KOMISSION PÄÄTÖS (EU, Euratom) 2018/559,

annettu 6 päivänä huhtikuuta 2018,

viestintä- ja tietojärjestelmien turvallisuudesta Euroopan komissiossa annetun päätöksen (EU, Euratom) 2017/46 6 artiklan täytäntöönpanosäännöistä

EUROOPAN KOMISSIO, joka

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

ottaa huomioon Euroopan atomienergiayhteisön perustamissopimuksen,

ottaa huomioon viestintä- ja tietojärjestelmien turvallisuudesta Euroopan komissiossa 10 päivänä tammikuuta 2017 annetun komission päätöksen (EU, Euratom) 2017/46 ([1]) ja erityisesti sen 6 artiklan,

sekä katsoo seuraavaa:

(1) Päätöksen (EU, Euratom) 2017/46 hyväksymisen jälkeen on tarpeen, että komissio tarkistaa, saattaa ajan tasalle ja konsolidoi täytäntöönpanosäännöt, jotka liittyvät komission käyttämien viestintä- ja tietojärjestelmien turvallisuutta koskevaan kumottuun komission päätökseen K(2006) 3602.

(2) Turvallisuudesta vastaavalle komission jäsenelle on sisäisiä menettelysääntöjä täysimääräisesti noudattaen annettu tehtäväksi laatia täytäntöönpanosäännöt päätöksen (EU, Euratom) 2017/46 ([2]) 13 artiklan mukaisesti.

(3) Sen vuoksi olisi kumottava päätöksen K(2006) 3602 täytäntöönpanosäännöt,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Tämän päätöksen kohde ja soveltamisala esitetään päätöksen (EU, Euratom) 2017/46 1 artiklassa.

2. Tämän päätöksen säännöksiä sovelletaan kaikkiin viestintä- ja tietojärjestelmiin. Tässä päätöksessä määriteltyjä velvollisuuksia ei kuitenkaan sovelleta viestintä- ja tietojärjestelmiin, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja. Kyseisiin järjestelmiin liittyvät velvollisuudet määrittelee järjestelmän omistaja ja komission turvallisuusviranomainen komission päätöksen (EU, Euratom) 2015/444 ([3]) mukaisesti.

3. Tämän päätöksen 2 luvussa esitetään yleiskatsaus käytännön järjestelyihin, jotka koskevat tietotekniikan turvallisuuteen liittyvää organisaatiota ja vastuualueita. Tämän päätöksen 3 luvussa esitetään yleiskatsaus menettelyihin, jotka liittyvät päätöksen (EU, Euratom) 2017/46 6 artiklaan.

2 artikla

Määritelmät

Tässä päätöksessä sovelletaan päätöksen (EU, Euratom) 2017/46 2 artiklan määritelmiä. Lisäksi tässä päätöksessä tarkoitetaan

1) ’salauslaitteiden hyväksyntäviranomaisella’ komission turvallisuusviranomaisen hoitamaa tehtävää, joka kuuluu henkilöstöhallinnon ja turvallisuustoiminnan pääosaston toimivaltaan;

([1]) EUVL L 6, 11.1.2017, s. 40.
([2]) Komission päätös C(2017) 7428 final, annettu 8 päivänä marraskuuta 2017, Euroopan komission viestintä- ja tietojärjestelmien turvallisuutta koskevien täytäntöönpanosääntöjen, standardien ja suuntaviivojen hyväksymistä koskevien valtuuksien myöntämisestä.
([3]) Komission päätös (EU, Euratom) 2015/444, annettu 13 päivänä maaliskuuta 2015, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä (EUVL L 72, 17.3.2015, s. 53).

2) 'ulkoisella verkkoyhteydellä' sähköistä viestintäyhteyttä komission sisäisen verkon ja kaikkien muiden verkkojen, myös internetin, välillä. Määritelmään eivät sisälly kolmansien osapuolten verkot, jotka ovat sopimuksen mukaan osa komission sisäistä verkkoa;

3) 'vara-avainjärjestelmällä' menettelyä, jonka mukaisesti salausavainten jäljennökset tallennetaan yhden tai useamman kolmannen osapuolen haltuun ja jolla varmistetaan tehtävien eriyttäminen, jotta salausavaimet voidaan palauttaa silloin, kun käytössä oleva kappale on kadonnut. Avaimet voidaan jakaa kahteen tai useampaan osaan, joista kukin on eri osapuolen hallussa, sen varmistamiseksi, että millään yksittäisellä osapuolella ei ole hallussaan koko avainta;

4) lyhenteellä 'RASCI' vastuunjakoa, joka perustuu seuraaviin indikaattoreihin:

   a) ilmaisulla 'olla vastuussa' ("responsible" eli R) velvollisuutta toimia ja tehdä päätöksiä edellytettyjen tulosten saavuttamiseksi;

   b) ilmaisulla 'olla vastuuvelvollinen' ("accountable" eli A) vastuuvelvollisuutta toimista, päätöksistä ja suorituksista;

   c) ilmaisulla 'tukija' ("supports" eli S) velvollisuutta tehdä yhteistyötä vastuussa olevan henkilön kanssa tehtävän loppuun saattamiseksi;

   d) ilmaisulla 'neuvoja' ("consulted" eli C) velvollisuutta antaa neuvoja tai esittää mielipide;

   e) ilmaisulla 'tietoihin oikeutettu' ("informed" eli I) oikeutta saada ajantasaisia tietoja.

2 LUKU

ORGANISAATIO JA VASTUUALUEET

3 artikla

Roolit ja vastuualueet

Tämän päätöksen 4–8 artiklaan liittyvät roolit ja vastuualueet määritellään liitteessä RASCI-mallin mukaisesti.

4 artikla

Yhdenmukaisuus komission tietoturvapolitiikan kanssa

1. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto tarkastelee komission tietotekniikan turvallisuutta koskevaa politiikkaa ja siihen liittyviä standardeja ja ohjeita sen varmistamiseksi, että ne vastaavat komission yleisiä turvallisuuspolitiikkoja ja etenkin komission päätöstä (EU, Euratom) 2015/443 ([1]) ja päätöstä (EU, Euratom) 2015/444.

2. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto voi muiden komission osastojen pyynnöstä tarkistaa niiden tietotekniikan turvallisuutta koskevia politiikkoja tai muita asiakirjoja sen varmistamiseksi, että ne ovat yhdenmukaisia komission tietoturvapolitiikan kanssa. Kyseisen komission osaston päällikön on varmistettava, että mahdolliset ristiriidat korjataan.

3. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto tekee tietoturvallisuutta koskevan vastuualueensa mukaisesti yhteistyötä tietotekniikan pääosaston kanssa varmistaakseen, että tietotekniikan turvallisuutta koskevissa prosesseissa otetaan kaikilta osin huomioon päätöksessä (EU, Euratom) 2015/443 ja erityisesti sen 3 ja 9 artiklassa vahvistetut turvallisuusluokat ja -periaatteet.

3 LUKU

TIETOTEKNIIKAN TURVALLISUUTTA KOSKEVAT PROSESSIT

5 artikla

Salausteknologiat

1. Kun salausteknologioita käytetään EU:n turvallisuusluokiteltujen tietojen suojaamiseen, on noudatettava päätöstä (EU, Euratom) 2015/444.

2. Päätökset salausteknologioiden käytöstä EU:n turvallisuusluokittelemattomien tietojen suojaamiseksi tekee kunkin viestintä- ja tietojärjestelmän omistaja ottaen huomioon sekä riskit, joita salauksella on tarkoitus lieventää, että riskit, joita salaus aiheuttaa.

3. Salausteknologioiden käyttö edellyttää aina salauslaitteiden hyväksyntäviranomaisen ennakkohyväksyntää, paitsi jos salausta käytetään ainoastaan EU:n turvallisuusluokittelemattomien tietojen luottamuksellisuuden suojaamiseksi ja siinä hyödynnetään tavanomaisia verkon yhteyskäytäntöjä.

([1]) Komission päätös (EU, Euratom) 2015/443, annettu 13 päivänä maaliskuuta 2015, turvallisuudesta komissiossa (EUVL L 72, 17.3.2015, s. 41).

4. Ottaen huomioon tämän artiklan 3 kohdassa tarkoitettu poikkeus komission osastot varmistavat, että salausavainten varmuuskopiot varastoidaan vara-avainjärjestelmään, jotta tallennetut tiedot voidaan palauttaa siinä tapauksessa, että salausavain ei enää ole saatavilla. Salattujen tietojen palauttaminen salausavainten varmuuskopioiden avulla voidaan toteuttaa vain siinä tapauksessa, että se on salauslaitteiden hyväksyntäviranomaisen vahvistaman standardin mukaisesti sallittua.

5. Salausteknologioiden käytön hyväksyntäpyynnöt dokumentoidaan virallisesti, ja niihin on sisällyttävä yksityiskohtaiset tiedot viestintä- ja tietojärjestelmästä ja suojattavista tiedoista, käytettävistä teknologioista ja niihin liittyvistä turvamenettelyistä. Järjestelmän omistajan on allekirjoitettava nämä pyynnöt.

6. Salauslaitteiden hyväksyntäviranomainen arvioi salausteknologioiden käytön hyväksyntäpyynnöt julkaistujen standardien ja vaatimusten mukaisesti.

6 artikla

Tietotekniikan turvallisuutta koskevat tarkastukset

1. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto tekee tietotekniikan turvallisuutta koskevia tarkastuksia varmistaakseen, että tietotekniikan turvallisuutta koskevat toimenpiteet ovat komission tietotekniikan turvallisuutta koskevien politiikkojen mukaisia, ja tarkastaakseen valvontatoimenpiteiden eheyden.

2. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto voi tehdä tietotekniikan turvallisuutta koskevan tarkastuksen

a) omasta aloitteestaan;

b) tietoturvajohtoryhmän pyynnöstä;

c) järjestelmän omistajan pyynnöstä;

d) turvavälikohtauksen takia; tai

e) sen jälkeen, kun johonkin järjestelmään on havaittu kohdistuvan suuri riski.

3. Tietojen omistaja voi pyytää tietotekniikan turvallisuutta koskevaa tarkastusta ennen tietojen tallentamista viestintä- ja tietojärjestelmään.

4. Tarkastuksen tulokset on dokumentoitava järjestelmän omistajalle toimitettavaan viralliseen selvitykseen, josta annetaan jäljennös paikallistietojärjestelmien tietoturvavastaavalle ja johon sisältyvien päätelmien ja suositusten tarkoituksena on parantaa viestintä- ja tietojärjestelmän yhdenmukaisuutta tietotekniikan turvallisuutta koskevan politiikan kanssa. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto raportoi merkittävistä ongelmista ja suosituksista tietoturvajohtoryhmälle.

5. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto seuraa suositusten täytäntöönpanoa.

6. Tietotekniikan turvallisuutta koskeviin tarkastuksiin sisällytetään tarvittaessa järjestelmän omistajalle tarjottujen, sekä sisäisten että ulkoisten palveluntarjoajien tarjoamien palvelujen, tilojen ja laitteiden tarkastuksia.

7 artikla

Pääsy ulkoisista verkoista käsin

1. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto vahvistaa säännöt standardissa, joka koskee yhteyden myöntämistä komission viestintä- ja tietojärjestelmien ja ulkoisten verkkojen välillä.

2. Säännöissä on erotettava toisistaan erityyppiset ulkoiset verkkoyhteydet ja vahvistettava asianmukaiset turvallisuussäännöt kutakin yhteystyyppiä varten, mukaan lukien toimivaltaiselta viranomaiselta tämän artiklan 4 kohdan mukaisesti mahdollisesti tarvittava ennakkohyväksyntä.

3. Jos hyväksyntä tarvitaan, se myönnetään virallisen pyynnön ja hyväksymisprosessin perusteella. Hyväksyntä on voimassa määräajan, ja se on hankittava ennen yhteyden aktivoimista.

4. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto on kokonaisvastuussa pyyntöjen hyväksymisestä, mutta se voi delegoida hyväksymisvastuun tietyntyyppisten yhteyksien osalta oman harkintansa mukaisesti päätöksen (EU; Euratom) 2015/443 17 artiklan 3 kohdan ja tämän artiklan 8 kohdassa vahvistettujen edellytysten mukaisesti.

5. Luvan myöntäjä voi asettaa hyväksynnän ehdoksi ylimääräisiä turvallisuusvaatimuksia suojatakseen komission viestintä- ja tietojärjestelmiä ja verkkoja luvattoman pääsyn ja muiden tietoturvaloukkausten riskeiltä.

6. Tietotekniikan pääosasto on lähtökohtaisesti komission verkkopalvelujen tarjoaja. Kaikkien muiden komission osastojen, jotka käyttävät muuta kuin tietotekniikan pääosaston tarjoamaa verkkoa, on ensin saatava tietoturvajohtoryhmän suostumus. Komission osaston on dokumentoitava pyynnön liiketaloudelliset perustelut ja osoitettava, että verkon valvontatoimet riittävät täyttämään saapuvien ja lähtevien tietoliikennevirtojen valvontaa koskevat vaatimukset.

7. Viestintä- ja tietojärjestelmän omistaja vahvistaa turvallisuusvaatimukset, jotka koskevat pääsyä viestintä- ja tietojärjestelmään ulkopuolelta, ja varmistaa paikallistietojärjestelmien tietoturvavastaavien tuella, että järjestelmän suojaamiseksi toteutetaan asianmukaiset toimenpiteet.

8. Ulkoisia verkkoyhteyksiä koskevat turvatoimenpiteet perustuvat tarpeellisuusperiaatteeseen ja pienimmän mahdollisen etuoikeuden periaatteeseen, joiden avulla varmistetaan, että henkilöille annetaan vain ne tiedot ja pääsyoikeudet, joita he tarvitsevat voidakseen hoitaa viralliset tehtävänsä komission puolesta.

9. Kaikki ulkoiset verkkoyhteydet on suodatettava ja niitä on seurattava, jotta voidaan havaita mahdolliset tietoturvaloukkaukset.

10. Jos luodaan yhteyksiä viestintä- ja tietojärjestelmän ulkoistamista varten, hyväksymisen ehtona on 8 artiklassa kuvatun menettelyn saattaminen päätökseen.

8 artikla

Viestintä- ja tietojärjestelmien ulkoistaminen

1. Tässä päätöksessä viestintä- ja tietojärjestelmä katsotaan ulkoistetuksi, kun se perustuu jonkin kolmannen osapuolen kanssa tehtyyn sopimukseen, jonka mukaan järjestelmä sijaitsee komission tilojen ulkopuolella. Tähän sisältyy yksittäisten tai useiden viestintä- ja tietojärjestelmien tai muiden tietotekniikkapalvelujen ja tietokeskusten ulkoistaminen komission tilojen ulkopuolelle sekä ulkoisten yksiköiden suorittama komission tietokokonaisuuksien käsittely.

2. Viestintä- ja tietojärjestelmän ulkoistamisessa on otettava huomioon käsiteltävien tietojen arkaluonteisuus tai luokittelu seuraavasti:

a) Jos viestintä- ja tietojärjestelmässä käsitellään EU:n turvallisuusluokiteltuja tietoja, järjestelmän on saatava hyväksyntä päätöksen (EU, Euratom) 2015/444 mukaisesti ja komission turvallisuusjärjestelyjen hyväksyntäviranomaista on kuultava etukäteen. Järjestelmiä, joissa käsitellään EU:n turvallisuusluokiteltuja tietoja, ei saa ulkoistaa.

b) Jos viestintä- ja tietojärjestelmässä käsitellään EU:n turvallisuusluokittelemattomia tietoja, järjestelmän omistajan on toteutettava oikeasuhteisia toimenpiteitä turvallisuustarpeisiin vastaamiseksi ottaen huomioon asiaankuuluvat oikeudelliset velvoitteet tai tietojen arkaluonteisuus sekä ulkoistamiseen liittyvät riskit. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto voi asettaa lisävaatimuksia.

c) Ulkoistetuissa kehittämishankkeissa on otettava huomioon kehitettävän koodin arkaluonteisuus ja kehittämisen aikana mahdollisesti käytettävä testausaineisto.

3. Ulkoistettuihin viestintä- ja tietojärjestelmiin sovelletaan seuraavia periaatteita päätöksen (EU, Euratom) 2017/46 3 artiklassa vahvistettujen lisäksi:

a) ulkoistamisjärjestelyt suunnitellaan siten, että voidaan välttää riippuvuus yksittäisistä toimittajista;

b) ulkoistamiseen liittyvissä turvallisuusjärjestelyissä on minimoitava kolmansien osapuolten työntekijöiden mahdollisuudet päästä käsiksi komission tietoihin tai muuttaa niitä;

c) kolmansien osapuolten työntekijöiden, joilla on pääsy ulkoistettuun viestintä- ja tietojärjestelmään, on allekirjoitettava luottamuksellisuutta koskeva sopimus;

d) viestintä- ja tietojärjestelmän ulkoistaminen on mainittava viestintä- ja tietojärjestelmien luettelossa.

4. Järjestelmän omistajan on yhdessä tietojen omistajan kanssa

a) arvioitava ja dokumentoitava ulkoistamiseen liittyvät riskit;

b) vahvistettava asianomaiset turvallisuusvaatimukset;

c) kuultava kaikkien järjestelmään liittyvien muiden viestintä- ja tietojärjestelmien omistajia sen varmistamiseksi, että niiden turvallisuusvaatimukset on otettu huomioon;

d) varmistettava, että asianmukaiset turvallisuusvaatimukset ja oikeudet sisällytetään ulkoistamissopimukseen;

e) täytettävä mahdolliset muut vaatimukset, jotka esitetään yksityiskohtaisessa menettelyssä tämän artiklan 8 kohdan mukaisesti.

Nämä toimet on saatettava päätökseen ennen kuin sopimus yhden tai useamman viestintä- ja tietojärjestelmän ulkoistamisesta allekirjoitetaan.

5. Järjestelmien omistajien on hallittava ulkoistamiseen liittyviä riskejä viestintä- ja tietojärjestelmän elinkaaren aikana, jotta järjestelmät täyttävät määritellyt turvavaatimukset.

6. Järjestelmien omistajien on varmistettava, että kolmannet osapuolet (toimeksisaajat) ovat velvollisia viipymättä ilmoittamaan komissiolle kaikista ulkoistettuun komission viestintä- ja tietojärjestelmään vaikuttavista tietotekniikan turvallisuushäiriöistä.

7. Järjestelmän omistajan vastuulla on varmistaa, että viestintä- ja tietojärjestelmä, ulkoistamissopimus ja turvallisuusjärjestelyt ovat yhdenmukaisia tietoturvallisuutta ja tietotekniikan turvallisuutta koskevien komission sääntöjen kanssa.

8. Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto vahvistaa 10 artiklan mukaisesti yksityiskohtaisen standardin, joka koskee tämän artiklan 1–7 kohdassa esitettyjä vastuualueita ja toimia.

4 LUKU

MUUT SÄÄNNÖKSET JA LOPPUSÄÄNNÖKSET

9 artikla

Avoimuus

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

10 artikla

Standardit

1. Tämän päätöksen säännösten pohjalta voidaan tarvittaessa antaa yksityiskohtaisempia standardeja ja/tai suuntaviivoja, jotka hyväksytään päätöksen (EU, Euratom) 2017/46 ja päätöksen C(2017) 7428 mukaisesti. Nämä täytäntöönpanosäännöt ja päätöksen (EU, Euratom) 2017/46 säännökset vahvistetaan yksityiskohtaisemmin tietotekniikan turvallisuutta koskevissa standardeissa ja suuntaviivoissa, joita voidaan antaa tiettyjen turvallisuuden osa-alueiden osalta ISO-standardin 27001:2013 liitteen A mukaisesti. Nämä standardit ja suuntaviivat perustuvat toimialan parhaisiin käytäntöihin, ja ne on valittu siten, että ne sopivat komission tietotekniikkaympäristöön.

2. Standardeja kehitetään tarvittaessa ISO-standardin 27001:2013 liitteen A mukaisesti seuraavilla aloilla:

1) tietoturvallisuuden organisointi;

2) henkilöstöturvallisuus;

3) omaisuudenhoito;

4) pääsynvalvonta;

5) salaustekniikat;

6) fyysinen ja ympäristön turvallisuus;

7) käyttövarmuus;

8) tietoliikenneturvallisuus;

9) järjestelmien hankinta, kehittäminen ja ylläpito;

10) suhteet tavarantoimittajiin;

11) tietoturvaloukkausten hallinta;

12) toiminnan jatkuvuuden hallintaan liittyvät tietoturvallisuusnäkökohdat;

13) vaatimusten noudattaminen.

3. Tietoturvajohtoryhmä hyväksyy tämän artiklan 1 ja 2 kohdassa mainitut standardit ennen niiden vahvistamista.

4. Kumotaan tämän päätöksen soveltamisalaan liittyvät päätöksen K(2006) 3602 täytäntöönpanosäännöt.

5. 16 päivänä elokuun 2006 tehdyn päätöksen K(2006) 3602 nojalla hyväksytyt standardit ja suuntaviivat ovat edelleen voimassa siltä osin kuin ne eivät ole ristiriidassa näiden täytäntöönpanosääntöjen kanssa tai kunnes ne kumotaan tai korvataan päätöksen (EU, Euratom) 2017/46 13 artiklan nojalla hyväksyttävillä standardeilla tai suuntaviivoilla.

11 artikla

Voimaantulo

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

Tehty Brysselissä 6 päivänä huhtikuuta 2018.

Komission puolesta,
puheenjohtajan nimissä
Günther OETTINGER
Komission jäsen

LIITE

ROOLIT JA VASTUUALUEET (RASCI)

RASCI-mallissa eri yhteisöille jaettavia rooleja kuvataan seuraavilla lyhenteillä:

a) R on vastuussa

b) A on vastuuvelvollinen

c) S on tukija

d) C on neuvoja

e) I on tietoihin oikeutettu.

Rooli / Prosessi	Tietoturva-johtoryhmä	PO HR (turvalli-suusosasto)	Komission osastot	Järjestelmän omistaja	Tietojen omistaja	Paikallistieto-järjestelmien tietoturva-vastaava	Tietotek-niikan pää-osasto	Toimeksi-saajat
Yhdenmukaisuus komission tietoturvapolitiikan kanssa		**R/A**	**S**				**S**	
Salausteknologiat		**C**	**A**	**R**	**I**	**C**		
Tietotekniikan turvallisuustarkas-tukset	**I**	**A/R**		**S**	**I**	**I**	**S**	
Pääsy ulkoisista verkoista käsin	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Viestintä- ja tietojärjestelmien ulkoistaminen		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Tietoturvajohtoryhmä on neuvojana silloin, kun on kyse minkä tahansa muun komission osaston kuin tietotekniikan pääosaston sisäisten verkkojen toiminnasta.

[2] Ulkoistettavan viestintä- ja tietojärjestelmän omistaja on vastuussa, ja sellaisen muun viestintä- ja tietojärjestelmän omistaja, johon ulkoistettu järjestelmä on yhteydessä, on neuvoja.