BESLUT

KOMMISSIONENS BESLUT (EU, Euratom) 2017/46

av den 10 januari 2017

om säkerheten i Europeiska kommissionens kommunikations- och informationssystem

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 249,

med beaktande av fördraget om upprättandet av Europeiska atomenergigemenskapen, och

av följande skäl:

(1) Kommissionens kommunikations- och informationssystem är en integrerad del av kommissionens verksamhet, och säkerhetsincidenter på it-området kan få allvarliga följder för såväl kommissionens arbete som tredje part, däribland fysiska personer, företag och medlemsstater.

(2) Det finns många hot mot kommissionens kommunikations- och informationssystem som kan skada såväl sekretessen, integriteten och tillgängligheten, som den information som behandlas i dessa system. Hotet inbegriper olyckor, misstag, avsiktliga attacker och naturfenomen och måste erkännas som operativa risker.

(3) Kommunikations- och informationssystemen måste ges en skyddsnivå som står i proportion till den risk som de är utsatta för, med hänsyn tagen till riskens sannolikhet, följder och art.

(4) It-säkerheten inom kommissionen bör säkerställa att kommissionens kommunikations- och informationssystem skyddar den information som de behandlar och att de fungerar som de ska när så krävs, under kontroll av behöriga användare.

(5) Kommissionens strategi för it-säkerhet bör tillämpas på ett sätt som är förenligt med EU:s politik om säkerhet inom kommissionen.

(6) Direktoratet för säkerhet inom generaldirektoratet för personal och säkerhet har det övergripande ansvaret för säkerheten inom kommissionen, under överinseende av kommissionsledamoten med ansvarar för säkerhetsfrågor som är ansvarig för detta.

(7) Kommissionens strategi bör beakta EU:s politiska initiativ och lagstiftning om nät- och informationssäkerhet, branschnormer och bästa praxis för att efterleva all tillämplig lagstiftning och möjliggöra driftskompatibilitet och kompatibilitet.

(8) Lämpliga åtgärder bör utarbetas och tillämpas av kommissionens avdelningar med ansvar för kommunikations- och informationssystem, och it-säkerhetsåtgärder till skydd för kommunikations- och informationssystem bör samordnas inom hela kommissionen för att säkerställa effektivitet och ändamålsenlighet.

(9) Bestämmelser och förfaranden som gäller tillgång till information i samband med it-säkerhet, också hantering av säkerhetsincidenter på it-området, måste stå i proportion till hotet mot kommissionen eller dess personal och överensstämma med principerna i Europaparlamentets och rådets förordning (EG) nr 45/2001 [1] om skydd för enskilda då unionsinstitutionerna och unionsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter samt med beaktande av principen om tystnadsplikt i enlighet med artikel 339 i EUF-fördraget.

[1] Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

(10) Strategier och bestämmelser för kommunikations- och informationssystem som behandlar säkerhetsskyddsklassificerade EU-uppgifter och känsliga icke-skyddsklassificerade uppgifter ska till fullo överensstämma med kommissionens beslut (EU, Euratom) 2015/443 ([1]) och (EU, Euratom) 2015/444 ([2]).

(11) Kommissionen behöver se över och uppdatera bestämmelserna om säkerhet i de kommunikations- och informationssystem som används av kommissionen.

(12) Kommissionens beslut K(2006) 3602 bör därför upphävas.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. Detta beslut är tillämpligt på samtliga kommunikations- och informationssystem som ägs, förvaltas eller drivs av kommissionen eller för dess räkning och på all kommissionens användning av dessa system.

2. I detta beslut fastställs de grundläggande principerna, målen och ansvaret för säkerheten med avseende på dessa kommunikations- och informationssystem, i synnerhet för de avdelningar inom kommissionen som äger, upphandlar, förvaltar eller driver sådana system och system som tillhandahålls av interna leverantörer av it-tjänster. När ett kommunikations- och informationssystem tillhandahålls, ägs, förvaltas eller drivs av en extern part på grundval av ett bilateralt avtal eller kontrakt med kommissionen, ska avtals- eller kontraktsvillkoren vara förenliga med föreliggande beslut.

3. Detta beslut ska tillämpas på alla kommissionens avdelningar och genomförandeorganen. När något av kommissionens kommunikations- och informationssystem används av andra organ och institutioner på grundval av ett bilateralt avtal med kommissionen, ska avtalsvillkoren vara förenliga med föreliggande beslut.

4. Utan hinder av särskilda beteckningar för vissa grupper av anställda, ska detta beslut tillämpas på ledamöterna av kommissionen, kommissionens personal som omfattas av tjänsteföreskrifterna för tjänstemän i Europeiska unionen (nedan kallade *tjänsteföreskrifterna*) och anställningsvillkoren för övriga anställda i Europeiska unionen (nedan kallade *anställningsvillkoren*) ([3]), de nationella experter som är utstationerade vid kommissionen (nedan kallade *nationella experter*) ([4]), externa tjänsteleverantörer och deras anställda, praktikanter och vem som helst som har tillgång till sekretessbelagd information som omfattas av detta beslut.

5. Detta beslut ska tillämpas på Europeiska byrån för bedrägeribekämpning (Olaf), i den mån detta är förenligt med unionslagstiftningen och kommissionens beslut 1999/352/EG, EKSG, Euratom ([5]). I synnerhet ska de åtgärder som föreskrivs i detta beslut, inbegripet anvisningar, inspektioner, utredningar och motsvarande åtgärder, inte tillämpas på kommunikations- och informationssystemen vid en byrå där detta inte är förenligt med byråns oberoende utredningsfunktion och/eller konfidentialiteten med avseende på information som Olaf erhållit under fullgörandet av sitt uppdrag.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner:

1. *ansvarig*: person med ansvar för insatser, beslut och resultat.

([1]) Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41).
([2]) Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).
([3]) Enligt rådets förordning (EEG, Euratom, EKSG) nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper samt om införande av särskilda tillfälliga åtgärder beträffande kommissionens tjänstemän (EGT L 56, 4.3.1968, s. 1).
([4]) Kommissionens beslut av den 12 november 2008 om bestämmelser för utstationering till kommissionen av nationella experter och nationella experter under utbildning (K(2008) 6866 slutlig).
([5]) Kommissionens beslut 1999/352/EG, EKSG, Euratom av den 28 april 1999 om inrättande av en europeisk byrå för bedrägeribekämpning (OLAF) (EGT L 136, 31.5.1999, s. 20).

2. *Cert-EU*: incidenthanteringsorganisationen för EU:s institutioner och byråer. Dess uppgift är att hjälpa EU:s institutioner att skydda sig mot avsiktliga och illvilliga angrepp som negativt skulle påverka integriteten i deras it-system och skada EU:s intressen. Cert-EU:s verksamhet omfattar förebyggande, upptäckt, reaktion och återställande.

3. *Kommissionsavdelning*: kommissionens generaldirektorat eller avdelningar, eller en kommissionsledamots kansli.

4. *kommissionens säkerhetsmyndighet*: det uppdrag som fastställs i beslut (EU, Euratom) 2015/444.

5. *kommunikations- och informationssystem*: system som möjliggör hantering av information i elektronisk form, inbegripet de resurser som krävs för att driva dessa system, också infrastruktur, organisation, personal och informationsresurser. Denna definition inbegriper verksamhetsanpassade tillämpningar, delade it-tjänster, utlokaliserade system och apparater för slutanvändare.

6. *förvaltningens styrelse*: den högsta nivån inom förvaltningens tillsyn av operativa och administrativa frågor inom kommissionen.

7. *dataägare*: person som ansvarar för att säkerställa skyddet och användningen av specifika data som hanteras i ett kommunikations- och informationssystem.

8. *dataset*: uppsättning uppgifter som används i vissa verksamhetsprocesser eller aktiviteter inom kommissionen.

9. *nödförfarande*: förutbestämd uppsättning metoder och ansvarsuppgifter för att reagera på nödsituationer i syfte att förhindra allvarliga följder för kommissionen.

10. *strategi för informationssäkerhet*: uppsättning mål för informationssäkerheten som ställts upp eller behöver ställas upp, tillämpas och kontrolleras. Strategin omfattar, men är inte begränsad till, besluten (EU, Euratom) 2015/444 och (EU, Euratom) 2015/443.

11. *Styrelsen för informationssäkerhet*: styrorgan som bistår förvaltningens styrelse i dess uppgifter med koppling till it-säkerheten.

12. *intern leverantör av it-tjänster*: kommissionsavdelning som tillhandahåller delade it-tjänster.

13. *it-säkerhet* eller *kommunikations- och informationssystemens säkerhet*: bevarande av kommunikations- och informationssystemens konfidentialitet, integritet och tillgänglighet, vilket också inbegriper de dataset som de behandlar.

14. *riktlinjerna för it-säkerhet*: består av rekommenderade och frivilliga åtgärder som bidrar till att underbygga it-säkerhetsnormerna eller tjäna som referens när inga tillämpliga normer finns.

15. *säkerhetsincident på it-området*: en händelse som negativt kan påverka ett kommunikations- och informationssystems konfidentialitet, integritet eller tillgänglighet.

16. *säkerhetsåtgärd på it-området*: en teknisk eller organisatorisk åtgärd för att minska it-säkerhetsriskerna.

17. *it-säkerhetsbehov*: exakt och entydig definition av nivåerna för konfidentialitet, integritet och tillgänglighet med anknytning till viss information eller ett it-system i syfte att fastställa vilken skyddsnivå som krävs.

18. *it-säkerhetsmål*: avsiktsförklaring för att motverka specifika hot och/eller uppfylla vissa organisatoriska krav eller antaganden med avseende på säkerheten.

19. *it-säkerhetsplan*: dokumentation av de säkerhetsåtgärder som krävs för att tillgodose säkerhetsbehoven i ett kommunikations- och informationssystem.

20. *strategi för it-säkerhet*: uppsättning it-säkerhetsmål, som har ställts upp eller behöver ställas upp, tillämpas och kontrolleras. Strategin omfattar detta beslut och dess tillämpningsföreskrifter.

21. *it-säkerhetskrav*: ett it-säkerhetsbehov som formaliserats genom ett förutbestämt förfarande.

22. *it-säkerhetsrisk*: den effekt som ett it-säkerhetshot kan få på ett kommunikations- och informationssystem om sårbarheten utnyttjas. It-säkerhetsrisker kännetecknas av två faktorer: 1) osäkerhet, dvs. sannolikheten för att ett it-säkerhetshot leder till en oönskad effekt, och 2) följder, dvs. de konsekvenser som en sådan oönskad händelse kan få för ett kommunikations- och informationssystem.

23. *it-säkerhetsnormer*: särskilda obligatoriska åtgärder för it-säkerheten som bidrar till att stärka och underbygga strategin för it-säkerhet.

24. *strategi för it-säkerhet*: ett antal projekt och insatser utformade för att uppnå kommissionens mål och som måste påbörjas, tillämpas och kontrolleras.

25. *it-säkerhetshot*: faktor som potentiellt kan leda till en oönskad händelse vilken kan skada ett kommunikations- och informationssystem. Sådana hot kan vara oavsiktliga eller avsiktliga och kännetecknas av hotande element, potentiella mål och angreppsmetoder.

26. *säkerhetsansvarig för de lokala datasystemen*: tjänsteman med ansvar för it-säkerhetssambandet inom en avdelning vid kommissionen.

27. *personuppgifter, behandling av personuppgifter, registeransvarig* och *register med personuppgifter*: samma innebörd som i förordning (EG) nr 45/2001, särskilt artikel 2.

28. *uppgiftsbehandling*: alla funktioner i ett kommunikations- och informationssystem med avseende på dataset, också upprättande, ändring, visning, lagring, överföring, lagring, gallring och arkivering av uppgifter. Informationsbehandling kan utföras av ett kommunikations- och informationssystem i form av en uppsättning funktioner för användare och it-tjänster till andra kommunikations- och informationssystem.

29. *tystnadsplikt*: skyddet för uppgifter om företag av det slag som omfattas av tystnadsplikt, särskilt uppgifter om företag, deras affärsförbindelser eller deras kostnadsförhållanden som fastställs i artikel 339 i EUF-fördraget.

30. *ansvarig*: person med skyldighet att agera och fatta beslut för att uppnå nödvändiga resultat.

31. *säkerhet inom kommissionen*: säkerheten för personer, tillgångar och information inom kommissionen, särskilt fysisk integritet för personer och tillgångar, integritet, sekretess och tillgång till både information och kommunikations- och informationssystem samt förutsättningar för att kommissionens arbete ska kunna fungera obehindrat.

32. *delad it-tjänst*: tjänst som ett kommunikations- och informationssystem erbjuder andra kommunikations- och informationssystem för informationsbehandling.

33. *systemägare*: person som har det övergripande ansvaret för upphandling, utveckling och integration, ändring, drift, underhåll och nedläggning av ett kommunikations- och informationssystem.

34. *användare*: fysisk person som använder funktionerna i ett kommunikations- och informationssystem, oavsett om detta sker inom eller utanför kommissionen.

Artikel 3

Principerna för it-säkerheten inom kommissionen

1. It-säkerheten inom kommissionen ska grunda sig på principerna om lagenlighet, öppenhet, proportionalitet och ansvarighet.

2. It-säkerhetsfrågor ska beaktas redan när kommissionens kommunikations- och informationssystem börjar utvecklas och tillämpas. För att göra detta kommer generaldirektoratet för informationsteknik och generaldirektoratet för personal och säkerhet att anlitas inom sina respektive ansvarsområden.

3. Effektiv it-säkerhet ska säkerställa lämpliga nivåer för följande:

a) Autenticitet: Garanti för att uppgifterna är riktiga och härrör från pålitliga källor.

b) Tillgänglighet: Egenskapen att finnas tillgänglig och vara användbar för en behörig enhet.

c) Konfidentialitet: Egenskapen att uppgifter skyddas mot insyn av obehöriga personer, enheter eller processer.

d) Riktighet: Egenskapen att säkersälla att uppgifter och tillgångar är exakta och fullständiga.

e) Oavvislighet: Möjlighet att bevisa att en åtgärd eller händelse har ägt rum, så att denna händelse eller åtgärd inte senare kan förnekas.

f) Skydd av personuppgifter: Tillhandahållande av lämpliga skyddsåtgärder för personuppgifter i fullständig överensstämmelse med förordning (EG) nr 45/2001.

g) Tystnadsplikt: Skydd för upplysningar av det slag som omfattas av tystnadsplikt, särskilt uppgifter om företag, deras affärsförbindelser eller deras kostnadsförhållanden som fastställs i artikel 339 i EUF-fördraget.

4. It-säkerheten ska grunda sig på en riskhanteringsprocess. Syftet med processen är att fastställa nivåerna på it-säkerhetsriskerna och fastställa säkerhetsåtgärder för att till en proportionerlig kostnad sänka risknivån till en lämplig grad.

5. Samtliga kommunikations- och informationssystem ska identifieras och tillskrivas en systemägare samt registreras i en förteckning.

6. Säkerhetskraven för alla kommunikations- och informationssystem ska fastställas på grundval av deras säkerhetsbehov och av säkerhetsbehoven för de uppgifter som de behandlar. Kommunikations- och informationssystem som erbjuder andra system tjänster kan utformas för att stödja särskilda säkerhetsbehov.

7. It-säkerhetsplaner och it-säkerhetsåtgärder ska stå i proportion till säkerhetsbehoven i systemet.

De processer som rör dessa principer och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

KAPITEL 2

ORGANISATION OCH ANSVAR

Artikel 4

Förvaltningens styrelse

Förvaltningens styrelse ska ha det övergripande ansvaret för förvaltningen av all it-säkerhet inom kommissionen.

Artikel 5

Styrelsen för informationssäkerhet

1. Styrelsen för informationssäkerhet ska ledas av biträdande generalsekreteraren med ansvar för förvaltningen av it-säkerheten inom kommissionen. Styrelsens ledamöter ska företräda verksamhet-, teknik- och säkerhetsintressen inom alla kommissionens avdelningar och inbegripa företrädare för generaldirektoratet för informationsteknik, generaldirektoratet för personal och säkerhet, generaldirektoratet för budget och, enligt ett tvåårigt rotationssystem, företrädare för fyra andra avdelningar inom kommissionen som är involverade på områden som innebär att it-säkerheten är en viktig fråga för deras arbete. Medlemskapet ska vara knutet till chefsnivån.

2. Styrelsen för informationssäkerhet ska stödja förvaltningens styrelse i dess uppgifter avseende it-säkerheten. Styrelsen för informationssäkerhet ska ta det operativa ansvaret för förvaltningen av it-säkerheten som helhet inom kommissionen.

3. Styrelsen för informationssäkerhet ska rekommendera kommissionen att anta kommissionens strategi för it-säkerhet.

4. Styrelsen för informationssäkerhet ska granska och två gånger om året avlägga rapport inför förvaltningens styrelse om både ledningsfrågor och frågor som rör it-säkerhet, inbegripet allvarliga säkerhetsincidenter på it-området.

5. Styrelsen för informationssäkerhet ska övervaka och granska den allmänna tillämpningen av detta beslut och avlägga rapport om det inför förvaltningens styrelse.

6. På förslag av generaldirektoratet för informationsteknik ska styrelsen för informationssäkerhet granska, godkänna och övervaka tillämpningen av den löpande strategin för it-säkerhet. Styrelsen för informationssäkerhet ska avlägga rapport inför förvaltningens styrelse.

7. Styrelsen för informationssäkerhet ska övervaka, utvärdera och kontrollera förvaltningens riskhantering och ha befogenhet att utfärda formella krav på förbättringar när så krävs.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 6

Generaldirektoratet för personal och säkerhet

Generaldirektoratet för personal och säkerhet har nedanstående ansvar i fråga om it-säkerhet. Byrån ska

1. säkerställa samstämmighet mellan strategin för it-säkerhet och kommissionens strategi för informationssäkerhet,

2. fastställa en ram för godkännande av tillämpningen av krypteringsteknik för lagring och överföring av information från kommunikations- och informationssystem,

3. informera generaldirektoratet för informationsteknik om specifika hot som kan få betydande följder för säkerheten i kommunikations- och informationssystemen och de uppgifter som de behandlar,

4. utföra inspektioner av it-säkerheten för att bedöma huruvida kommissionens kommunikations- och informationssystem överensstämmer med säkerhetsstrategin, och avlägga rapport om resultaten till styrelsen för informationssäkerhet,

5. inrätta en ram, och lämpliga associerade säkerhetsbestämmelser, för auktorisation av tillgång till kommissionens kommunikations- och informationssystem från externa nätverk, samt, i nära samarbete med generaldirektoratet för informationsteknik, utveckla relaterade normer och riktlinjer för it-säkerheten,

6. lägga fram förslag om principer och bestämmelser för utlokalisering av kommunikations- och informationssystem för att upprätthålla lämplig kontroll över informationssäkerheten,

7. i nära samarbete med generaldirektoratet för informationsteknik utveckla relaterade normer och riktlinjer för it-säkerheten i förhållande till artikel 6.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 7

Generaldirektoratet för informationsteknik

I fråga om den övergripande it-säkerheten inom kommissionen ansvarar generaldirektoratet för informationsteknik för följande: Byrån ska

1. i nära samarbete med generaldirektoratet för personal och säkerhet utveckla normer och riktlinjer för it-säkerheten, med undantag för det som föreskrivs i artikel 6, för att garantera överensstämmelse mellan strategin för it-säkerhet och kommissionens strategi för informationssäkerhet, samt lägga fram dem som ett förslag för styrelsen för informationssäkerhet,

2. inom alla kommissionens avdelningar bedöma metoderna, processerna och resultaten för hanteringen av it-säkerhetsrisker och regelbundet avlägga rapport om detta inför styrelsen för informationssäkerhet,

3. lägga fram förslag till en löpande strategi för it-säkerhet, som ska granskas och godkännas av styrelsen för informationssäkerhet och därefter antas av förvaltningens styrelse, samt föreslå ett program, med tillhörande planering av projekt och åtgärder för tillämpningen av it-säkerhetsstrategin,

4. övervaka genomförandet av kommissionens strategi för it-säkerhet och regelbundet avlägga rapport inför styrelsen för informationssäkerhet,

5. övervaka it-säkerhetsriskerna och de it-säkerhetsåtgärder som vidtas inom kommunikations- och informationssystemen och regelbundet avlägga rapport om detta inför styrelsen för informationssäkerhet,

6. regelbundet avlägga rapport om genomförandet och efterlevnaden av detta beslut inför styrelsen för informationssäkerhet,

7. efter samråd med generaldirektoratet för personal och säkerhet uppmana systemägare att vidta särskilda it-säkerhetsåtgärder för att minska säkerhetsriskerna för kommissionens kommunikations- och informationssystem,

8. säkerställa att generaldirektoratet för informationsteknik erbjuder it-säkerhetstjänster som gör att systemägare och dataägare kan fullfölja sitt ansvar för säkerheten och följa strategin för it-säkerhet och it-säkerhetsnormerna,

9. förse system- och dataägare med lämplig dokumentation och, i tillämpliga fall, samråda med dem om de it-säkerhetsåtgärder som införts för deras it-tjänster för att underlätta efterlevnaden av strategin för it-säkerhet och stödja systemägare i deras it-riskhantering,

10. anordna regelbundna möten inom nätverket för säkerhetsansvariga för de lokala datasystemen och stödja de säkerhetsansvariga i deras arbete,

11. i samarbete med kommissionens avdelningar fastställa fortbildningsbehoven och samordna fortbildningsprogram om it-säkerhet, samt i nära samarbete med generaldirektoratet för personal utveckla, genomföra och samordna upplysningskampanjer om it-säkerhet,

12. säkerställa att systemägare, dataägare och andra funktioner med ansvar för it-säkerhet inom kommissionens avdelningar görs medvetna om strategin för it-säkerhet,

13. informera generaldirektoratet för personal och säkerhet om specifika hot mot it-säkerheten, incidenter och undantag från kommissionens strategi för it-säkerhet som anmälts av systemägare och som kan få betydande följder för säkerheten inom kommissionen,

14. med avseende på sin roll som intern leverantör av it-tjänster, förse kommissionen med en förteckning över delade it-tjänster som omfattar fastställda säkerhetsnivåer. Detta ska ske genom systematisk bedömning, hantering och övervakning av it-säkerhetsriskerna för genomförandet av säkerhetsåtgärderna i syfte att uppnå den fastställda säkerhetsnivån.

De därmed sammanhängande processerna och ansvaret i detalj ska fastställas närmare i tillämpningsföreskrifterna.

Artikel 8

Kommissionens avdelningar

I fråga om it-säkerheten inom deras avdelningar, ska cheferna för kommissionens avdelningar

1. formellt utse en systemägare, som ska vara tjänsteman eller tillfälligt anställd, för varje kommunikations- och informationssystem, som kommer att vara ansvarig för it-säkerheten inom det kommunikations- och informationssystemet, och formellt utse en dataägare till varje dataset som behandlas i ett kommunikations- och informationssystem, som bör ingå i samma administrativa enhet som ansvarar för uppgifter som omfattas av förordning (EG) nr 45/2001,

2. formellt utse en säkerhetsansvarig för de lokala datasystemen som, oberoende av systemägare och dataägare, kan fullgöra ansvarsuppgifterna, En säkerhetsansvarig för de lokala datasystemen kan utses för en eller flera av kommissionens avdelningar,

3. säkerställa att lämpliga riskbedömningar av it-säkerheten och it-säkerhetsplaner har utarbetats och genomförts,

4. säkerställa att en sammanfattning av it-säkerhetsriskerna och säkerhetsåtgärderna regelbundet rapporteras till generaldirektoratet för informationsteknik,

5. med bistånd av generaldirektoratet för informationsteknik, säkerställa, att lämpliga processer, förfaranden och lösningar införts för att säkerställa effektiv upptäckt, rapportering och lösning av it-säkerhetsincidenter som rör deras kommunikations- och informationssystem,

6. inleda ett nödförfarande i fall av it-säkerhetskriser,

7. ha det yttersta ansvaret för it-säkerheten, vilket även inbegriper systemägarens och dataägarens ansvar,

8. äga de risker som är förenade med deras kommunikations- och informationssystem och dataset,

9. lösa eventuella tvister mellan dataägare och systemägare, och i händelse av fortsatt oenighet ta upp ärendet för lösning i styrelsen för informationssäkerhet,

10. säkerställa att it-säkerhetsplaner och åtgärder för it-säkerheten genomförs och att riskerna hanteras på ett lämpligt sätt.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 9

Systemägare

1. Systemägaren ansvarar för kommunikations- och informationssystemets it-säkerhet och avlägger rapport till avdelningschefen.

2. I fråga om it-säkerheten ska systemägaren

a) säkerställa att kommunikations- och informationssystemet överensstämmer med strategin för it-säkerhet,

b) säkerställa att kommunikations- och informationssystemet är korrekt registrerat i den relevanta förteckningen,

c) i samarbete med dataägarna och i samråd med generaldirektoratet för informationsteknik bedöma it-säkerhetsrisker och avgöra it-säkerhetsbehoven för varje kommunikations- och informationssystem,

d) utarbeta en säkerhetsplan som, i tillämpliga fall, omfattar närmare upplysningar om de bedömda riskerna och alla ytterligare säkerhetsåtgärder som krävs,

e) vidta lämpliga it-säkerhetsåtgärder som står i proportion till de identifierade it-säkerhetsriskerna och följa rekommendationer som godkänts av styrelsen för informationssäkerhet,

f) identifiera eventuella kopplingar till andra kommunikations- och informationssystem eller delade it-tjänster och tillämpa lämpliga säkerhetsåtgärder grundade på de säkerhetsnivåer som föreslagits av dessa kommunikations- och informationssystem eller gemensamma it-tjänster,

g) hantera och övervaka it-säkerhetsrisker,

h) regelbundet avlägga rapport till chefen för kommissionsavdelningen om riskprofilen i deras kommunikations- och informationssystem med avseende på it-säkerhet och rapportera till generaldirektoratet för informationsteknik relaterade risker, riskhanteringåtgärder och vidtagna säkerhetsåtgärder,

i) samråda med den säkerhetsansvarige för de lokala datasystemen och berörd(a) kommissionsavdelning(ar) om aspekter av it-säkerheten,

j) utfärda anvisningar för användare om användningen av kommunikations- och informationssystemet och tillhörande uppgifter samt om det ansvar som åligger användare av kommunikations- och informationssystem,

k) begära tillstånd från generaldirektoratet för personal och säkerhet, i dess egenskap av krypteringsmyndighet, för varje kommunikations- och informationssystem som använder krypteringsteknik,

l) i förväg samråda med kommissionens säkerhetsmyndighet om varje system som behandlar säkerhetsskyddsklassificerade EU-uppgifter,

m) säkerställa att backup-kopior av krypteringsnycklar lagras på ett spärrat konto, Återställande av krypterade uppgifter får ske endast efter godkännande enligt den ram som fastställts av generaldirektoratet för personal och säkerhet.

n) följa eventuella anvisningar från den eller de registeransvariga om skydd av personuppgifter och tillämpningen av dataskyddsbestämmelser på bearbetningen,

o) underrätta generaldirektoratet för informationsteknik om eventuella undantag från kommissionens strategi för it-säkerhet, inbegripet nödvändiga motiveringar,

p) avlägga rapport om eventuella olösliga oenigheter mellan dataägaren och systemägaren till chefen för avdelningen inom kommissionen, i god tid och på lämpligt sätt meddela berörda parter om it-säkerhetsincidenter med hänsyn till dess allvarlighetsgrad på det sätt som om fastställs i artikel 15,

q) i fråga om utlokaliserade system säkerställa att lämpliga it-säkerhetsbestämmelser införs i entreprenadavtalen, och att säkerhetsincidenter på it-området som inträffar i det utlokaliserade kommunikations- och informationssystemet rapporteras i enlighet med artikel 15,

r) för system som tillhandahåller delade it-tjänster, säkerställa att en bestämd skyddsnivå tillhandahålls, klart och tydligt dokumenteras och att säkerhetsåtgärder har vidtagits för att systemen för att uppnå den fasställda säkerhetsnivån,

3. Systemägare kan formellt delegera en del av eller alla sina uppgifter, men de förblir ansvariga för it-säkerheten i sina kommunikations- och informationssystem.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 10

Dataägare

1. Dataägarna ansvarar för it-säkerheten i ett specifikt dataset inför chefen för den avdelning inom kommissionen som är ansvarig för konfidentialitet, integritet och tillgänglighet till dataset.

2. I fråga om detta dataset ska dataägaren

a) säkerställa att alla uppgifter som han eller hon ansvarar för är korrekt klassificerade i enlighet med besluten (EU, Euratom) 2015/443 och (EU, Euratom) 2015/444,

b) definiera säkerhetsbehoven på informationsområdet och underrätta berörda systemägare om dessa behov,

c) delta i riskbedömningen för kommunikations- och informationssystem,

d) till chefen för kommissionens avdelning avlägga rapport om eventuella olösliga oenigheter mellan informationsägaren och systemägaren,

e) vidarebefordra uppgifter om säkerhetsincidenter på it-området på det sätt som föreskrivs i artikel 15.

3. Dataägare kan formellt delegera vissa eller alla av sina uppgifter, men de förblir ansvariga på det sätt som fastställs i denna artikel.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 11

Säkerhetsansvarig för de lokala datasystemen

I fråga om it-säkerheten ska den säkerhetsansvarige för de lokala datasystemen

a) förutseende identifiera och informera systemägare, dataägare och andra funktioner med ansvar för it-säkerhet inom kommissionens avdelning(ar) om strategin för it-säkerhet,

b) upprätta förbindelser i frågor som rör it-säkerheten mellan kommissionens avdelningar och generaldirektoratet för informationsteknik som en del i nätverket för de säkerhetsansvariga för de lokala datasystemen,

c) delta i de regelbundna möten som de säkerhetsansvariga för de lokala datasystemen håller,

d) upprätthålla en överblick över arbetet med att hantera säkerhetsrisker på informationsområdet och över utvecklingen och tillämpningen av säkerhetplanerna för informationssystemet,

e) underrätta dataägarna, systemägarna och cheferna för kommissionens avdelningar om frågor som rör it-säkerheten,

f) samarbeta med generaldirektoratet för informationsteknik för att sprida god praxis och lägga fram förslag till särskilda orienterings- och fortbildningsprogram,

g) avlägga rapport om it-säkerheten, identifiera brister och förbättringar till chefen för kommissionens avdelning(ar).

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 12

Användare

1. I fråga om it-säkerheten ska användarna

a) efterleva strategin för it-säkerhet och de anvisningar som utfärdas av systemägaren om användningen av vart och ett av kommunikations- och informationssystemen,

b) vidarebefordra uppgifter om säkerhetsincidenter på it-området på det sätt som föreskrivs i artikel 15.

2. Användning av kommissionens kommunikations- och informationssystem i strid med strategin för it-säkerhet eller anvisningar utfärdade av systemägaren kan leda till disciplinära förfaranden.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

KAPITEL 3

SÄKERHETSKRAV OCH SKYLDIGHETER

Artikel 13

Tillämpningen av detta beslut

1. Antagandet av tillämpningsföreskrifter för artikel 6, och av tillhörande normer och riktlinjer, kommer att bli föremål för beslut i kommissionen om bemyndigande av den kommissionsledamot som ansvarar för säkerhetsfrågor.

2. Antagandet av alla andra tillämpningsföreskrifter med koppling till detta beslut, och av tillhörande normer och riktlinjer för it-säkerhet som hänger samman därmed, kommer att bli föremål för beslut i kommissionen om bemyndigande av den kommissionsledamot som ansvarar för informationsteknik.

3. Styrelsen för informationssäkerhet ska godkänna tillämpningsföreskrifter, normer och riktlinjer som nämns i punkterna 1 och 2 ovan, innan dessa antas.

Artikel 14

Skyldighet att efterleva bestämmelser

1. Efterlevnaden av de bestämmelser som beskrivs i strategin och normerna för it-säkerhet är obligatorisk.

2. Bristande efterlevnad av säkerhetsstrategin och normerna på it-området kan leda till disciplinära åtgärder i enlighet med fördragen, tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i Europeiska unionen, till kontraktsenliga sanktioner och/eller till rättsliga åtgärder enligt nationella lagar och andra författningar.

3. Generaldirektoratet för informationsteknik ska underrättas om eventuella undantag från strategin för it-säkerhet.

4. Om styrelsen för informationssäkerhet anser att det föreligger en ihållande oacceptabel risk för ett kommunikations- och informationssystem inom kommissionen, ska generaldirektoratet för informationsteknik i samarbete med systemägaren för styrelsen för informationssäkerhet lägga fram förslag till riskreducerande åtgärder för godkännande. Dessa åtgärder kan bland annat omfatta förstärkt övervakning och rapportering, begränsningar och bortkoppling.

5. Styrelsen för informationssäkerhet ska, när så är nödvändigt, kräva tillämpning av de godkända riskreducerande åtgärderna. Styrelsen för informationssäkerhet kan också rekommendera generaldirektören för generaldirektoratet för personal och säkerhet att inleda en administrativ utredning. Generaldirektoratet för informationsteknik ska inför styrelsen för informationssäkerhet avlägga rapport om varje situation där riskreducerande åtgärder vidtas.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

Artikel 15

Hantering av säkerhetsincidenter på it-området

1. Generaldirektoratet för informationsteknik ansvarar för att tillhandahålla den huvudsakliga operativa incidenthanteringsförmågan på it-området inom Europeiska kommissionen.

2. Generaldirektoratet för personal och säkerhet ska, i egenskap av bidragande aktör till incidenthanteringen på it-området,

a) ha tillgång till kortfattad information om alla uppgifter om incidenter och fullständiga uppgifter på begäran,

b) ingå i krishanteringsgrupperna för incidenter som rör it-säkerhet och nödförfaranden i fråga om it-säkerhet,

c) ansvara för kontakterna med brottsbekämpande organ och underrättelsetjänster,

d) utföra kriminalteknisk analys av it-säkerheten i enlighet med artikel 11 i beslut (EU, Euratom) 2015/443,

e) fatta beslut om behovet av att inleda en formell granskning,

f) underrätta generaldirektoratet för informationsteknik om säkerhetsincidenter på it-området som kan utgöra en risk för andra system.

3. Generaldirektoratet för informationssamhället och medier och generaldirektoratet för personal och säkerhet ska regelbundet kommunicera med varandra för att utbyta information och samordna hanteringen av säkerhetsincidenter, i synnerhet alla säkerhetsincidenter på it-området som kan kräva en formell utredning.

4. De samordningstjänster som tillhandahålls av incidenthanteringsorganisationen för EU:s institutioner och byråer (även kallat *Cert-EU*) kan i tillämpliga fall användas till stöd för incidenthanteringen och i fråga om kunskapsutbyte med andra av EU-institutioner och organ som kan vara berörda.

5. Systemägare som berörs av en säkerhetsincident på it-området ska

a) omedelbart underrätta sin avdelningschef vid kommissionen, generaldirektoratet för informationsteknik, generaldirektoratet för personal, den säkerhetsansvarige för de lokala datasystemen och, i tillämpliga fall, dataägaren om allvarliga säkerhetsincidenter på it-området, särskilt om dessa inbegriper brott mot sekretessen,

b) samarbeta och följa instruktionerna från kommissionens behöriga avdelningar om underrättelse om incidenter, insatser och återställande.

6. Användarna ska inom rimlig tid avlägga rapport till berörd it-stödtjänst om alla faktiska eller misstänkta säkerhetsincidenter på it-området.

7. Dataägare ska inom rimlig tid avlägga rapport till berörd incidenthanteringsgrupp om alla faktiska eller misstänkta säkerhetsincidenter på it-området.

8. Generaldirektoratet för informationsteknik, med stöd från andra bidragande parter, ansvarar för hanteringen av säkerhetsincidenter på it-området som upptäcks i anslutning till de kommunikations- och informationssystem inom kommissionen som inte utlokaliserats.

9. Generaldirektoratet för informationsteknik ska säkerställa att säkerhetsincidenter på it-området rapporteras till berörda avdelningar inom kommissionen, berörd säkerhetsansvarig för de lokala datasystemen och, i tillämpliga fall, Cert-EU på grundval av principen om behovsenlig underrättelse.

10. Generaldirektoratet för informationsteknik ska regelbundet avlägga rapport för styrelsen för informationssäkerhet om allvarliga säkerhetsincidenter på it-området som påverkar kommissionens kommunikations- och informationssystem.

11. De berörda säkerhetsansvariga för de lokala datasystemen ska på begäran ges tillgång till uppgifter om incidenter på it-området som rör kommunikations- och informationssystemen inom kommissionens avdelningar.

12. Om en större säkerhetsincident inträffar, ska generaldirektoratet för informationsteknik fungera som kontaktpunkt för hanteringen av krissituationer genom att samordna krishanteringsgrupperna för säkerhetsincidenter på it-området.

13. I nödlägen kan generaldirektören för generaldirektoratet för informationsteknik fatta beslut om att inleda ett nödförfarande för it-säkerheten. Generaldirektoratet för informationsteknik ska utarbeta förfaranden för nödlägen som ska godkännas av styrelsen för informationssäkerhet.

14. Generaldirektoratet för informationsteknik ska inför styrelsen för informationssäkerhet och cheferna för de avdelningar inom kommissionen som berörs avlägga rapport om genomförandet av nödförfaranden.

De processer som rör dessa ansvarsuppdrag och uppgifter ska beskrivas närmare i tillämpningsföreskrifterna.

KAPITEL 4

SLUTBESTÄMMELSER

Artikel 16

Öppenhet

Kommissionens tjänstemän och övriga personer som berörs ska informeras om detta beslut, som ska offentliggöras i *Europeiska unionens officiella tidning*.

Artikel 17

Förhållande till andra akter

Bestämmelserna i detta beslut ska inte påverka tillämpningen av beslut (EU, Euratom) 2015/443, beslut (EU, Euratom) 2015/444, förordning (EG) nr 45/2001, Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([1]), kommissionens beslut 2002/47/EG, EKSG, Euratom ([2]), Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 ([3]) och beslut 1999/352/EG, EKSG, Euratom.

Artikel 18

Upphävande och övergångsbestämmelser

Beslut K(2006) 3602 av den 16 augusti 2006 ska upphöra att gälla.

De tillämpningsföreskrifter och it-säkerhetsnormer som antagits enligt artikel 10 i beslut K(2006) 3602 ska, såvida de inte strider mot detta beslut, fortsatt gälla tills de ersätts av de tillämpningsföreskrifter och normer som kommer att antas enligt artikel 13 i detta beslut. Varje hänvisning till artikel 10 i beslut K(2006) 3602 ska förstås som en hänvisning till artikel 13 i det här beslutet.

Artikel 19

Ikraftträdande

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 10 januari 2017.

På kommissionens vägnar
Jean-Claude JUNCKER
Ordförande

([1]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).
([2]) Kommissionens beslut 2002/47/EG, EKSG, Euratom av den 23 januari 2002 om ändring av dess arbetsordning (EUT L 21, 24.1.2002, s. 23).
([3]) Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999 (EUT L 248, 18.9.2013, s. 1).