PÄÄTÖKSET

KOMISSION PÄÄTÖS (EU, Euratom) 2017/46,

annettu 10 päivänä tammikuuta 2017,

viestintä- ja tietojärjestelmien turvallisuudesta Euroopan komissiossa

EUROOPAN KOMISSIO, joka

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

ottaa huomioon Euroopan atomienergiayhteisön perustamissopimuksen,

sekä katsoo seuraavaa:

(1) Komission viestintä- ja tietojärjestelmät ovat olennainen osa komission toimintaa, ja tietotekniikan turvallisuushäiriöillä voi olla vakavia vaikutuksia sekä komission toimintoihin että kolmansiin osapuoliin, yksittäiset henkilöt, yritykset ja jäsenvaltiot mukaan lukien.

(2) Komission viestintä- ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen sekä niissä käsiteltäviin tietoihin voi kohdistua monia uhkia. Tällaisia uhkia ovat muun muassa onnettomuudet, virheet, tahalliset hyökkäykset ja luonnontapahtumat, ja ne on määriteltävä operatiivisiksi riskeiksi.

(3) Viestintä- ja tietojärjestelmissä on tarjottava suojataso, joka on suhteutettu niihin kohdistuvien riskien todennäköisyyteen, vaikutuksiin ja luonteeseen.

(4) Komission tietotekniikan turvallisuuden osalta olisi varmistettava, että komission viestintä- ja tietojärjestelmät suojaavat niissä käsiteltävät tiedot ja toimivat tarkoituksenmukaisella tavalla, oikeaan aikaan ja oikeutettujen käyttäjien valvonnassa.

(5) Komission tietotekniikan turvallisuutta koskevaa politiikkaa olisi toteutettava johdonmukaisesti muiden turvallisuuspolitiikkojen kanssa.

(6) Yleinen vastuu komission turvallisuudesta on henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuusosastolla turvallisuusasioista vastaavan komission jäsenen valvonnassa ja vastuulla.

(7) Jotta komission lähestymistapa olisi asiaankuuluvan lainsäädännön mukainen ja jotta mahdollistettaisiin yhteentoimivuus ja -sopivuus, siinä olisi otettava huomioon EU:n poliittiset aloitteet, verkko- ja tietoturvaa koskeva lainsäädäntö sekä alan standardit ja parhaat käytännöt.

(8) Komission viestintä- ja tietojärjestelmistä vastaavien komission osastojen olisi laadittava ja pantava täytäntöön asiaankuuluvia toimenpiteitä, ja viestintä- ja tietojärjestelmien tietotekniikan turvallisuutta koskevat toimenpiteet olisi sovitettava yhteen koko komissiossa tehokkuuden ja vaikuttavuuden varmistamiseksi.

(9) Niiden sääntöjen ja menettelyjen, jotka koskevat tietoihin pääsyä tietotekniikan turvallisuuden yhteydessä, mukaan lukien tietotekniikan turvallisuushäiriöiden käsittely, olisi oltava oikeassa suhteessa komissioon tai sen henkilöstöön kohdistuvaan uhkaan sekä yksilöiden suojelusta unionin toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 45/2001 [1] säädettyjen periaatteiden mukaiset, ja niissä olisi otettava huomioon SEUT-sopimuksen 339 artiklassa säädetty salassapitovelvollisuuden periaate.

[1] Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, 12.1.2001, s. 1).

(10) EU:n turvaluokiteltua tietoa, arkaluonteista turvallisuusluokittelematonta tietoa ja luokittelematonta tietoa käsitteleviä viestintä- ja tietojärjestelmiä koskevien politiikkojen ja sääntöjen on oltava täysin komission päätösten (EU, Euratom) 2015/443 ([1]) ja (EU, Euratom) 2015/444 ([2]) mukaiset.

(11) Komission on tarpeen tarkistaa ja ajantasaistaa komission käyttämiä viestintä- ja tietojärjestelmiä koskevia säännöksiä.

(12) Sen vuoksi komission päätös K(2006) 3602 olisi kumottava,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Tätä päätöstä sovelletaan kaikkiin komission omistamiin, hankkimiin, hallinnoimiin tai ylläpitämiin tai komission puolesta omistettuihin, hankittuihin, hallinnoituihin tai ylläpidettyihin komission viestintä- ja tietojärjestelmiin ja kaikkeen kyseisten järjestelmien käyttöön komission toimesta.

2. Tässä päätöksessä vahvistetaan kyseisten viestintä- ja tietojärjestelmien turvallisuutta koskevat perusperiaatteet, tavoitteet, organisointi ja velvollisuudet erityisesti viestintä- ja tietojärjestelmiä omistaville, hankkiville, hallinnoiville tai ylläpitäville komission osastoille, mukaan lukien sisäisen tietopalvelun tarjoajan tarjoamat viestintä- ja tietojärjestelmät. Kun viestintä- ja tietojärjestelmän tarjoaa tai omistaa tai sitä hallinnoi tai ylläpitää ulkopuolinen taho komission kanssa tehdyn kahdenvälisen sopimuksen perusteella, kyseisen sopimuksen ehtojen on oltava tämän päätöksen mukaiset.

3. Tätä päätöstä sovelletaan kaikkiin komission osastoihin ja toimeenpanovirastoihin. Kun muut elimet ja toimielimet käyttävät komission viestintä- ja tietojärjestelmää komission kanssa tehdyn kahdenvälisen sopimuksen perusteella, kyseisen sopimuksen ehtojen on oltava tämän päätöksen mukaiset.

4. Riippumatta tiettyjä henkilöstöryhmiä koskevista erityismaininnoista tätä päätöstä sovelletaan komission jäseniin, Euroopan unionin virkamiehiin sovellettavien henkilöstösääntöjen, jäljempänä 'henkilöstösäännöt', ja unionin muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen ([3]), jäljempänä 'palvelussuhteen ehdot', alaiseen komission henkilöstöön, komission palvelukseen tilapäisesti siirrettyihin kansallisiin asiantuntijoihin ([4]), ulkopuolisiin palvelun-tarjoajiin ja niiden henkilöstöön, harjoittelijoihin ja kaikkiin henkilöihin, joilla on pääsy tämän päätöksen soveltamisalaan kuuluviin viestintä- ja tietojärjestelmiin.

5. Tätä päätöstä sovelletaan Euroopan petostentorjuntavirastoon (OLAF), siltä osin kuin se on unionin lainsäädännön ja komission päätöksen 1999/352/EY, EHTY, Euratom ([5]) mukaista. Tässä päätöksessä säädettyjä toimenpiteitä, mukaan lukien ohjeistukset, tarkastukset, tutkimukset ja vastaavat toimenpiteet, ei sovelleta kyseisen viraston viestintä- ja tietojärjestelmiin, jos se ei ole yhteensopivaa viraston tutkintatehtävien riippumattomuuden ja/tai viraston kyseisiä tehtäviä toteuttaessaan saamien tietojen luottamuksellisuuden kanssa.

2 artikla

Määritelmät

Tässä päätöksessä tarkoitetaan

1) ilmaisulla 'olla vastuuvelvollinen' vastuuvelvollisuutta toimista, päätöksistä ja suorituksista;

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

([2]) 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).

([3]) Säädetään neuvoston asetuksessa (ETY, Euratom, EHTY) N:o 259/68, annettu 29 päivänä helmikuuta 1968, Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta ja komission virkamiehiin väliaikaisesti sovellettavista erityistoimenpiteistä (Muuta henkilöstöä koskevat palvelussuhteen ehdot) (EYVL L 56, 4.3.1968, s. 1.)

([4]) Komission päätös, tehty 12 päivänä marraskuuta 2008, komission palvelukseen tilapäisesti siirrettyihin ja komissiossa ammatillisessa jatkokoulutuksessa oleviin kansallisiin asiantuntijoihin sovellettavista säännöistä (K(2008) 6866 lopullinen).

([5]) Komission päätös 1999/352/EY, EHTY, Euratom, tehty 28 päivänä huhtikuuta 1999, Euroopan petostentorjuntaviraston (OLAF) perustamisesta (EYVL L 136, 31.5.1999, s. 20).

2) ’CERT-EU:lla’ EU:n toimielinten ja virastojen tietotekniikan kriisiryhmää. Sen tehtävänä on tukea EU:n toimielimiä, jotta nämä voivat suojautua tahallisilta ja vihamielisiltä hyökkäyksiltä, jotka voisivat haitata niiden tietoteknisten resurssien eheyttä ja vahingoittaa EU:n etuja. CERT-EU:n toiminta-alaan kuuluvat ennaltaehkäisy, havaitseminen, reagoiminen ja toimintakunnon palauttaminen;

3) ’komission osastolla’ mitä tahansa komission pääosastoa tai yksikköä taikka komission jäsenen kabinettia;

4) ’komission turvallisuusviranomaisella’ päätöksessä (EU, Euratom) 2015/444 säädettyä roolia;

5) ’viestintä- ja tietojärjestelmällä’ järjestelmää, jolla tietoa käsitellään sähköisessä muodossa, mukaan lukien kaikki järjestelmän toiminnan kannalta tarpeelliset resurssit, myös infrastruktuuri, organisaatio, henkilöstö ja tietoresurssit. Määritelmä sisältää liiketoimintasovellukset, jaetut tietotekniikkapalvelut, ulkoistetut järjestelmät ja loppukäyttäjien laitteet;

6) ’hallintoneuvostolla’ operatiivisten ja hallinnollisten seikkojen korkeimman tason valvontaelintä komissiossa;

7) ’tietojen omistajalla’ henkilöä, joka on vastuussa viestintä- ja tietojärjestelmän käsittelemän tietyn tietokokonaisuuden suojaamisen ja käytön varmistamisesta;

8) ’tietokokonaisuudella’ tietokokonaisuutta, joka palvelee komission tiettyä komission liiketoimintaprosessia tai toimea;

9) ’kiireellisellä menettelyllä’ ennalta määriteltyä menetelmien ja velvollisuuksien kokonaisuutta, jolla reagoidaan kiireellisiin tilanteisiin komissioon kohdistuvan merkittävän vaikutuksen estämiseksi;

10) ’tietoturvapolitiikalla’ vahvistettujen tai vahvistettavien, täytäntöönpantujen tai täytäntöönpantavien sekä tarkastettujen tai tarkastettavien tietoturvatavoitteiden kokonaisuutta. Siihen sisältyvät muun muassa mutteivät yksinomaan päätökset (EU, Euratom) 2015/444 ja (EU, Euratom) 2015/443;

11) ’tietoturvajohtoryhmällä’ hallintoelintä, joka tukee hallintoneuvostoa tietotekniikan turvallisuuteen liittyvissä tehtävissä;

12) ’sisäisellä tietopalvelun tarjoajalla’ jaettuja tietotekniikkapalveluja tarjoavaa komission osastoa;

13) ’tietotekniikan turvallisuudella’ tai ’viestintä- ja tietojärjestelmän turvallisuudella’ viestintä- ja tietojärjestelmien sekä niiden käsittelemien tietokokonaisuuksien luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä;

14) ’tietotekniikan turvallisuutta koskevilla ohjeilla’ suositeltavia mutta vapaaehtoisia toimenpiteitä, joilla helpotetaan tietotekniikan turvallisuutta koskevien standardien tukemista tai joihin viitataan silloin, kun sovellettavaa standardia ei ole;

15) ’tietotekniikan turvallisuushäiriöllä’ tapahtumaa, josta voi olla haittaa viestintä- ja tietojärjestelmän luottamuksellisuudelle, eheydelle ja käytettävyydelle;

16) ’tietotekniikan turvallisuutta koskevalla toimenpiteellä’ teknistä tai organisatorista toimenpidettä tietoturvariskien hillitsemiseksi;

17) ’tietotekniikan turvallisuutta koskevalla tarpeella’ johonkin tietoon tai tietotekniseen järjestelmään liittyvien luottamuksellisuus-, eheys- ja käytettävyystasojen tarkkaa ja yksiselitteistä määrittelyä vaadittavan suojatason määrittelemiseksi;

18) ’tietotekniikan turvallisuutta koskevalla tavoitteella’ ilmaistua aietta torjua määritellyt uhat ja/tai vastata määriteltyihin turvallisuutta koskeviin organisatorisiin vaatimuksiin tai olettamuksiin;

19) ’tietotekniikan turvallisuutta koskevalla suunnitelmalla’ viestintä- ja tietojärjestelmän tietotekniikan turvallisuutta koskeviin tarpeisiin vastaamiseksi tarvittavien tietotekniikan turvallisuutta koskevien toimenpiteiden dokumentointia;

20) ’tietotekniikan turvallisuutta koskevalla politiikalla’ vahvistettujen tai vahvistettavien, täytäntöönpantujen tai täytäntöönpantavien sekä tarkastettujen tai tarkastettavien tietotekniikan turvallisuutta koskevien tavoitteiden kokonaisuutta. Se sisältää tämän päätöksen ja sen täytäntöönpanosäännöt;

21) ’tietotekniikan turvallisuutta koskevalla vaatimuksella’ ennaltamääritellyn prosessin kautta muotoiltua tietotekniikan turvallisuutta koskevaa tarvetta;

22) ’tietotekniikan turvallisuutta koskevalla riskillä’ vaikutusta, jonka tietotekniikan turvallisuutta koskeva uhka voi aiheuttaa viestintä- ja tietojärjestelmään sen haavoittuvuutta hyväksi käyttäen. Tietotekniikan turvallisuutta koskevalla riskillä on kaksi ominaisuutta: 1) epävarmuus eli todennäköisyys, että tietotekniikan turvallisuutta koskeva uhka aiheuttaa epätoivotun tapahtuman, ja 2) vaikutus eli tällaisen epätoivotun tapahtuman mahdolliset vaikutukset viestintä- ja tietojärjestelmään;

23) ’tietotekniikan turvallisuutta koskevilla standardeilla’ erityisiä tietotekniikan turvallisuutta koskevia toimenpiteitä tietotekniikan turvallisuutta koskevan politiikan täytäntöönpanemisen ja tukemisen helpottamiseksi;

24) ’tietotekniikan turvallisuutta koskevalla strategialla’ sellaisten komission tavoitteiden saavuttamiseksi tarkoitettujen hankkeiden ja toimien kokonaisuutta, jotka on vahvistettava, pantava täytäntöön ja tarkastettava;

25) ’tietotekniikan turvallisuutta koskevalla uhalla’ tekijää, joka voi johtaa viestintä- ja tietojärjestelmää vahingoittavaan epätoivottuun tapahtumaan. Tällaiset uhat voivat olla tahattomia tai tahallisia, ja niille ovat ominaisia uhkaavat seikat sekä mahdolliset kohteet ja hyökkäysmenetelmät;

26) ’paikallistietojärjestelmien tietoturvavastaavalla’ virkamiestä, joka toimii komission osastossa yhteyshenkilönä tietotekniikan turvallisuutta koskevissa asioissa;

27) ’henkilötiedoilla’, ’henkilötietojen käsittelyllä’, ’rekisterinpitäjällä’ ja ’henkilötietojen rekisteröintijärjestelmällä’ on samat määritelmät kuin asetuksessa (EY) N:o 45/2001 ja erityisesti sen 2 artiklassa;

28) ’tietojen käsittelyllä’ kaikkia tietokokonaisuuksiin liittyviä viestintä- ja tietojärjestelmän toimintoja, mukaan lukien tietojen luominen, muuttaminen, näyttäminen, varastoiminen, siirtäminen, poistaminen ja arkistoiminen. Viestintä- ja tietojärjestelmä voi suorittaa tietojen käsittelyn toimintokokonaisuutena käyttäjille ja tietotekniikkapalveluina toiselle viestintä- ja tietojärjestelmälle;

29) ’salassapitovelvollisuudella’ salassapitovelvollisuuden piiriin kuuluvien liiketietojen, erityisesti yrityksiä taikka niiden liikesuhteita tai kustannustekijöitä koskevien tietojen suojaa, kuten SEUT-sopimuksen 339 artiklassa määrätään;

30) ilmaisulla ’olla vastuussa’ velvollisuutta toimia ja tehdä päätöksiä edellytettyjen tulosten saavuttamiseksi;

31) ’turvallisuudella komissiossa’ henkilöiden, omaisuuden ja tiedon turvallisuutta komissiossa ja erityisesti henkilöiden ja omaisuuden fyysistä koskemattomuutta, tiedon ja viestintä- ja tietojärjestelmien koskemattomuutta, luottamuksellisuutta ja saatavuutta sekä komission toiminnan esteetöntä toimivuutta;

32) ’jaetuilla tietotekniikkapalveluilla’ viestintä- ja tietojärjestelmän tarjoamaa tietojen käsittelyyn liittyvää palvelua muille viestintä- ja tietojärjestelmille;

33) ’järjestelmän omistajalla’ henkilöä, joka vastaa viestintä- ja tietojärjestelmän yleisestä hankinnasta, kehittämisestä, integroinnista, muuttamisesta, toiminnasta, ylläpitämisestä ja käytöstä poistamisesta;

34) ’käyttäjällä’ henkilöä, joka käyttää viestintä- ja tietojärjestelmän tarjoamaa toimintoa komissiossa tai sen ulkopuolella.

3 artikla

Periaatteet, jotka koskevat tietotekniikan turvallisuutta komissiossa

1. Tietotekniikan turvallisuus komissiossa perustuu laillisuuden, avoimuuden, suhteellisuuden ja vastuuvelvollisuuden periaatteisiin.

2. Tietotekniikan turvallisuuteen liittyvät seikat on otettava huomioon alusta lähtien laadittaessa ja toteutettaessa komission viestintä- ja tietojärjestelmiä. Tätä varten tietotekniikan pääosaston sekä henkilöstöhallinnon ja turvallisuustoiminnan pääosaston on osallistuttava omien vastuualueidensa osalta.

3. Tehokkaassa tietotekniikan turvallisuudessa on varmistettava asianmukaiset tasot seuraaville:

a) aitous: tae siitä, että tiedot ovat aitoja ja vilpittömässä mielessä toimivista lähteistä;

b) käytettävyys: tiedot ovat valtuutetun yksikön pyynnöstä saatavilla ja käytettävissä;

c) luottamuksellisuus: tiedot eivät tule ilmi sivullisille henkilöille, yksiköille eikä prosesseille;

d) eheys: omaisuuden ja tietojen oikeellisuus ja täydellisyys turvataan;

e) kiistattomuus: tietty toimi tai tapahtuma voidaan todistaa tapahtuneeksi niin, ettei sitä voida myöhemmin kiistää;

f) henkilötietojen suoja: henkilötietojen osalta tarjotaan asianmukaiset takeet noudattaen täysin asetusta (EY) N:o 45/2001:

g) salassapitovelvollisuus: salassapitovelvollisuuden piiriin kuuluvien liiketietojen, erityisesti yrityksiä taikka niiden liikesuhteita tai kustannustekijöitä koskevien tietojen suojaaminen, kuten SEUT-sopimuksen 339 artiklassa määrätään.

4. Tietotekniikan turvallisuuden on perustuttava riskinhallintaprosessiin. Tämän prosessin tarkoituksena on määritellä tietotekniikan turvallisuutta koskevien riskien tasot ja turvatoimenpiteet tällaisten riskien pienentämiseksi asianmukaiselle tasolle kohtuullisin kustannuksin.

5. Jokainen viestintä- ja tietojärjestelmä on tunnistettava, sille on määrättävä järjestelmän omistaja ja se on kirjattava luetteloon.

6. Jokaisen viestintä- ja tietojärjestelmän turvavaatimukset on määriteltävä kyseisen järjestelmän ja sen käsittelemien tietojen turvallisuustarpeiden perusteella. Viestintä- ja tietojärjestelmä, joka tarjoaa palveluja toiselle viestintä- ja tietojärjestelmälle, voi olla suunniteltu tukemaan erityisiä turvallisuustarvetasoja.

7. Tietotekniikan turvallisuutta koskevien suunnitelmien ja toimenpiteiden on oltava oikeassa suhteessa viestintä- ja tietojärjestelmän turvallisuustarpeisiin nähden.

Näihin periaatteisiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

2 LUKU

ORGANISAATIO JA VASTUUALUEET

4 artikla

Hallintoneuvosto

Hallintoneuvostolla on yleinen vastuu tietotekniikan turvallisuuden kokonaishallinnosta komissiossa.

5 artikla

Tietoturvajohtoryhmä

1. Tietoturvajohtoryhmän puheenjohtajana toimii komission tietotekniikan turvallisuushallinnosta vastaava varapääsihteeri. Sen komission eri osastoista tulevien jäsenten on edustettava yritys-, teknologia- ja turvallisuusasioita, ja siinä on oltava edustajia tietotekniikan pääosastosta, henkilöstöhallinnon ja turvallisuustoiminnan pääosastosta ja budjettipääosastosta sekä vuorotellen kahden vuoden välein edustajia neljästä muusta komission osastosta silloin, kun tietotekniikan turvallisuus on merkittävä huolenaihe niiden toiminnan kannalta. Jäsenet kuuluvat ylempään johtoon.

2. Tietoturvajohtoryhmä tukee hallintoneuvostoa tietotekniikan turvallisuuteen liittyvissä tehtävissä. Tietoturvajohtoryhmällä on operatiivinen vastuu tietotekniikan turvallisuuden kokonaishallinnosta komissiossa.

3. Tietoturvajohtoryhmä suosittelee komission tietotekniikan turvallisuuspolitiikkaa komission hyväksyttäväksi.

4. Tietoturvajohtoryhmä tarkastelee hallintoasioita ja tietotekniikan turvallisuuteen liittyviä kysymyksiä, vakavat tietotekniikan turvallisuushäiriöt mukaan lukien, ja raportoi niistä joka toinen vuosi hallintoneuvostolle.

5. Tietoturvajohtoryhmä seuraa ja tarkastelee tämän päätöksen yleistä täytäntöönpanoa ja raportoi siitä hallintoneuvostolle.

6. Tietoturvajohtoryhmä tarkastelee, arvioi ja valvoo päivittyvän tietotekniikan turvallisuutta koskevan strategian täytäntöönpanoa tietotekniikan pääosaston ehdotuksesta. Tietoturvajohtoryhmä raportoi siitä hallintoneuvostolle.

7. Tietoturvajohtoryhmä seuraa, arvioi ja valvoo yleistä tietoturvariskitilannetta, ja sillä on valtuudet antaa tarvittaessa virallisia parannussuosituksia.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

6 artikla

Henkilöstöhallinnon ja turvallisuustoiminnan pääosasto

Henkilöstöhallinnon ja turvallisuustoiminnan pääosastolla on tietotekniikan turvallisuuden osalta seuraavat velvollisuudet: Sen on

1) varmistettava, että tietotekniikan turvallisuutta koskeva politiikka ja komission tietoturvapolitiikka ovat yhdenmukaiset;

2) laadittava puitteet salausteknologioiden käytön sallimiseksi viestintä- ja tietojärjestelmien suorittamaa tietojen varastointia ja välittämistä varten;

3) ilmoitettava tietotekniikan pääosastolle uhkista, jotka voivat vaikuttaa merkittävästi viestintä- ja tietojärjestelmien ja niiden käsittelemien tietokokonaisuuksien turvallisuuteen;

4) tehtävä tietotekniikan turvallisuutta koskevia tarkastuksia arvioidakseen, ovatko komission viestintä- ja tietojärjestelmät turvallisuuspolitiikan mukaiset, ja raportoitava tuloksista tietoturvajohtoryhmälle;

5) laadittava puitteet ja asianmukaiset turvallisuussäännöt pääsyn sallimiseksi komission viestintä- ja tietojärjestelmiin ulkoisista verkostoista sekä kehitettävä asiaan liittyvät tietotekniikan turvallisuutta koskevat standardit ja ohjeet tiiviissä yhteistyössä tietotekniikan pääosaston kanssa;

6) ehdotettava viestintä- ja tietojärjestelmien ulkoistamista koskevia periaatteita ja sääntöjä, joiden avulla tietoturvan asianmukainen valvonta säilytetään;

7) kehitettävä 6 artiklaan liittyviä tietotekniikan turvallisuutta koskevia standardeja ja ohjeita tiiviissä yhteistyössä tietotekniikan pääosaston kanssa.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

7 artikla

Tietotekniikan pääosasto

Tietotekniikan pääosastolla on komission yleisen tietotekniikan turvallisuuden osalta seuraavat velvollisuudet: Sen on

1) tietotekniikan turvallisuutta koskevan politiikan ja komission tietoturvapolitiikan yhdenmukaisuuden varmistamiseksi kehitettävä tietotekniikan turvallisuutta koskevia standardeja ja ohjeita – lukuun ottamatta niitä, joista säädetään 6 artiklassa – tiiviissä yhteistyössä henkilöstöhallinnon ja turvallisuustoiminnan pääosaston kanssa, ja ehdotettava niitä tietoturvajohtoryhmälle;

2) arvioitava tietotekniikan turvallisuutta koskevien riskien hallintamenetelmiä ja kaikkien komission osastojen prosesseja ja tuotoksia sekä raportoitava niistä säännöllisesti tietoturvajohtoryhmälle;

3) esitettävä tietoturvajohtoryhmälle päivittyvän tietotekniikan turvallisuutta koskevan strategian päivittämistä ja hyväksymistä sekä hallintoneuvostolle sen vahvistamista sekä ehdotettava ohjelmaa, joka sisältää muun muassa hankkeiden ja toimien suunnittelun tietotekniikan turvallisuutta koskevan strategian täytäntöönpanemiseksi;

4) valvottava komission tietotekniikan turvallisuutta koskevan strategian täytäntöönpanoa ja raportoitava siitä säännöllisesti tietoturvajohtoryhmälle;

5) valvottava tietotekniikan turvallisuutta koskevia riskejä ja viestintä- ja tietojärjestelmissä toteutettavia tietotekniikan turvallisuutta koskevia toimenpiteitä, sekä raportoitava niistä säännöllisesti tietoturvajohtoryhmälle;

6) raportoitava säännöllisesti tietoturvajohtoryhmälle tämän päätöksen yleisestä täytäntöönpanosta ja noudattamisesta;

7) pyydettävä henkilöstöhallinnon ja turvallisuustoiminnan pääosastoa kuultuaan järjestelmän omistajia toteuttamaan erityisiä tietotekniikan turvallisuutta koskevia toimenpiteitä komission viestintä- ja tietojärjestelmille aiheutuvien tietotekniikan turvallisuutta koskevien riskien vähentämiseksi;

8) varmistettava, että järjestelmien ja tietojen omistajien saatavilla on asianmukainen luettelo tietotekniikan pääosaston tarjoamista tietotekniikan turvallisuuspalveluista, jotta nämä voivat täyttää tietotekniikan turvallisuuteen liittyvät velvollisuutensa ja noudattaa tietotekniikan turvallisuutta koskevaa politiikkaa ja standardeja;

9) annettava järjestelmien ja tietojen omistajille asianmukaiset asiakirjat ja tapauksen mukaan kuultava tällaisia omistajia niiden tietotekniikkapalvelujen osalta toteutetuista tietotekniikan turvallisuutta koskevista toimenpiteistä tietotekniikan turvallisuutta koskevan politiikan noudattamisen helpottamiseksi ja järjestelmän omistajien tukemiseksi tietoturvallisuuteen liittyvien riskien hallinnassa;

10) järjestettävä säännöllisesti paikallistietojärjestelmien tietoturvavastaavien verkoston kokouksia ja tuettava paikallistietojärjestelmien tietoturvavastaavia näiden suorittaessa velvollisuuksiaan;

11) määriteltävä koulutustarpeet ja koordinoitava koulutusohjelmia tietotekniikan turvallisuuden osalta yhteistyössä komission osastojen kanssa sekä kehitettävä, toteutettava ja koordinoitava kampanjoita tietoisuuden lisäämiseksi tietotekniikan turvallisuudesta tiiviissä yhteistyössä henkilöstöhallinnon pääosaston kanssa;

12) varmistettava, että järjestelmän omistajat, tietojen omistajat ja muut, joilla on tietotekniikan turvallisuuteen liittyviä velvollisuuksia komission osastoissa, saavat tietoa tietotekniikan turvallisuutta koskevasta politiikasta;

13) annettava henkilöstöhallinnon ja turvallisuustoiminnan pääosastolle tiedoksi sellaiset järjestelmien omistajien ilmoittamat tietotekniikan turvallisuuteen liittyvät uhat ja häiriöt sekä poikkeukset komission tietotekniikan turvallisuutta koskevaan politiikkaan, jotka voivat vaikuttaa merkittävästi turvallisuuteen komissiossa;

14) toimitettava komissiolle sisäisen tietotekniikkapalvelun tarjoajan ominaisuudessa luettelo jaetuista tietotekniikkapalveluista, jotka tarjoavat määritellyt turvallisuustasot. Tämä voidaan tehdä arvioimalla, hallinnoimalla ja seuraamalla tietotekniikan turvallisuutta koskevia riskejä säännöllisesti, jotta voidaan toteuttaa turvallisuustoimenpiteitä määritellyn turvallisuustason saavuttamiseksi.

Näihin liittyvät menettelyt ja tarkemmat vastuukuvaukset vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

8 artikla

Komission osastot

Komission jokaisen osaston päällikön on osastonsa tietotekniikan turvallisuuden osalta

1) nimitettävä virallisesti jokaiselle viestintä- ja tietojärjestelmälle kyseisen järjestelmän tietotekniikan turvallisuudesta vastuussa oleva järjestelmän omistaja, jonka on oltava virkamies tai väliaikainen toimihenkilö, sekä jokaiselle viestintä- ja tietojärjestelmässä käsiteltävälle tietokokonaisuudelle tietojen omistaja, jonka on kuuluttava samaan hallinnolliseen yksikköön kuin asetuksen (EY) N:o 45/2001 soveltamisalaan kuuluvien tietokokonaisuuksien rekisterinpitäjä;

2) nimitettävä virallisesti paikallistietojärjestelmien tietoturvavastaava, joka voi toteuttaa velvollisuuksia riippumattomasti järjestelmän omistajista ja tietojen omistajista. Sama paikallistietojärjestelmien tietoturvavastaava voidaan nimittää yhdelle tai useammalle komission osastolle;

3) varmistettava, että asianmukaiset tietotekniikan turvallisuutta koskevien riskien arvioinnit ja tietotekniikan turvallisuutta koskevat suunnitelmat on laadittu ja pantu täytäntöön;

4) varmistettava, että tietotekniikan pääosastolle toimitetaan säännöllisesti yhteenveto tietotekniikan turvallisuuteen liittyvistä riskeistä ja toimenpiteistä;

5) varmistettava tietotekniikan pääosaston tuella, että käytössä on asianmukaiset prosessit, menettelyt ja ratkaisut sen viestintä- ja tietojärjestelmiin liittyvien tietotekniikan turvallisuushäiriöiden tehokkaan havaitsemisen, raportoinnin ja ratkaisemisen varmistamiseksi;

6) käynnistettävä kiireellinen menettely tietotekniikan turvallisuutta koskevissa hätätilanteissa;

7) oltava viime kädessä vastuuvelvollinen tietotekniikan turvallisuudesta, mukaan lukien järjestelmän omistajan ja tietojen omistajan velvollisuudet;

8) omistettava viestintä- ja tietojärjestelmiinsä ja tietokokonaisuuksiinsa liittyvät riskit;

9) ratkaistava tietojen omistajien ja järjestelmän omistajien väliset erimielisyydet ja erimielisyyden jatkuessa saatettava asia tietoturvajohtoryhmän ratkaistavaksi;

10) varmistettava, että tietotekniikan turvallisuutta koskevat suunnitelmat ja toimenpiteet pannaan täytäntöön ja että riskeihin on varauduttu asianmukaisesti.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

9 artikla

Järjestelmän omistajat

1. Järjestelmän omistaja vastaa viestintä- ja tietojärjestelmän tietotekniikan turvallisuudesta ja raportoi komission osaston päällikölle.

2. Järjestelmän omistajan on tietotekniikan turvallisuuden osalta

a) varmistettava, että viestintä- ja tietojärjestelmä on tietotekniikan turvallisuutta koskevan politiikan mukainen;

b) varmistettava, että viestintä- ja tietojärjestelmä kirjataan tarkoin asiaankuuluvaan luetteloon;

c) arvioitava tietotekniikan turvallisuutta koskevat riskit ja määriteltävä tietotekniikan turvallisuutta koskevat tarpeet kunkin viestintä- ja tietojärjestelmän osalta yhteistyössä tietojen omistajien kanssa ja tietotekniikan pääosastoa kuullen;

d) laadittava turvallisuussuunnitelma, joka sisältää tapauksen mukaan tiedot arvioiduista riskeistä ja mahdolliset muut vaadittavat lisäturvallisuustoimenpiteet;

e) pantava täytäntöön asianmukaiset tietotekniikan turvallisuutta koskevat toimenpiteet, jotka ovat oikeassa suhteessa havaittuihin tietotekniikan turvallisuutta koskeviin riskeihin ja ovat tietoturvajohtoryhmän vahvistamien suositusten mukaiset;

f) määriteltävä riippuvuussuhteet muihin viestintä- ja tietojärjestelmiin tai jaettuihin tietotekniikkapalveluihin ja toteutettava turvallisuustoimenpiteitä, jotka perustuvat tapauksen mukaan kyseisten viestintä- ja tietojärjestelmien tai jaettujen tietotekniikkapalvelujen ehdottamiin turvallisuustasoihin;

g) hallittava ja seurattava tietotekniikan turvallisuutta koskevia riskejä;

h) raportoitava säännöllisesti komission osaston päällikölle tämän viestintä- ja tietojärjestelmien tietoturvallisuuteen liittyvistä riskiprofiileista ja tietotekniikan pääosastolle asiaan liittyvistä riskeistä sekä toteutetuista riskihallinta-toimista ja turvallisuustoimenpiteistä;

i) kuultava asianomaisten komission osastojen paikallistietojärjestelmien tietoturvavastaavia tietotekniikan turvallisuuteen liittyvistä näkökohdista;

j) annettava käyttäjille ohjeistusta, joka koskee viestintä- ja tietojärjestelmien ja niihin liittyvien tietojen käyttöä sekä käyttäjien viestintä- ja tietojärjestelmiin liittyviä velvollisuuksia;

k) pyydettävä salausasioista vastaavana viranomaisena toimivalta henkilöstöhallinnon ja turvallisuustoiminnan pääosastolta lupa salausteknologiaa käyttäville viestintä- ja tietojärjestelmille;

l) kuultava etukäteen komission turvallisuusviranomaista kaikista EU:n turvaluokiteltuja tietoja käsittelevistä järjestelmistä;

m) varmistettava, että salausavainten varmuuskopiot varastoidaan sulkutilille. Salatut tiedot voidaan palauttaa vain, jos se on etukäteen sallittu henkilöstöhallinnon ja turvallisuustoiminnan pääosaston määrittelemien puitteiden mukaisesti;

n) noudatettava rekisterinpitäjien ohjeistusta, joka koskee henkilötietojen suojaa ja tietosuojasääntöjen soveltamista käsittelyn turvallisuuteen;

o) ilmoitettava tietotekniikan pääosastolle poikkeuksista komission tietotekniikan turvallisuutta koskevaan politiikkaan ja annettava asianmukaiset perustelut;

p) raportoitava tietojen omistajien ja järjestelmän omistajien välisistä ratkaisemattomista erimielisyyksistä komission osaston päällikölle sekä ilmoitettava asianomaisille osapuolille tietotekniikan turvallisuushäiriöistä oikea-aikaisesti tarvittaessa niiden vakavuuden mukaan, kuten 15 artiklassa säädetään;

q) ulkoistettujen järjestelmien osalta varmistettava, että ulkoistamissopimuksissa on asianmukaiset tietotekniikan turvallisuutta koskevat määräykset ja että ulkoistetuissa viestintä- ja tietojärjestelmissä esiintyvistä tietotekniikan turvallisuushäiriöistä raportoidaan 15 artiklan mukaisesti;

r) jaettuja tietotekniikkapalveluja tarjoavien viestintä- ja tietojärjestelmien osalta varmistettava, että ne tarjoavat selkeästi dokumentoidun määritellyn turvallisuustason ja että määritellyn turvallisuustason saavuttamiseksi toteutetaan turvallisuustoimenpiteitä.

3. Järjestelmän omistaja voi virallisesti antaa tietotekniikan turvallisuuteen liittyvät tehtävät kokonaan tai osittain muille, mutta vastuu viestintä- ja tietojärjestelmän tietotekniikan turvallisuudesta säilyy hänellä itsellään.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

10 artikla

Tietojen omistajat

1. Tietojen omistaja vastaa komission osaston päällikölle tietyn tietokokonaisuuden tietotekniikan turvallisuudesta ja on vastuuvelvollinen tietokokonaisuuden luottamuksellisuudesta, eheydestä ja käytettävyydestä.

2. Tietojen omistajan on tällaisen tietokokonaisuuden osalta

a) varmistettava, että kaikki hänen vastuullaan olevat tietokokonaisuudet luokitellaan päätösten (EU, Euratom) 2015/443 ja (EU, Euratom) 2015/444 mukaisesti;

b) määriteltävä tietoturvatarpeet ja ilmoitettava niistä asianomaisille järjestelmän omistajille;

c) osallistuttava viestintä- ja tietojärjestelmän riskinarviointiin;

d) raportoitava tietojen omistajien ja järjestelmän omistajien välisistä ratkaisemattomista erimielisyyksistä komission osaston päällikölle;

e) ilmoitettava tietotekniikan turvallisuushäiriöistä 15 artiklan mukaisesti.

3. Tietojen omistaja voi virallisesti siirtää tietotekniikan turvallisuuteen liittyvät tehtävät kokonaan tai osittain muille, mutta vastuu säilyy hänellä itsellään tässä artiklassa säädetyllä tavalla.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

11 artikla

Paikallistietojärjestelmien tietoturvavastaavat

Paikallistietojärjestelmien tietoturvavastaavan on tietotekniikan turvallisuuden osalta

a) ennakoivasti yksilöitävä järjestelmän omistajat, tietojen omistajat ja muut, joilla on tietotekniikan turvallisuuteen liittyviä velvollisuuksia komission osastoissa, sekä annettava näille tietoa tietotekniikan turvallisuutta koskevasta politiikasta;

b) oltava osana paikallistietojärjestelmien tietoturvavastaavien verkostoa yhteydessä tietotekniikan pääosastoon asioissa, jotka liittyvät tietotekniikan turvallisuuteen komission osastoissa;

c) osallistuttava paikallistietojärjestelmien tietoturvavastaavien säännöllisiin kokouksiin;

d) oltava ajan tasalla tietoturvallisuusriskien hallintaprosessista ja tietojärjestelmien turvallisuussuunnitelmien laadinnasta ja täytäntöönpanosta;

e) neuvottava tietojen omistajia, järjestelmän omistajia ja komission osastojen päälliköitä tietotekniikan turvallisuuteen liittyvissä kysymyksissä;

f) tehtävä yhteistyötä tietotekniikan pääosaston kanssa hyvien tietotekniikan turvallisuutta koskevien käytäntöjen levittämiseksi ja ehdotettava tiedotus- ja koulutusohjelmia;

g) raportoitava tietotekniikan turvallisuudesta ja ilmoitettava puutteista ja parannuksista komission osastoille.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

12 artikla

Käyttäjät

1. Käyttäjien on tietotekniikan turvallisuuden osalta

a) noudatettava tietotekniikan turvallisuutta koskevaa politiikkaa ja järjestelmän omistajan antamia kunkin viestintä- ja tietojärjestelmän käyttöä koskevaa ohjeistusta;

b) ilmoitettava tietotekniikan turvallisuushäiriöistä 15 artiklan mukaisesti.

2. Komission viestintä- ja tietojärjestelmän käyttö tietotekniikan turvallisuutta koskevan politiikan tai järjestelmän omistajan antaman ohjeistuksen vastaisesti voi johtaa kurinpidollisiin menettelyihin.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

3 LUKU

TURVALLISUUSVAATIMUKSET JA VELVOLLISUUDET

13 artikla

Tämän päätöksen täytäntöönpano

1. Edellä olevan 6 artiklan soveltamista koskevat säännöt ja asiaan liittyvät standardit ja ohjeet edellyttävät valtuutuspäätöstä, jonka komissio antaa turvallisuusasioista vastaavalle komission jäsenelle.

2. Kaikki muut tämän asetuksen soveltamista koskevat säännöt ja asiaan liittyvät tietotekniikan turvallisuutta koskevat standardit ja ohjeet edellyttävät valtuutuspäätöstä, jonka komissio antaa tietotekniikasta vastaavalle komission jäsenelle.

3. Tietoturvajohtoryhmä hyväksyy 1 ja 2 kohdassa mainitut soveltamissäännöt, standardit ja ohjeet ennen niiden hyväksymistä.

14 artikla

Noudattamisvelvollisuus

1. Tietotekniikan turvallisuutta koskevassa politiikassa ja standardeissa olevien määräysten noudattaminen on pakollista.

2. Tietotekniikan turvallisuutta koskevan politiikan ja standardien noudattamatta jättäminen saattaa antaa aiheen kurinpitotoimiin perussopimusten, henkilöstösääntöjen ja palvelussuhteen ehtojen mukaisesti sekä sopimusseuraamuksiin ja/tai oikeustoimiin kansallisten lakien ja säännösten mukaisesti.

3. Tietotekniikan pääosastolle on ilmoitettava kaikista poikkeuksista tietotekniikan turvallisuutta koskevaan politiikkaan.

4. Jos tietoturvajohtoryhmä päättää, että komission viestintä- ja tietojärjestelmälle aiheutuu jatkuva kohtuuton riski, tietotekniikan pääosaston on järjestelmän omistajan kanssa yhteistyössä ehdotettava tietoturvajohtoryhmän hyväksyttäväksi riskiä vähentäviä toimenpiteitä. Kyseisiin toimenpiteisiin voi sisältyä muun muassa tehostettua seurantaa ja raportointia, palvelurajoituksia ja yhteyden katkaiseminen.

5. Tietoturvajohtoryhmän on tarvittaessa määrättävä hyväksyttyjen lieventävien toimenpiteiden toteuttaminen pakolliseksi. Tietoturvajohtoryhmä voi myös suositella, että henkilöstöhallinnon ja turvallisuustoiminnan pääosaston pääjohtaja käynnistää hallinnollisen tutkimuksen. Tietotekniikan pääosaston on raportoitava tietoturvajohtoryhmälle kaikista tilanteista, joissa on määrätty lieventäviä toimenpiteitä.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

15 artikla

Tietotekniikan turvallisuushäiriöiden käsittely

1. Vastuu pääasiallisesta operatiivisesta kyvystä vastata tietotekniikan turvallisuushäiriöihin Euroopan unionissa on tietotekniikan pääosastolla.

2. Kun henkilöstöhallinnon ja turvallisuustoiminnan pääosasto osallistuu osapuolena tietotekniikan turvallisuushäiriöihin reagoimiseen, sen on

a) saatava oikeus tutustua kaikkia häiriökirjauksia koskeviin yhteenvetotietoihin ja pyydettäessä täydellisiin tiedostoihin;

b) osallistuttava tietotekniikan turvallisuushäiriöitä käsitteleviin kriisinhallintaryhmiin ja tietotekniikan turvallisuutta koskeviin kiireellisiin menettelyihin;

c) vastattava suhteista lainvalvonta- ja tiedustelupalvelujen kanssa;

d) tehtävä tietoverkkoturvallisuutta koskeva rikostekninen analyysi päätöksen (EU, Euratom) 2015/443 11 artiklan mukaisesti;

e) päätettävä virallisen tutkinnan aloittamisen tarpeesta;

f) ilmoitettava tietotekniikan pääosastolle kaikista tietotekniikan turvallisuushäiriöistä, joista voi aiheutua riski toisille viestintä- ja tietojärjestelmille.

3. Tietotekniikan pääosaston sekä henkilöstöhallinnon ja turvallisuustoiminnan pääosaston välillä on oltava säännöllistä viestintää tietojen vaihtamiseksi ja turvallisuushäiriöiden käsittelyn koordinoimiseksi, erityisesti kun kyseessä on tietotekniikan turvallisuushäiriö, joka voi vaatia virallista tutkintaa.

4. EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) tietoturvapoikkeamien koordinointipalvelua voidaan käyttää tapauksen mukaan tukemaan häiriöiden käsittelyprosessia ja tietojen jakamista muille EU:n toimielimille ja virastoille, joihin tilanteella saattaa olla vaikutusta.

5. Järjestelmän omistajien, joihin tietotekniikan turvallisuushäiriö vaikuttaa, on

a) ilmoitettava välittömästi komission osastonsa päällikölle, tietotekniikan pääosastolle, henkilöstöhallinnon ja turvallisuustoiminnan pääosastolle, paikallistietojärjestelmien tietoturvavastaaville ja tapauksen mukaan tietojen omistajalle kaikista merkittävistä tietotekniikan turvallisuushäiriöistä ja erityisesti niistä, joihin liittyy tietosuojan rikkominen;

b) tehtävä yhteistyötä ja seurattava asiaankuuluvien komission viranomaisten antamaa ohjeistusta, joka koskee häiriöstä ilmoittamista, häiriöön reagoimista ja häiriön korjaamista;

6. Käyttäjien on ilmoitettava kaikista tosiasiallisista ja epäillyistä tietotekniikan turvallisuushäiriöistä nopeasti asiaankuuluvalle tietotekniikan tukipalvelulle.

7. Tietojen omistajien on ilmoitettava kaikista tosiasiallisista ja epäillyistä tietotekniikan turvallisuushäiriöistä nopeasti asiaankuuluvalle tietotekniikan turvallisuushäiriöitä käsittelevälle kriisiryhmälle.

8. Vastuu komission muissa kuin ulkoistetuissa viestintä- ja tietojärjestelmissä havaittujen tietotekniikan turvallisuushäiriöiden käsittelemisestä on tietotekniikan pääosastolla, jota muut osallistuvat osapuolet tukevat.

9. Tietotekniikan pääosaston on tarpeellisuusperiaatteen mukaisesti ilmoitettava tietotekniikan turvallisuushäiriöistä asianomaisille komission osastoille, asianomaisille paikallistietojärjestelmien tietoturvavastaaville ja tapauksen mukaan CERT-EU:lle.

10. Tietotekniikan pääosaston on raportoitava säännöllisesti tietoturvajohtoryhmälle merkittävistä komission viestintä- ja tietojärjestelmiin vaikuttavista tietotekniikan turvallisuushäiriöistä.

11. Asianomaisella paikallistietojärjestelmien tietoturvavastaavalla on oltava pyynnöstä pääsy rekisteriin, johon kirjataan komission osaston viestintä- ja tietojärjestelmää koskevat tietotekniikan turvallisuushäiriöt.

12. Kun kyseessä on merkittävä tietotekniikan turvallisuushäiriö, tietotekniikan pääosasto toimii yhteystahona kriisitilanteen hallinnoinnissa ja koordinoi tietotekniikan turvallisuushäiriöitä käsitteleviä kriisinhallintaryhmiä.

13. Tietotekniikan pääosaston pääjohtaja voi hätätapauksessa päättää käynnistää tietotekniikan turvallisuutta koskevan kiireellisen menettelyn. Tietotekniikan pääosaston on laadittava kiireelliset menettelyt, jotka tietoturvajohtoryhmä hyväksyy.

14. Tietotekniikan pääosaston on raportoitava kiireellisten menettelyjen toteuttamisesta tietoturvajohtoryhmälle ja asianomaisten komission osastojen päälliköille.

Näihin velvollisuuksiin ja toimintoihin liittyvät menettelyt vahvistetaan yksityiskohtaisemmin täytäntöönpanosäännöissä.

4 LUKU

LOPPUSÄÄNNÖKSET

16 artikla

Avoimuus

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

17 artikla

Suhde toisiin säädöksiin

Tämän päätöksen säännöksiä sovelletaan rajoittamatta seuraavien säädösten soveltamista: päätös (EU, Euratom) 2015/443, päätös (EU, Euratom) 2015/444, asetus (EY) N:o 45/2001, Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001 ([1]), komission päätös 2002/47/EY, EHTY, Euratom ([2]), Euroopan parlamentin ja neuvoston asetus (EU, Euratom) N:o 883/2013 ([3]) ja päätös 1999/352/EY, EHTY, Euratom.

18 artikla

Kumoaminen ja siirtymäsäännökset

Kumotaan 16 päivänä elokuuta 2006 tehty päätös K(2006) 3602.

Päätöksen K(2006) 3602 nojalla hyväksytyt soveltamissäännöt ja tietotekniikan turvallisuutta koskevat standardit ovat voimassa edelleen, jolleivät ne ole ristiriidassa tämän päätöksen kanssa, siihen saakka kun ne korvataan tämän päätöksen 13 artiklan nojalla hyväksyttävillä soveltamissäännöillä ja standardeilla. Viittauksia päätöksen K(2006) 3602 10 artiklaan pidetään viittauksina tämän päätöksen 13 artiklaan.

19 artikla

Voimaantulo

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

Tehty Brysselissä 10 päivänä tammikuuta 2017.

Komission puolesta

Puheenjohtaja

Jean-Claude JUNCKER

([1]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi (EYVL L 145, 31.5.2001, s. 43).

([2]) Komission päätös 2002/47/EY, EHTY, Euratom, tehty 23 päivänä tammikuuta 2002, työjärjestyksensä muuttamisesta (EYVL L 21, 24.1.2002, s. 23).

([3]) Euroopan parlamentin ja neuvoston asetus (EU, Euratom) N:o 883/2013, annettu 11 päivänä syyskuuta 2013, Euroopan petostentorjuntaviraston (OLAF) tutkimuksista sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1073/1999 ja neuvoston asetuksen (Euratom) N:o 1074/1999 kumoamisesta (EUVL L 248, 18.9.2013, s. 1).