KOMISSION PÄÄTÖS (EU) 2022/640,

annettu 7 päivänä huhtikuuta 2022,

keskeisten turvallisuusalan toimijoiden rooleja ja vastuita koskevista soveltamissäännöistä

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 249 artiklan,

ottaa huomioon turvallisuudesta komissiossa 13 päivänä maaliskuuta 2015 annetun komission päätöksen (EU, Euratom) 2015/443 ([1]),

ottaa huomioon EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä 13 päivänä maaliskuuta 2015 annetun komission päätöksen (EU, Euratom) 2015/444 ([2]),

sekä katsoo seuraavaa:

(1) Päätöksiä (EU, Euratom) 2015/443 ja (EU, Euratom) 2015/444 sovelletaan kaikkiin komission osastoihin ja kaikissa komission tiloissa.

(2) Päätöstä (EU, Euratom) 2015/444 täydentävät tai tukevat soveltamissäännöt hyväksytään tarvittaessa saman päätöksen 60 artiklan mukaisesti.

(3) Turvatoimien, jotka koskevat EU:n turvallisuusluokiteltujen tietojen suojaamista koko niiden elinkaaren ajan, olisi oltava oikeassa suhteessa erityisesti kyseisten tietojen turvallisuusluokitukseen.

(4) Komission viestintä- ja tietojärjestelmien turvallisuutta koskevat toimenpiteet vahvistetaan komission päätöksessä (EU, Euratom) 2017/46 ([3]) ja erityisesti sen 3 artiklassa (”Periaatteet, jotka koskevat tietotekniikan turvallisuutta komissiossa”) ja 9 artiklassa (”Järjestelmän omistajat”).

(5) Keskeisten turvallisuusalan toimijoiden rooleja ja vastuita koskevien soveltamissääntöjen tarkoituksena on antaa ohjeistusta edellytyksistä ja velvollisuuksista, jotka on kyseisten roolien osalta vahvistettu päätöksissä (EU, Euratom) 2015/443 ja (EU, Euratom) 2015/444.

(6) Päätöksen (EU, Euratom) 2015/444 36 artiklan 7 kohdassa esitetään useita komission turvallisuusviranomaiselle kuuluvia, turvallisuuteen liittyviä lisätehtäviä. Näistä tehtävistä säädetään tarkemmin tässä päätöksessä.

(7) Paikallisilla turvavastaavilla ja rekisterin valvontavastaavilla on päätöksen (EU, Euratom) 2015/444 mukaisesti erityinen vastuu EU:n turvallisuusluokiteltujen tietojen suojaamisesta omassa osastossaan.

(8) Komissio antoi 4 päivänä toukokuuta 2016 päätöksen ([4]), jolla turvallisuusasioista vastaavalle komission jäsenelle annetaan valtuudet hyväksyä komission puolesta ja sen vastuulla komission päätöksen (EU, Euratom) 2015/444 60 artiklassa tarkoitetut soveltamissäännöt. Turvallisuusasioista vastaava komission jäsen hyväksyi 13 päivänä huhtikuuta 2021 komission puolesta ja sen vastuulla päätöksen ([5]), jossa soveltamissääntöjä koskevat valtuudet siirretään edelleen henkilöstöhallinnon ja turvallisuustoiminnan pääosaston pääjohtajalle,

([1]) EUVL L 72, 17.3.2015, s. 41.
([2]) EUVL L 72, 17.3.2015, s. 53.
([3]) Komission päätös (EU, Euratom) 2017/46, annettu 10 päivänä tammikuuta 2017, viestintä- ja tietojärjestelmien turvallisuudesta Euroopan komissiossa (EUVL L 6, 11.1.2017, s. 40).
([4]) Päätös C(2016) 2797 final, annettu 4 päivänä toukokuuta 2016, turvallisuuteen liittyvästä valtuutuksesta.
([5]) Decision C(2021) 2684 final of 13 April 2021 granting a subdelegation of powers granted in Commission Decision C(2016)2797 on an empowerment relating to security (päätöstä ei ole julkaistu suomeksi).

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 LUKU

Yleiset säännökset

1 artikla

Kohde ja soveltamisala

1. Tässä päätöksessä vahvistetaan niiden keskeisten turvallisuusalan toimijoiden roolit ja vastuut, jotka vastaavat EU:n turvallisuusluokiteltujen tietojen suojaamisesta komissiossa päätösten (EU, Euratom) 2015/443 ja (EU, Euratom) 2015/444 mukaisesti.

2. Tätä päätöstä sovelletaan kaikkiin komission osastoihin ja kaikissa komission tiloissa.

2 LUKU

Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto

2 artikla

Komission turvallisuusviranomainen

1. Turvallisuudesta vastaavan linjan johtaja henkilöstöhallinnon ja turvallisuustoiminnan pääosastossa toimii päätöksen (EU, Euratom) 2015/444 7 artiklassa tarkoitettuna komission turvallisuusviranomaisena.

2. Komission turvallisuusviranomainen hoitaa tehtäviään seuraavilla aloilla, joista säädetään päätöksessä (EU, Euratom) 2015/444, tämän päätöksen 3–7 artiklan mukaisesti:

a) henkilöstöturvallisuus;

b) fyysinen turvallisuus;

c) EU:n turvallisuusluokiteltujen tietojen hallinnointi;

d) EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien hyväksyntä;

e) yhteisöturvallisuus; sekä

f) turvallisuusluokiteltujen tietojen vaihto.

3. Komission turvallisuusviranomainen tarjoaa paikallisille turvavastaaville, näiden varavastaaville, rekisterin valvontavastaaville ja näiden varavastaaville pakollista koulutusta näiden vastuista ja tehtävistä.

3 artikla

Tiedonturvaamisviranomainen

Tiedonturvaamisviranomainen on vastuussa seuraavista EU:n turvallisuusluokiteltujen tietojen suojaamiseen liittyvistä toimista:

a) tietojen turvaamista koskevien turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen laatiminen sekä niiden toimivuuden ja asianmukaisuuden valvominen;

b) salaustuotteisiin liittyvien teknisten tietojen tallessa pitäminen ja hallinnointi;

c) sen varmistaminen, että tiedonturvaamistoimenpiteet ovat soveltuvin osin komission turvallisuus- ja hankintapolitiikkojen mukaisia;

d) sen varmistaminen, että salaustuotteiden valinnassa noudatetaan niiden kelpoisuutta ja valintaa koskevia periaatteita;

e) järjestelmän omistajien, järjestelmän tarjoajien, turvallisuusalan toimijoiden ja käyttäjien edustajien kuuleminen tietojen turvaamista koskevista turvallisuusperiaatteista ja turvallisuutta koskevista suuntaviivoista.

4 artikla

Turvallisuusjärjestelyjen hyväksyntäviranomainen

1. Komission turvallisuusviranomainen vastaa päätöksen (EU) 2015/444 18 artiklan vaatimukset täyttävien turva-alueiden sekä EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien hyväksymisestä.

2. Tapauksen mukaan komission osastot kuulevat yhdessä paikallisen turvavastaavansa ja paikallistietojärjestelmien tietoturvavastaavansa kanssa turvallisuusjärjestelyjen hyväksyntäviranomaista aina, kun osasto aikoo

a) perustaa turva-alueen;

b) ottaa käyttöön viestintä- ja tietojärjestelmän EU:n turvallisuusluokiteltujen tietojen käsittelyä varten;

c) asentaa muita laitteita turvallisuusluokiteltujen tietojen käsittelyä varten, mukaan lukien yhteydet kolmannen osapuolen viestintä- ja tietojärjestelmään.

Turvallisuusjärjestelyjen hyväksyntäviranomainen antaa neuvoja näiden toimien osalta sekä suunnittelun että rakennus- tai kehittämisprosessien aikana.

3. EU:n turvallisuusluokiteltuja tietoja ei saa käsitellä turva-alueella eikä viestintä- ja tietojärjestelmässä ennen kuin turvallisuusjärjestelyjen hyväksyntäviranomainen on antanut hyväksynnän asianmukaisessa EU:n turvallisuusluokiteltujen tietojen turvallisuusluokassa.

4. Turva-alueen hyväksyntää koskeviin vaatimuksiin on sisällyttävä

a) turva-aluetta koskevien suunnitelmien hyväksyminen;

b) ulkopuolisten toimeksisaajien työsuorituksia koskevien sopimusten hyväksyminen ottaen huomioon yhteisöturvallisuutta koskevat säännökset, kuten toimeksisaajien ja niiden henkilöstön turvallisuusselvityksiä koskevat vaatimukset;

c) kaikkien vaadittujen vaatimustenmukaisuusvakuutusten ja -todistusten saatavuus;

d) turva-alueen fyysinen tarkastus sen todentamiseksi, että rakennusmateriaalit ja -menetelmät, pääsynvalvonta, turvalaitteet ja mahdolliset muut osatekijät ovat komission turvallisuusviranomaisen vahvistamien vaatimusten mukaisia;

e) sähkömagneettista säteilyä koskevien vastatoimien vahvistaminen mitä tahansa teknisesti suojattua turva-aluetta varten;

f) turva-alueen turvallisuusmenettelyjen hyväksyminen.

5. EU:n turvallisuusluokiteltuja tietoja käsittelevän viestintä- ja tietojärjestelmän hyväksyntää koskeviin vaatimuksiin on sisällyttävä

a) järjestelmän hyväksymisstrategian laatiminen;

b) viestintä- ja tietojärjestelmän turvallisuussuunnitelman vahvistaminen riskinhallintaan perustuvan lähestymistavan pohjalta;

c) viestintä- ja tietojärjestelmän turvallisuusmenettelyjen vahvistaminen;

d) kaikkien muiden vaadittujen turvallisuusasiakirjojen vahvistaminen sellaisina kuin turvallisuusjärjestelyjen hyväksyntäviranomainen on ne määrittänyt;

e) salausteknologioiden käytön hyväksyminen;

f) sähkömagneettista säteilyä koskevien vastatoimien vahvistaminen CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuja tietoja käsittelevää viestintä- ja tietojärjestelmää varten;

g) viestintä- ja tietojärjestelmän tarkastus sen varmistamiseksi, että dokumentoidut turvatoimet on toteutettu asianmukaisesti.

6. Sen jälkeen kun hyväksyntää koskevat vaatimukset on täytetty, turvallisuusjärjestelyjen hyväksyntäviranomainen antaa virallisen valtuutuksen EU:n turvallisuusluokiteltujen tietojen käsittelyyn turva-alueella tai viestintä- ja tietojärjestelmässä ilmoitettuun EU:n turvallisuusluokiteltujen tietojen enimmäistasoon asti ja enintään viideksi vuodeksi riippuen käsiteltävien EU:n turvallisuusluokiteltujen tietojen turvallisuusluokista ja käsittelyyn liittyvistä riskeistä.

7. Jos turvallisuusjärjestelyjen hyväksyntäviranomainen saa ilmoituksen tietoturvaloukkauksesta tai huomattavasta muutoksesta turva-alueen tai viestintä- ja tietojärjestelmän suunnittelussa tai turvatoimissa, se tarkastelee uudelleen EU:n turvallisuusluokiteltujen tietojen käsittelyä varten myönnettyä valtuutusta ja voi tarvittaessa peruuttaa sen, kunnes havaitut ongelmat on ratkaistu.

5 artikla

TEMPEST-viranomainen

1. CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien suojaamiseksi on toteutettava TEMPEST-turvatoimia, ja näitä toimia voidaan toteuttaa myös RESTREINT UE/EU RESTRICTED -tasolle luokiteltujen tietojen tapauksessa.

2. TEMPEST-viranomainen vastaa niiden toimenpiteiden hyväksymisestä, joilla estetään EU:n turvallisuusluokiteltujen tietojen vaarantuminen tahattoman sähkömagneettisen säteilyn takia.

3. TEMPEST-viranomainen määrittää EU:n turvallisuusluokiteltuja tietoja käsittelevän viestintä- ja tietojärjestelmän omistajan pyynnöstä eritelmät, jotka koskevat tietojen turvallisuusluokan kannalta asianmukaisia TEMPEST-turvatoimia.

4. TEMPEST-viranomainen suorittaa turva-alueiden ja CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuja EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien hyväksynnän aikana teknistä testausta ja antaa onnistuneiden testien jälkeen TEMPEST-todistuksen.

5. TEMPEST-todistuksen on sisällettävä vähintään seuraavat:

a) testauspäivä;

b) TEMPEST-turvatoimien kuvaus ja tilojen suunnitelmat;

c) todistuksen viimeinen voimassaolopäivä;

d) mahdolliset muutokset, joiden seurauksena todistus mitätöidään;

e) TEMPEST-viranomaisen allekirjoitus.

6. Paikallinen turvavastaava tai luottamuksellisen kokouksen järjestämisestä vastaava taho voi yhteistyössä paikallisen turvavastaavan kanssa pyytää TEMPEST-viranomaista suorittamaan kokoustiloissa testausta sen varmistamiseksi, että tilat ovat teknisesti suojattuja.

6 artikla

Salauslaitteiden hyväksyntäviranomainen

1. Salauslaitteiden hyväksyntäviranomainen on vastuussa salausteknologioiden käytön hyväksymisestä.

2. Salauslaitteiden hyväksyntäviranomainen antaa ohjeita salausteknologioiden käyttöä ja hyväksymistä varten.

3. Salauslaitteiden hyväksyntäviranomainen hyväksyy salausratkaisujen käytön järjestelmän omistajan pyynnöstä. Hyväksynnän on perustuttava vähintään seuraavien seikkojen tyydyttävään arviointiin:

a) suojattavan tiedon turvallisuutta koskevat tarpeet;

b) yleiskuva ratkaisuun osallistuvasta viestintä- ja tietojärjestelmästä;

c) arvio toiminnan luonteesta johtuvista ja jäännösriskeistä;

d) ehdotetun ratkaisun kuvaus;

e) salausratkaisun turvallisuusmenettelyt.

4. Salauslaitteiden hyväksyntäviranomainen pitää kirjaa hyväksytyistä salausratkaisuista.

7 artikla

Salatun aineiston jakelusta vastaava viranomainen

1. Salatun aineiston jakelusta vastaava viranomainen vastaa EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytettävän salausaineiston (lähinnä salauslaitteet, salausavaimet, varmenteet ja niihin liittyvät todennussovellukset) jakelusta seuraaville:

a) komissiossa olevat käyttäjät tai komission osastot, kun on kyse ulkopuolisten tahojen hallinnoimista viestintä- ja tietojärjestelmistä;

b) komission ulkopuolella olevat käyttäjät tai organisaatiot, kun on kyse komission hallinnoimista viestintä- ja tietojärjestelmistä.

2. Salatun aineiston jakelusta vastaava viranomainen voi päätöksen (EU) 2015/443 17 artiklan 3 kohdan mukaisesti antaa muille osastoille tehtäväksi huolehtia salausaineiston jakelusta kolmansille osapuolille.

3. Salatun aineiston jakelusta vastaava viranomainen varmistaa, että kaikki salausaineisto lähetetään suojatuissa kanavissa, jotka suojaavat aineistoa luvattomalta käsittelyltä ja havaitsevat mahdollisen luvattoman käsittelyn, niiden EU:n turvallisuusluokiteltujen tietojen turvallisuusluokkaa koskevien turvallisuussääntöjen mukaisesti, joita kyseisellä salausaineistolla on tarkoitus suojata.

4. Salatun aineiston jakelusta vastaava viranomainen antaa ohjeita paikalliselle turvavastaavalle ja tapauksen mukaan paikallistietojärjestelmien tietoturvavastaavalle jokaisessa komission osastossa, joka osallistuu salausaineiston tuotantoon, jakeluun tai käyttöön.

5. Salatun aineiston jakelusta vastaava viranomainen varmistaa, että jakeluprosessia varten luodaan asianmukaiset turvallisuusmenettelyt.

3 LUKU

Komission osastot

8 artikla

Osastopäälliköt

1. Kukin osastopäällikkö nimittää

a) paikallisen turvavastaavan ja tarvittaessa yhden tai useamman varavastaavan kyseistä osastoa tai kabinettia varten;

b) rekisterin valvontavastaavan ja tarvittaessa yhden tai useamman varavastaavan kutakin sellaista osastoa varten, joka ylläpitää EU:n turvallisuusluokiteltujen tietojen rekisteriä;

c) järjestelmän omistajan kutakin EU:n turvallisuusluokiteltuja tietoja käsittelevää viestintä- ja tietojärjestelmää varten.

2. Osastopäällikkö pyytää henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuudesta vastaavan linjan johtajalta hyväksyntää ennen paikallisten turvavastaavien, rekisterin valvontavastaavien ja näiden varavastaavien nimittämistä.

3. Osastopäällikkö määrittää yhteistyössä paikallisen turvavastaavan kanssa kaikki virat/toimet, joissa edellytetään turvallisuusselvitystä EU:n turvallisuusluokiteltuihin tietoihin pääsyä varten. Näihin virkoihin/toimiin hakeville ilmoitetaan turvallisuusselvitystä koskevasta vaatimuksesta palvelukseenottomenettelyn aikana.

4. EU:n turvallisuusluokiteltuja tietoja hallussaan pitävän osaston päällikön vastuulla on tarvittaessa aktivoida suunnitelmat, jotka koskevat tietojen hävittämistä ja evakuointia hätätapauksissa. Suunnitelmiin on sisällyttävä vaihtoehto sellaisia tilanteita varten, joissa osastopäällikköön ei saada yhteyttä.

9 artikla

EU:n turvallisuusluokiteltuja tietoja käsittelevien viestintä- ja tietojärjestelmien omistajat

1. Järjestelmän omistajan on otettava yhteyttä turvallisuusjärjestelyjen hyväksyntäviranomaiseen mahdollisimman pian, kun on kyse hankkeesta, jonka tarkoituksena on ottaa käyttöön EU:n turvallisuusluokiteltuja tietoja käsittelevä viestintä- ja tietojärjestelmä, jotta voidaan määrittää asianmukaiset turvallisuutta koskevat standardit ja vaatimukset ja käynnistää turvallisuusjärjestelyjen hyväksyntäprosessi.

2. Järjestelmän omistajan on varmistettava, että turvatoimet täyttävät turvallisuusjärjestelyjen hyväksyntäviranomaisen vaatimukset ja että viestintä- ja tietojärjestelmässä ei käsitellä EU:n turvallisuusluokiteltuja tietoja ennen kuin järjestelmälle on annettu hyväksyntä.

3. Järjestelmän omistajan on otettava yhteyttä salauslaitteiden hyväksyntäviranomaiseen saadakseen hyväksynnän mahdollisen salausteknologian käytölle. Järjestelmän omistajat eivät saa käyttää salausteknologiaa tuotantojärjestelmissä ilman ennakkohyväksyntää.

4. Järjestelmän omistajan on kuultava osaston paikallistietojärjestelmien tietoturvavastaavaa viestintä- ja tietojärjestelmien turvallisuuteen liittyvissä asioissa.

5. Järjestelmän omistajan on tarkasteltava uudelleen järjestelmään sovellettavia turvatoimia, mukaan lukien turvallisuussuunnitelmaa, vähintään kerran vuodessa.

6. Jos viestintä- ja tietojärjestelmässä ilmenee turvallisuushäiriö, joka osoittaa, että viestintä- ja tietojärjestelmä ei kykene enää suojelemaan asianmukaisesti EU:n turvallisuusluokiteltuja tietoja, järjestelmän omistajan on ilmoitettava asiasta paikalliselle turvavastaavalle ja otettava välittömästi yhteyttä turvallisuusjärjestelyjen hyväksyntäviranomaiseen saadakseen neuvoja siitä, miten asiassa olisi toimittava. Tällöin hyväksyntä voidaan keskeyttää ja järjestelmä voidaan poistaa käytöstä, kunnes on toteutettu asianmukaiset korjaavat toimenpiteet.

7. Järjestelmän omistajan on tuettava aina ja kaikin keinoin turvallisuusjärjestelyjen hyväksyntäviranomaista tämän hoitaessa viestintä- ja tietojärjestelmän hyväksyntään liittyviä tehtäviä.

10 artikla

Operatiivinen tiedonturvaamisviranomainen

Operatiivinen tiedonturvaamisviranomainen hoitaa jokaisen viestintä- ja tietojärjestelmän osalta seuraavia tehtäviä:

a) turvallisuusasiakirjojen ja erityisesti turvallisuussuunnitelman, järjestelmään liittyvien turvallisuusmenettelyjen ja viestintä- ja tietojärjestelmän hyväksymisprosessiin kuuluvien salausasiakirjojen laatiminen turvallisuusperiaatteiden ja turvallisuutta koskevien suuntaviivojen mukaisesti;

b) osallistuminen järjestelmäkohtaisten teknisten turvatoimien, laitteiden ja ohjelmistojen valintaan ja testaamiseen niiden käyttöönoton valvomiseksi ja sen varmistamiseksi, että ne on asennettu ja konfiguroitu turvallisesti ja että niitä ylläpidetään asiaankuuluvien turvallisuusasiakirjojen mukaisesti;

c) osallistuminen TEMPEST-turvatoimien ja -laitteiden valintaan, jos sitä edellytetään turvallisuussuunnitelmassa, ja laitteiden turvallisen asennuksen ja ylläpidon varmistaminen yhteistyössä TEMPEST-viranomaisen kanssa;

d) järjestelmän toimintaan liittyvien turvallisuusmenettelyjen käyttöönoton ja soveltamisen seuranta;

e) salaustuotteiden hallinnointi ja käsittely yhteistyössä salatun aineiston jakelusta vastaavan viranomaisen kanssa salausaineiston ja valvottujen esineiden asianmukaisen hallussapidon ja tarvittaessa salauksessa käytettävien muuttujien generoinnin varmistamiseksi;

f) turvallisuusanalyysien, tarkistusten ja testien suorittaminen erityisesti turvallisuusjärjestelyjen hyväksyntäviranomaisen vaatimien asiaankuuluvien riskiraporttien laatimiseksi;

g) viestintä- ja tietojärjestelmäkohtaisen tiedonturvaamiskoulutuksen tarjoaminen;

h) viestintä- ja tietojärjestelmäkohtaisten turvatoimien täytäntöönpano ja toteutus.

4 LUKU

Paikallinen turvavastaava

11 artikla

Paikallisen turvavastaavan nimittäminen

1. Paikallisen turvavastaavan ja varavastaavien on oltava virkamiehiä tai väliaikaisia toimihenkilöitä.

2. Kaikilla paikallisilla turvavastaavilla ja varavastaavilla on oltava voimassa oleva turvallisuusvaltuutus EU:n turvallisuusluokiteltuihin tietoihin pääsemiseksi SECRET UE/EU SECRET -turvallisuusluokkaan ja tarvittaessa TRES SECRET UE/EU TOP SECRET -turvallisuusluokkaan asti. Paikallisen turvavastaavan tai varavastaavan on hankittava turvallisuusvaltuutus ennen nimittämistään.

3. Komission edustustot voivat pyytää komission turvallisuusviranomaista myöntämään poikkeuksen 1 ja 2 kohdassa säädetyistä vaatimuksista.

12 artikla

Turva-alueiden turvallisuusmenettelyt

1. Asianomaisen komission osaston paikallinen turvavastaava vahvistaa turvallisuusmenettelyt kutakin vastuullaan olevaa turva-aluetta varten.

2. Paikallisen turvavastaavan on varmistettava, että turvallisuusmenettelyihin kuuluvat seuraavat vaatimukset:

a) ainoastaan sellaiset henkilöstön jäsenet, joilla on voimassa oleva turvallisuusvaltuutus ja todettu tarve päästä käsiksi CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuihin asiakirjoihin, pääsevät turva-alueelle ilman saattajaa virka-aikana;

b) turva-alueelle pääsevät virka-ajan ulkopuolella ilman saattajaa ainoastaan osaston paikallinen turvavastaava, turva-alueen rekisterin valvontavastaava(t), näiden varavastaavat sekä henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuudesta vastaavan linjan valtuutettu henkilöstö;

c) tallennus- ja viestintälaitteita, kuten matkapuhelimia, tietokoneita, kameroita tai muita älylaitteita, ei saa viedä turva-alueelle ilman komission turvallisuusviranomaisen ennakkohyväksyntää; poikkeuslupaa on pyydettävä komission turvallisuusviranomaiselta etukäteen; paikallinen turvavastaava toimii yhteyspisteenä;

d) kaikilla sisäisen tai ulkopuolisen henkilöstön jäsenillä, joiden on päästävä turva-alueelle mutta jotka eivät täytä edellä a alakohdassa vahvistettuja kriteerejä, on oltava koko ajan mukanaan asianmukaisesti valtuutettu henkilöstön jäsen, joka valvoo heitä; kaikki tällainen pääsy turva-alueelle on kirjattava lokikirjaan, jota säilytetään turva-alueen sisäänkäynnin luona;

e) paikallinen turvavastaava varmistaa, että turva-aluetta valvovat tunkeutumisenhavaitsemisjärjestelmät toimivat asianmukaisesti kaikkina aikoina, ja hallinnoi kaikkia niihin liittyviä salasanoja, avaimia, tunnuslukuja tai muita pääsy- ja todentamismekanismeja;

f) turva-alueella tapahtuvista hälytyksistä on ilmoitettava henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuudesta vastaavalle linjalle, joka ilmoittaa asiasta välittömästi paikalliselle turvavastaavalle;

g) sen osaston paikallisen turvavastaavan, jossa turva-alue sijaitsee, on pidettävä kirjaa kaikista toimenpiteistä, jotka toteutetaan hälytyksen tai turvallisuushäiriön johdosta;

h) käytössä on oltava menettelyt turva-alueella tapahtuvan hälytyksen tai muun hätätilanteen varalta, mukaan lukien henkilöstön evakuointi ja komission turvallisuusviranomaisen valvonnassa toimivan kriisiryhmän ja tarvittaessa ulkoisten pelastuspalvelujen nopean toiminnan varmistaminen;

i) paikallisen turvavastaavan on raportoitava kaikista turva-alueen sisällä tapahtuvista tai turva-aluetta koskevista tietoturvaloukkauksista välittömästi komission turvallisuusviranomaiselle asianmukaisten toimenpiteiden määrittämiseksi;

j) turva-alueella olevat toimistot, huoneet ja kassakaapit on pidettävä lukittuina aina kun ne ovat ilman valvontaa;

k) henkilöstön on vältettävä keskustelemasta turvallisuusluokitelluista tiedoista käytävillä tai muissa turva-alueen yhteistiloissa silloin, kun lähettyvillä on muuta kuin valtuutettua henkilöstöä.

13 artikla

Avaimet ja numeroyhdistelmät

1. Paikallinen turvavastaava on yleisesti vastuussa turva-alueilla käytettävien tai turva-alueille pääsyn antavien avainten ja numeroyhdistelmien asianmukaisen käsittelyn ja säilytyksen varmistamisesta. Avaimia ja numeroyhdistelmiä on säilytettävä turvakaapissa, ja niitä on suojattava vähintään samantasoisesti kuin aineistoa, johon ne antavat pääsyn.

2. Paikallisen turvavastaavan on pidettävä kirjaa turvakaapeista ja kassaholveista sekä päivitettyä luetteloa kaikista henkilöstön jäsenistä, joilla on niihin pääsy ilman saattajaa.

3. Paikallisen turvavastaavan on pidettävä kirjaa turvakaappien ja kassaholvien avaimista, myös henkilöstön jäsenistä, joille avaimia on jaettu. Jokaisesta henkilöstön jäsenelle annettavasta avaimesta on oltava kuitti, josta käyvät ilmi muun muassa avaimen tunnistetiedot, vastaanottaja, päivämäärä ja kellonaika.

4. Avaimia ja numeroyhdistelmiä annetaan vain sellaisille henkilöstön jäsenille, joilla on tiedonsaantitarve ja asianmukainen valtuutus päästä EU:n turvallisuusluokiteltuihin tietoihin. Paikallisen turvavastaavan on pyydettävä avain takaisin, jos nämä edellytykset eivät enää täyty.

5. Paikallisen turvavastaavan on säilytettävä vara-avaimia ja kunkin numeroyhdistelmän kirjallista tositetta erillisissä sinetöidyissä, läpinäkymättömissä, allekirjoitetuissa ja päivätyissä kirjekuorissa, jotka avaimista vastaava henkilöstön jäsen antaa paikalliselle turvavastaavalle. Kirjekuoria on säilytettävä turvakaapissa, joka on luokiteltu säilytettävän aineiston korkeimman turvallisuusluokan mukaan, tai kassaholvissa.

6. Jos jossakin kirjekuoressa havaitaan numeroyhdistelmän tai avainten vaihdon yhteydessä merkkejä kajoamisesta tai vahingoittumisesta, paikallisen turvavastaavan on pidettävä tätä turvallisuushäiriönä ja ilmoitettava asiasta välittömästi komission turvallisuusviranomaiselle.

7. Muutokset turva-alueella olevien turvakaappien numeroyhdistelmiin on tehtävä paikallisen turvavastaavan valvonnassa. Numeroyhdistelmät on vaihdettava vähintään 12 kuukauden välein ja aina kun

a) saadaan uusi turvakaappi tai asennetaan uusi lukko (erityisesti tehtaalla asetetut numeroyhdistelmät on vaihdettava välittömästi);

b) tiedot ovat vaarantuneet tai niiden epäillään vaarantuneen;

c) numeroyhdistelmää hallussaan pitävällä henkilöllä ei enää ole tarvetta pääsyyn.

8. Paikallisen turvavastaavan on pidettävä kirjaa päivämääristä, joina 7 kohdassa tarkoitetut numeroyhdistelmien muutokset on tehty.

14 artikla

Suunnitelmat EU:n turvallisuusluokiteltujen tietojen evakuointia ja hävittämistä varten hätätapauksissa

1. Paikallinen turvavastaava auttaa osastopäällikköä laatimaan suunnitelmat, jotka koskevat EU:n turvallisuusluokiteltujen tietojen evakuointia ja hävittämistä hätätapauksissa, henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuudesta vastaavan linjan antamien ohjeiden perusteella.

2. Paikallinen turvavastaava varmistaa, että 1 kohdassa tarkoitettujen suunnitelmien toteuttamiseen tarvittavat laitteet ovat heti käytettävissä ja toimintakunnossa.

3. Paikallinen turvavastaava tarkistaa 1 kohdassa tarkoitetuissa suunnitelmissa nimettyjen virkamiesten kanssa suunnitelmien valmiustason vähintään 12 kuukauden välein ja toteuttaa tarvittaessa toimenpiteitä niiden saattamiseksi ajan tasalle.

15 artikla

Turvallisuusvaltuutukset

1. Paikallinen turvavastaava pitää kirjaa kaikista osastossa olevista viroista/toimista, joissa tarvitaan komission turvallisuusvaltuutusta, sekä näissä viroissa/toimissa olevasta henkilöstöstä. Turvallisuusvaltuutusta koskeva vaatimus on mainittava avoinna olevaa virkaa/toimea koskevassa ilmoituksessa palvelukseenottomenettelyn aikana, ja siitä on ilmoitettava hakijalle haastattelun aikana.

2. Paikallisen turvavastaavan on valvottava kaikkia pyyntöjä, jotka koskevat turvallisuusvaltuutuksen saamista EU:n turvallisuusluokiteltuihin tietoihin pääsemiseksi. Paikallinen turvavastaava toimii osastossa yhteyspisteenä ja on yhteydessä komission turvallisuusviranomaiseen turvallisuusvaltuutusten osalta.

3. Paikallinen turvavastaava esittää pyynnön turvallisuusvaltuutusmenettelyn käynnistämiseksi tietyn henkilöstön jäsenen osalta ja varmistaa, että henkilöstön jäsen palauttaa kansallisen turvallisuusselvityslomakkeen viipymättä komission turvallisuusviranomaiselle.

4. Paikallinen turvavastaava varmistaa, että osaston turvallisuusselvitetyt henkilöstön jäsenet osallistuvat EU:n turvallisuusluokiteltuja tietoja koskevaan pakolliseen tiedotustilaisuuteen saadakseen turvallisuusvaltuutuksen.

5. Paikallinen turvavastaava on säännöllisesti yhteydessä osaston henkilöstöhallinnon yksikköön kaikista muutoksista turvallisuusvaltuutusta edellyttävissä viroissa/toimissa, ja hänen on ilmoitettava tällaisista muutoksista välittömästi komission turvallisuusviranomaiselle.

6. Paikallisen turvavastaavan on ilmoitettava komission turvallisuusviranomaiselle uusista henkilöstön jäsenistä, joilla on jo turvallisuusselvitys ja jotka aloittavat turvallisuusvaltuutusta edellyttävässä virassa/toimessa.

7. Paikallisen turvavastaavan on varmistettava, että osaston henkilöstön jäsenet saattavat turvallisuusselvityksen uusimismenettelyn päätökseen vaaditussa määräajassa. Henkilöstön jäsenen, joka kieltäytyy saattamasta menettelyä päätökseen, on siirryttävä virkaan/toimeen, jossa ei edellytetä turvallisuusvaltuutusta.

16 artikla

EU:n turvallisuusluokiteltujen tietojen rekisteri

1. Jos osastossa on EU:n turvallisuusluokiteltujen tietojen rekisteri, paikallinen turvavastaava valvoo rekisterin valvontavastaavien toimintaa siltä osin kuin on kyse EU:n turvallisuusluokiteltujen tietojen käsittelystä ja kyseisten tietojen suojaamista koskevien turvallisuussääntöjen noudattamisesta.

2. Paikallisen turvavastaavan on suoritettava seuraavat tarkastukset vähintään 12 kuukauden välein ja aina, kun rekisterin valvontavastaava tai varavastaava vaihtuu:

a) EU:n turvallisuusluokiteltujen tietojen rekisterissä olevien asiakirjojen otosta koskeva tarkastus, jonka tarkoituksena on varmistaa asiakirjojen status ja turvallisuusluokiteltujen asiakirjojen rekisterin oikeellisuus;

b) EU:n turvallisuusluokiteltujen tietojen rekisteriin ja rekisteristä lähetettyjä EU:n turvallisuusluokiteltuja tietoja koskevien tositteiden ja lähetystodistusten otoksen tarkastus;

c) hävittämistodistusten otosta koskeva tarkastus.

3. Paikallinen turvavastaava tekee vähintään kuukausittain satunnaistarkastuksia turvallisuusluokiteltujen asiakirjojen rekisteriin ja hiljattain saapuneisiin turvallisuusluokiteltuihin asiakirjoihin varmistaakseen, että asiakirjat on viety rekisteriin asianmukaisesti.

4. Kaikki tarkastukset on kirjattava turvallisuusluokiteltujen asiakirjojen rekisteriä koskevaan lokiin.

17 artikla

Muut turvallisuuteen liittyvät vastuut

Paikallisen turvavastaavan muut turvallisuuteen liittyvät vastuut esitetään turvallisuusohjeessa, joka kattaa erityisesti henkilöiden, tilojen ja muun omaisuuden fyysisen turvallisuuden sekä tietoturvan.

5 LUKU

Rekisterin valvontavastaava

18 artikla

Rekisterin valvontavastaavan nimittäminen

1. Rekisterin valvontavastaavan ja varavastaavien on oltava virkamiehiä tai väliaikaisia toimihenkilöitä.

2. Kaikilla rekisterin valvontavastaavilla ja varavastaavilla on oltava voimassa oleva turvallisuusvaltuutus EU:n turvallisuusluokiteltuihin tietoihin pääsemiseksi SECRET UE/EU SECRET -turvallisuusluokkaan ja tarvittaessa TRES SECRET UE/EU TOP SECRET -turvallisuusluokkaan asti. Rekisterin valvontavastaavan tai varavastaavan on hankittava turvallisuusvaltuutus ennen nimittämistään.

3. Komission edustustot voivat pyytää komission turvallisuusviranomaista myöntämään poikkeuksen 1 ja 2 kohdassa säädetyistä vaatimuksista.

19 artikla

Vastuut

1. Rekisterin valvontavastaava kirjaa CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokitellut tiedot rekisteriin turvallisuussyistä silloin kun

a) ne saapuvat komission osastoon tai lähtevät sieltä; tai

b) ne saapuvat viestintä- ja tietojärjestelmään tai lähtevät sieltä.

2. Rekisterin valvontavastaavat kirjaavat kaikki tapahtumat CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltujen tietojen elinkaaressa. Rekisterin valvontavastaavien on myös varmistettava, että kaikista kolmansien maiden ja kansainvälisten järjestöjen kanssa vaihdettavista RESTREINT UE/EU RESTRICTED -tasolle luokitelluista tai vastaavista tiedoista pidetään kirjaa. Tämä on toteutettava yhteistyössä pääsihteeristön hallinnoiman EU:n turvallisuusluokiteltujen tietojen rekisterin kanssa.

3. Rekisterin valvontavastaavan on kirjattava CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokitellut asiakirjat turvallisuusluokiteltujen asiakirjojen rekisteriin ja varmistettava, että ne tallennetaan suojatusti EU:n turvallisuusluokiteltujen tietojen rekisteriin.

4. Rekisterin valvontavastaavan on autettava komission henkilöstöä CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltujen tietojen luomisessa ja lähettämisessä.

5. Kun CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalle tasolle luokiteltuja asiakirjoja saadaan muilta osastoilta tai ulkopuolisilta tahoilta, rekisterin valvontavastaavan on varmistettava, että tietojen lähettäjälle toimitetaan asianmukaisesti toimitustodistus.

6. Ennen kun henkilöstön jäsenelle annetaan pääsy EU:n turvallisuusluokiteltujen tietojen rekisterissä olevaan turvallisuusluokiteltuun asiakirjaan, rekisterin valvontavastaavan on varmistettava paikalliselta turvavastaavalta, että komission turvallisuusviranomainen on antanut kyseiselle henkilöstön jäsenelle turvallisuusvaltuutuksen.

7. Rekisterin valvontavastaavan on kirjattava lokiin kaikki EU:n turvallisuusluokiteltujen tietojen rekisteriin saapuvat ja sieltä poistuvat henkilöstön jäsenet, joilla ei ole pääsyä rekisteriin ilman saattajaa, ja oltava heidän mukanaan koko vierailun ajan.

8. Silloin kun henkilöstön jäsen vie asiakirjan pois EU:n turvallisuusluokiteltujen tietojen rekisteristä tarkempaa tutustumista varten, rekisterin valvontavastaavan on varmistettava, että henkilö on tietoinen asiaankuuluvista korvaavista turvatoimista ja palauttaa asiakirjan heti kun sitä ei enää tarvita. Rekisterin valvontavastaavan on muistutettava henkilöstöä siitä, että kaikki tällaiset asiakirjat on palautettava mahdollisimman pian.

9. EU:n turvallisuusluokiteltujen tietojen rekisteri antaa kuriiritodistuksen, jos turvallisuusluokiteltuja asiakirjoja kuljetetaan henkilökohtaisesti sen maan ulkopuolelle, jossa rekisteri sijaitse.

10. Rekisterin valvontavastaaville annetaan turvallisuusohjeessa tarkempaa ohjeistusta turvallisuusluokiteltujen asiakirjojen rekisteröinnistä.

20 artikla

Turvallisuusluokan alentaminen tai poistaminen

Rekisterin valvontavastaava auttaa EU:n turvallisuusluokitellut tiedot rekisteriin luovuttaneita osastoja tietojen uudelleentarkastelussa sen tarkistamiseksi, onko alkuperäinen turvallisuusluokka edelleen asianmukainen vai voidaanko turvallisuusluokkaa alentaa tai voidaanko se poistaa kokonaan.

21 artikla

Hävittäminen

1. Rekisterin valvontavastaavat ovat vastuussa CONFIDENTIEL UE/EU CONFIDENTIAL- ja sitä korkeammalle tasolle luokiteltujen tietojen asianmukaisesta hävittämisestä, tarvittaessa turvallisuusselvitettyjen todistajien läsnä ollessa.

2. Rekisterin valvontavastaavat kirjaavat CONFIDENTIEL UE/EU CONFIDENTIAL- ja sitä korkeammalle tasolle luokiteltujen tietojen hävittämisen turvallisuusluokiteltujen asiakirjojen rekisteriin ja säilyttävät asianomaiset hävittämistodistukset EU:n turvallisuusluokiteltujen tietojen rekisterissä.

22 artikla

Lisätehtävät

1. Rekisterin valvontavastaava antaa paikalliselle turvavastaavalle kaiken tarvittavan avun tämän hoitaessa EU:n turvallisuusluokiteltujen tietojen rekisteriin liittyviä valvontatehtäviä.

2. Rekisterin valvontavastaavan on ilmoitettava kaikista epäillyistä tai tosiasiallisista turvallisuushäiriöistä paikalliselle turvavastaavalle, joka puolestaan ilmoittaa niistä komission turvallisuusviranomaiselle.

3. Silloin kun komission osasto järjestää luottamuksellisen kokouksen CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeammalla tasolla, kyseisen osaston EU:n turvallisuusluokiteltujen tietojen rekisterin valvontavastaava valmistelee kokouksessa käsiteltävät EU:n turvallisuusluokitellut tiedot ja koordinoi toimia kokouksen järjestäjän kanssa sen varmistamiseksi, että kaikkia asiakirjoja ja tositteita käsitellään asiaankuuluvien sääntöjen mukaisesti.

6 LUKU

Loppusäännökset

23 artikla

Avoimuus

Tämä päätös on saatettava komission henkilöstön ja kaikkien niiden henkilöiden tietoon, joihin sitä sovelletaan, ja se on julkaistava *Euroopan unionin virallisessa lehdessä*.

24 artikla

Tämä päätös tulee voimaan seuraavana päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 7 päivänä huhtikuuta 2022.

Komission puolesta,
puheenjohtajan nimissä
Gertrud INGESTAD
Pääjohtaja
Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto