä on tämä tieto.

10 artikla

Tietovälineiden ja laitteiden valvonta

1. Tietoja sisältävät erilliset tallennusvälineet suojataan luvattomalta käytöltä, väärinkäytöltä tai tietojen tuhoamiselta, ja välineiden luettavuudesta huolehditaan tietojen koko säilytysajan.

2. Tietovälineet poistetaan käytöstä turvallisesti sen jälkeen kun niitä ei enää tarvita, noudattaen turvapolitiikassa yksityiskohtaisesti kuvattavia menettelyjä.

3. Inventaarien avulla varmistetaan, että tiedot tallennettujen tietojen sijainnista, tietojen säilyttämisajasta ja tietoihin pääsyä koskevista valtuutuksista ovat saatavilla.

4. Kaikki viestintäinfrastruktuurin tärkeimmät osat luetteloidaan, jotta niitä voidaan suojella niiden tärkeysasteen mukaan. Keskeisistä tietoteknisistä laitteista pidetään ajantasaista rekisteriä.

5. Viestintäinfrastruktuuria koskevat ajantasaiset asiakirjat pidetään saatavilla. Asiakirjat on suojattava luvattomalta käytöltä.

6. Edellä olevia 1–5 kohtaa sovelletaan tarvittavin muutoksin SIS II:n keskusjärjestelmään. Sen vuoksi kaikki viittaukset viestintäinfrastruktuuriin on ymmärrettävä viittauksiksi SIS II:n keskusjärjestelmään.

11 artikla

Tietojen säilyttämisen valvonta

1. Tietojen asianmukainen säilyttäminen ja luvattoman käytön ehkäiseminen varmistetaan asianmukaisilla toimenpiteillä.

2. Kaikki tallennusvälineitä sisältävät laitteet tarkistetaan kokonaisuudessaan, jotta voidaan varmistaa, että arkaluonteiset tiedot on poistettu tai niiden päälle on kirjoitettu ennen välineiden käytöstä poistamista, tai laitteet hävitetään turvallisesti.

12 artikla

Salasanojen valvonta

1. Kaikki salasanat säilytetään turvallisesti ja niitä käsitellään luottamuksellisesti. Jos epäillään, että salasana on joutunut ulkopuolisten tietoon, se on vaihdettava välittömästi tai kyseinen käyttäjätili on poistettava käytöstä. Käyttäjätunnukset ovat yksilöllisiä ja ainutkertaisia.

2. Turvapolitiikassa määritellään luvattoman käytön estämiseksi menettelyt, joita noudattaen järjestelmään kirjaudutaan ja sieltä kirjaudutaan ulos.

13 artikla

Pääsyn valvonta

1. Turvapolitiikassa kuvataan henkilöstön rekisteriin ottamista ja rekisteristä poistamista varten virallinen menettely, jota noudattaen myönnetään tai kumotaan pääsy SIS II:n laitteisiin ja ohjelmistoihin toiminnan hallinnointia varten. Riittävien käyttöoikeuksien (salasanat tai muut asianmukaiset keinot) myöntämistä ja käyttöä valvotaan turvapolitiikkaan sisältyvällä virallisella hallinnointimenettelyllä.

2. Pääsy SIS II:n laitteisiin ja ohjelmistoihin CS-SIS:ssä

i) rajataan valtuutettuihin henkilöihin;

ii) rajataan tapauksiin, joissa voidaan todeta asetuksen (EY) N:o 1987/2006 45 artiklan ja päätöksen 2007/533/YOS 61 artiklan tai asetuksen (EY) N:o 1987/2006 50 artiklan 2 kohdan ja päätöksen 2007/533/YOS 66 artiklan 2 kohdan mukainen perusteltu tarkoitus;

iii) ei ylitä pääsyn tarkoituksen kannalta tarpeellista kestoa ja laajuutta; sekä

iv) tapahtuu ainoastaan turvapolitiikassa määriteltävän pääsynvalvontamenettelyn mukaisesti.

3. CS-SIS:ssä käytetään ainoastaan niitä konsoleja ja ohjelmistoja, jotka SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava on hyväksynyt. Sellaisten järjestelmän apuohjelmien käyttöä, joiden avulla on mahdollista ohittaa järjestelmän ja sen sovellusten valvonta, rajoitetaan ja valvotaan. Ohjelmien asennuksen valvontaa varten otetaan käyttöön erityiset menettelyt.

14 artikla

Tiedonsiirron valvonta

Viestintäinfrastruktuuria valvotaan tiedonvaihdon käytettävyyden, eheyden ja luottamuksellisuuden varmistamiseksi. Viestintäinfrastruktuurissa siirrettävät tiedot suojataan salausmenetelmillä.

15 artikla

Tallentamisen valvonta

SIS II:n keskusjärjestelmän paikallinen turvallisuusvastaava seuraa niiden henkilöiden käyttäjätilejä, joilla on oikeus käsitellä SIS II:n ohjelmia CS-SIS:n kautta. Käyttäjätilien käyttö, myös käyttöaika ja käyttäjän henkilöllisyys, kirjataan muistiin.

16 artikla

Kuljetuksen valvonta

1. Turvapolitiikassa vahvistetaan asianmukaiset toimenpiteet, joilla estetään henkilötietojen luvaton lukeminen, jäljentäminen, muuttaminen tai poistaminen siirrettäessä tietoja SIS II:een tai SIS II:sta tai tietovälineiden kuljetuksen aikana. Turvapolitiikassa määrätään hyväksyttävistä lähetys- tai kuljetustavoista sekä vastuumenettelyistä tietovälineiden kuljetusta ja niiden määränpäähän saapumista varten. Tietovälineellä ei saa olla muita tietoja kuin ne, jotka on tarkoitus siirtää järjestelmään.

2. Kolmansien osapuolten tarjoamiin palveluihin, jotka liittyvät tietojenkäsittelylaitteiden käyttämiseen, käsittelyyn, välittämiseen tai hallinnointiin tai tuotteiden tai palvelujen lisäämiseen tietojenkäsittelylaitteisiin, sovelletaan asianmukaisia yhdennettyjä turvatarkastuksia.

17 artikla

Viestintäinfrastruktuurin turvallisuus

1. Viestintäinfrastruktuurin asianmukaisesta hallinnosta ja valvonnasta huolehditaan, jotta sitä voidaan suojella uhkilta ja varmistaa viestintäinfrastruktuurin ja SIS II:n keskusjärjestelmän sekä sen kautta vaihdettavien tietojen turvallisuus.

2. Kaikkien verkkopalvelujen turvaominaisuudet, palvelutasot ja hallinnolliset vaatimukset määritetään palveluntarjoajan kanssa tehtävässä verkkopalvelusopimuksessa.

3. Sen lisäksi, että suojellaan SIS II:n liityntäpisteitä, suojataan myös kaikki muut palvelut, joita viestintäinfrastruktuuri hyödyntää. Asianmukaiset menetelmät määritetään turvapolitiikassa.

18 artikla

Seuranta

1. Lokitiedostot, joissa on asetuksen (EY) N:o 1987/2006 18 artiklan 1 kohdassa ja päätöksen 2007/533/YOS 18 artiklan 1 kohdassa tarkoitetut tiedot kaikesta CS-SIS:n käytöstä ja CS-SIS:ssä tapahtuneesta henkilötietojen vaihdosta, säilytetään luotettavasti CS-SIS:n pääkeskuksen ja varakeskuksen tiloissa, joista on pääsy lokitiedostoihin, asetuksen (EY) N:o 1987/2006 18 artiklan 3 kohdassa ja päätöksen 2007/533/YOS 18 artiklan 3 kohdassa tarkoitettu enimmäisaika.

2. Tietojenkäsittelylaitteiden käytön tai laitteissa esiintyvien vikojen seurantamenettelyt esitetään turvapolitiikassa, ja seurannan tuloksia tarkastellaan säännöllisesti. Tarvittaessa ryhdytään asianmukaisiin toimiin.

3. Tietojen kirjaamisvälineet ja lokitiedostot suojataan väärinkäytöltä ja luvattomalta käytöltä, jotta ne täyttäisivät todisteiden keräämiselle ja säilyttämiselle asetetut vaatimukset.

19 artikla

Salausmenetelmät

Tarvittaessa käytetään salausmenetelmiä tietojen suojaamiseksi. Järjestelmän turvallisuusvastaavan on etukäteen hyväksyttävä salausmenetelmien käyttö sekä käytön perusteet ja edellytykset.

IV LUKU

HENKILÖSTÖTURVALLISUUS

20 artikla

Henkilöstöprofiilit

1. Turvapolitiikassa määritellään niiden henkilöiden tehtävät ja vastuualueet, joilla on oikeus käyttää SIS II:n keskusjärjestelmää.

2. Turvapolitiikassa määritellään niiden henkilöiden tehtävät ja vastuualueet, joilla on oikeus käyttää viestintäinfrastruktuuria.

3. Operatiiviseen hallintoon osallistuvien komission henkilöstön, hankkijoiden ja niiden työntekijöiden turvallisuuteen liittyvät tehtävät ja velvollisuudet määritellään ja dokumentoidaan ja niistä ilmoitetaan henkilöille itselleen. Komission henkilöstön osalta nämä tehtävät ja velvollisuudet mainitaan työnkuvauksessa ja tavoitteissa, ja hankkijoiden osalta ne mainitaan sopimuksissa tai palvelutasosopimuksissa.

4. Kaikkien niiden henkilöiden kanssa, joihin ei sovelleta Euroopan unionin tai jonkin jäsenvaltion julkista hallintoa koskevia sääntöjä, tehdään salassapitosopimus. SIS II:een sisältyvien tietojen parissa työskentelevillä henkilöillä on oltava tarvittava turvallisuusselvitys tai vastaava todistus turvapolitiikassa määriteltävien yksityiskohtaisten menettelyjen mukaisesti.

21 artikla

Henkilöstölle tarkoitettu tiedotus

1. Koko henkilöstölle ja hankkijoille annetaan heidän työtehtäviensä edellyttämä koulutus turvallisuuskysymyksissä, lakisääteisissä vaatimuksissa, toimintaperiaatteissa ja menettelyissä.

2. Työsuhteen tai sopimuksen päättymisen varalta turvapolitiikassa määritellään sekä henkilöstön että hankkijoiden osalta työtehtävän muuttumiseen tai työsuhteen päättymiseen liittyvät velvoitteet ja menettelyt, joita sovelletaan omaisuuden palauttamiseen ja käyttöoikeuksien poistamiseen.

V LUKU

LOPPUSÄÄNNÖS

22 artikla

Soveltaminen

1. Tätä päätöstä aletaan soveltaa päivänä, jonka neuvosto määrää asetuksen (EY) N:o 1987/2006 55 artiklan 2 kohdan ja päätöksen 2007/533/YOS 71 artiklan 2 kohdan mukaisesti.

2. Edellä olevan 1 artiklan 1 kohdan, 2 artiklan 1 kohdan, 2 artiklan 3 kohdan b, d, f ja i alakohdan, 3 artiklan, 6 artiklan 5 kohdan, 7 artiklan 5 kohdan, 9 artiklan 6 kohdan, 10 artiklan 6 kohdan, 13 artiklan 2 ja 3 kohdan, 15 artiklan, 18 artiklan ja 20 artiklan 1 kohdan voimassaolo päättyy, kun tietokantaa hallinnoiva viranomainen ottaa tehtävänsä vastaan.

Tehty Brysselissä 4 päivänä toukokuuta 2010.

Komission puolesta

José Manuel BARROSO

Puheenjohtaja