KOMMISSIONENS BESLUT (EU, Euratom) 2018/559

av den 6 april 2018

om tillämpningsföreskrifter för artikel 6 i beslut (EU, Euratom) 2017/46 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,

med beaktande av kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem ([1]), särskilt artikel 6, och

av följande skäl:

(1) Antagandet av beslut (EU, Euratom) 2017/46 gör att kommissionen behöver se över, aktualisera och konsolidera tillämpningsföreskrifterna till det upphävda kommissionens beslut C(2006) 3602 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem.

(2) Kommissionsledamöten med ansvar för säkerhet har i enlighet med den interna arbetsordningen bemyndigats att fastställa tillämpningsföreskrifter i enlighet med artikel 13 i beslut (EU, Euratom) 2017/46 ([2]).

(3) Tillämpningsföreskrifterna till beslut C(2006) 3602 bör därför upphävas.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. Det här beslutets syfte och tillämpningsområde anges i artikel 1 i beslut (EU, Euratom) 2017/46.

2. Bestämmelserna i det här beslutet är tillämpliga på alla kommunikations- och informationssystem. De ansvarsområden som fastställs i det här beslutet ska dock inte tillämpas på de kommunikations- och informationssystem som används för att hantera säkerhetsskyddsklassificerade EU-uppgifter. De tillämpliga ansvarsområdena för system ska fastställas av systemägaren och kommissionens säkerhetsmyndighet i enlighet med kommissionens beslut (EU, Euratom) 2015/444 ([3]).

3. Kapitel 2 i det här beslutet innehåller en genomgång av hur it-säkerhetens organisation och ansvarsområden praktiskt ska genomföras. Kapitel 3 i det här beslutet innehåller en genomgång av de processer som rör artikel 6 i beslut (EU, Euratom) 2017/46.

Artikel 2

Definitioner

Definitionerna i artikel 2 i beslut (EU, Euratom) 2017/46 är tillämpliga på det här beslutet. I detta beslut gäller därutöver följande definitioner:

1. *kryptogodkännande myndighet* (CAA): en funktion som utförs av kommissionens säkerhetsmyndighet och som ingår i ansvarsområdet för generaldirektören för personal och säkerhet.

([1]) EUT L 6, 11.1.2017, s. 40.
([2]) Kommissionens beslut C(2017) 7428 final av den 8 november 2017, vilka ger behörighet att anta tillämpningsföreskrifter, normer och riktlinjer för säkerheten i Europeiska kommissionens kommunikations- och informationssystem.
([3]) 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).

2. *extern nätverksanslutning*: alla anslutningar för elektronisk kommunikation mellan kommissionens interna nätverk och andra nätverk, även internet. Denna definition omfattar inte externa nätverk som tillhandahålls enligt avtal för att ingå i kommissionens interna nätverk.

3. *nyckeldeponering*: ett förfarande för att lagra backup-kopior av krypteringsnycklar hos en eller flera separata parter med säkerställd åtskillnad mellan funktioner, så att nycklarna kan återställas om driftsexemplaret går förlorat. Nycklar kan separeras i två eller flera delar som lagras var för sig hos olika parter för att se till att ingen enskild har tillgång till hela nyckeln.

4. *RASCI*: en förkortning för fördelningen av olika ansvarsområden enligt följande:

   a) *ansvarig* (R): person med skyldighet att agera och fatta beslut för att uppnå nödvändiga resultat.

   b) *ansvarsskyldig* (A): person med ansvar för insatser, beslut och resultat.

   c) *stöd* (S): person med skyldighet att arbeta tillsammans med den ansvariga för att fullgöra en uppgift.

   d) *hörd* (C): person med vilken samråd hållits för rådgivning eller yttrande.

   e) *informerad* (I): person som hålls uppdaterad med relevant information.

KAPITEL 2

ORGANISATION OCH ANSVAR

Artikel 3

Roller och ansvar

De uppgifter och ansvarsområden som avser artiklarna 4–8 i det här beslutet definieras i bilagan i enlighet med RASCI-modellen.

Artikel 4

Förenlighet med kommissionens strategi för it-säkerhet

1. Generaldirektoratet för personal och säkerhet ska se över kommissionens strategi för it-säkerhet och därmed sammanhängande normer och riktlinjer för att säkerställa att de är förenliga med kommissionens allmänna säkerhetspolitik, särskilt kommissionens beslut (EU, Euratom) 2015/443 ([1]) och beslut (EU, Euratom) 2015/444.

2. På begäran från andra av kommissionens avdelningar får generaldirektoratet för personal och säkerhet se över sin strategi för it-säkerhet eller andra handlingar som avser it-säkerhet för att säkerställa att de är förenliga med kommissionens strategi för it-säkerhet. Chefen för den berörda kommissionsavdelningen ska säkerställa att eventuella inkonsekvenser åtgärdas.

3. Inom ramen för sitt ansvar för informationssäkerheten ska generaldirektoratet för personal och säkerhet samarbeta med generaldirektoratet för informationsteknik för att säkerställa att förfarandena för it-säkerhet tar full hänsyn till den klassificering och de säkerhetsprinciper som fastställs i beslut (EU, Euratom) 2015/443, särskilt artiklarna 3 och 9.

KAPITEL 3

FÖRFARANDEN FÖR IT-SÄKERHET

Artikel 5

Krypteringsteknik

1. Användningen av krypteringsteknik för att skydda säkerhetsskyddsklassificerade EU-uppgifter ska vara förenlig med beslut (EU, Euratom) 2015/444.

2. Beslut att använda krypteringsteknik för att skydda andra uppgifter än säkerhetsskyddsklassificerade EU-uppgifter ska fattas av varje kommunikations- och informationssystems systemägare med hänsyn både till de risker som ska avvärjas med hjälp av kryptering och till de risker tekniken medför.

3. Förhandstillstånd från den kryptogodkännande myndigheten krävs för all användning av krypteringsteknik, om inte kryptering används endast för att skydda konfidentialiteten hos andra uppgifter än säkerhetsskyddsklassificerade EU-uppgifter vid överföring med hjälp av vanliga kommunikationsprotokoll för nätverk.

([1]) Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41).

4. Med undantag för det fall som nämns i punkt 3 i denna artikel ska kommissionens avdelningar säkerställa att backup-kopior av krypteringsnycklar deponeras på ett sådant sätt att sparade uppgifter kan återställas om krypteringsnyckeln inte är tillgänglig. Återställning av krypterade uppgifter med hjälp av backup-kopior av krypteringsnycklar får bara göras när detta är tillåtet enligt de normer som fastställts av den kryptogodkännande myndigheten.

5. Begäran om godkännande av användning av krypteringsteknik ska formellt dokumenteras och innehålla uppgifter om kommunikations- och informationssystemet och de uppgifter som ska skyddas, den teknik som ska användas och därmed sammanhängande operativa säkerhetsförfaranden. Begäran om godkännande ska undertecknas av systemägaren.

6. Begäran om godkännande av användning av krypteringsteknik ska utvärderas av den kryptogodkännande myndigheten i enlighet med offentliggjorda normer och krav.

Artikel 6

Inspektioner av it-säkerhet

1. Generaldirektoratet för personal och säkerhet ska utföra inspektioner av it-säkerheten för att kontrollera om säkerhetsåtgärder på it-området är förenliga med kommissionens strategi för it-säkerhet och verifiera kontrollåtgärdernas integritet.

2. Generaldirektoratet för personal och säkerhet får utföra inspektioner av it-säkerheten

a) på eget initiativ,

b) på begäran från styrelsen för informationssäkerhet,

c) på begäran från en systemägare,

d) med anledning av en säkerhetsincident, eller

e) med anledning av att man identifierat hög risk för ett visst system.

3. Dataägare får begära inspektion av it-säkerheten innan de lagrar sina uppgifter i ett kommunikations- och informationssystem.

4. Utfallet av inspektionerna ska dokumenteras i en formell rapport till systemägaren med kopia till den säkerhetsansvariga för de lokala datasystemen; rapporten ska omfatta resultat och rekommendationer om hur kommunikations- och informationssystemets förenlighet med strategin för it-säkerhet kan förbättras. Generaldirektoratet för personal och säkerhet ska rapportera viktiga frågor och rekommendationer till styrelsen för informationssäkerhet.

5. Generaldirektoratet för personal och säkerhet ska övervaka hur rekommendationerna genomförs.

6. När det är lämpligt ska inspektionerna av it-säkerheten omfatta inspektioner av tjänster, lokaler och utrustning som tillhandahålls systemägaren, både med avseende på interna och externa tjänsteleverantörer.

Artikel 7

Tillgång från externa nätverk

1. Generaldirektoratet för personal och säkerhet ska föreskriva bestämmelser i en norm för beviljande av tillgång till kommissionens kommunikations- och informationssystem från externa nätverk.

2. Bestämmelserna ska skilja på olika typer av externa nätverksanslutningar och fastställa lämpliga säkerhetsbestämmelser för varje typ av anslutning, inbegripet huruvida det krävs förhandstillstånd för anslutningen från behörig myndighet i enlighet med punkt 4 i denna artikel.

3. Vid behov ska tillstånd beviljas efter en formell ansöknings- och godkännandeprocess. Godkännandet ska gälla för viss tid och måste erhållas innan anslutningen aktiveras.

4. Generaldirektoratet för personal och säkerhet ska ha det övergripande ansvaret för att bevilja ansökningar men får själv delegera ansvaret för att bevilja vissa typer av anslutningar i enlighet med artikel 17.3 i beslut (EU, Euratom) 2015/443 på de villkor som anges i punkt 8.

5. Den tillståndsbeviljande instansen får ställa ytterligare säkerhetskrav som villkor för godkännande, för att skydda kommissionens kommunikations- och informationssystem och nätverk från risken för obehörig åtkomst eller andra säkerhetsintrång.

6. Generaldirektoratet för informationsteknik är den normala tillhandahållaren av nätverkstjänster för kommissionen. Övriga kommissionsavdelningar som driver nätverk som inte tillhandahålls av generaldirektoratet för informationsteknik ska först inhämta tillstånd från styrelsen för informationssäkerhet. Kommissionens avdelningar ska dokumentera ansökans affärsmässiga berättigande och visa att kontrollerna av nätverket är tillräckliga för att uppfylla kraven på kontroll av inkommande och utgående informationsflöden.

7. Kommunikations- och informationssystemets systemägare ska fastställa säkerhetskrav för extern tillgång till kommunikations- och informationssystemet och säkerställa genomförandet av lämpliga åtgärder för att skydda säkerheten, med hjälp av den säkerhetsansvariga för de lokala datasystemen.

8. De säkerhetsåtgärder som vidtas för extern nätverksanslutning ska bygga på principerna för behovsenlig behörighet och begränsad behörighet, som säkerställer att enskilda bara får de upplysningar och den åtkomsträtt de behöver för sin tjänsteutövning vid kommissionen.

9. Alla externa nätverksanslutningar ska filtreras och övervakas för att spåra potentiella säkerhetsöverträdelser.

10. När anslutning upprättas för att möjliggöra utlokalisering av ett kommunikations- och informationssystem ska tillståndet vara avhängigt av fullständigt utförande av det förfarande som beskrivs i artikel 8.

Artikel 8

Utlokalisering av kommunikations- och informationssystem

1. I detta beslut avses med utlokalisering av ett kommunikations- och informationssystem att systemet tillhandahålls inom ramen för ett avtal med en extern uppdragstagare och att kommunikations- och informationssystemet inte är inhyst i kommissionens lokaler. Detta omfattar även utlokalisering av enskilda eller multipla kommunikations- och informationssystem eller andra it-tjänster, datacentraler som inte är inhysta i kommissonens lokaler och externa tjänsteleverantörers hantering av kommissionens uppgifter.

2. Utlokalisering av kommunikations- och informationssystem ska ta hänsyn till de hanterade uppgifternas känslighet eller klassificering enligt följande:

a) Kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska ackrediteras i enlighet med beslut (EU, Euratom) 2015/444 och kommissionens myndighet för säkerhetsackreditering ska höras i förväg. System som hanterar säkerhetsskyddsklassificerade EU-uppgifter får inte utlokaliseras.

b) Systemägare till kommunikations- och informationssystem som hanterar andra uppgifter än säkerhetsskyddsklassificerade EU-uppgifter ska vidta proportionella säkerhetsåtgärder för att fullgöra de tillämpliga rättsliga kraven eller ta hänsyn till uppgifternas känslighet, med hänsyn till riskerna med utlokalisering. Generaldirektoratet för personal och säkerhet får ställa ytterligare krav.

c) Utlokaliserade utvecklingsprojekt ska ta hänsyn till känsligheten i den utvecklade koden och eventuella testuppgifter som använts vid utvecklingen.

3. Följande principer ska tillämpas på utlokalisering av kommunikations- och informationssystem, utöver de som fastställs i artikel 3 i beslut (EU, Euratom) 2017/46:

a) Utlokaliseringen ska utformas så att den inte leder till beroende av vissa leverantörer.

b) Säkerhetsförfarandena vid utlokalisering ska minska den externa personalens möjligheter att få åtkomst till eller ändra kommissionens data.

c) Den externa personal som har tillgång till ett utlokaliserat kommunikations- och informationssystem ska skriva på sekretessavtal.

d) I förteckningen över kommunikations- och informationssystem ska det anges att systemet är utlokaliserat.

4. Systemägaren ska tillsammans med dataägaren göra följande:

a) Bedöma och dokumentera riskerna med utlokalisering.

b) Fastställa relevanta säkerhetskrav.

c) Höra systemägare till övriga anslutna kommunikations- och informationssystem för att säkerställa att deras säkerhetskrav inkluderas.

d) Säkerställa att lämpliga säkerhetskrav och rättigheter tas upp i utlokaliseringsavtalet.

e) Uppfylla alla andra krav som ställs i de närmare normer som avses i punkt 8 i denna artikel.

Dessa åtgärder ska vidtas innan avtal eller andra överenskommelser om utlokalisering av ett eller flera kommunikations- och informationssystem undertecknas.

5. Systemägarna ska hantera riskerna med utlokalisering under kommunikations- och informationssystemets hela livstid för att uppfylla de fastställda säkerhetskraven.

6. Systemägarna ska säkerställa att externa uppdragstagare åläggs att omedelbart underrätta kommissionen om alla it-relaterade säkerhetsincidenter som påverkar något av kommissionen utlokaliserat kommunikations- och informationssystem.

7. Systemägaren är ansvarig för att säkerställa att kommunikations- och informationssystemet, utlokaliseringsavtalet och säkerhetsförfarandena är förenliga med kommissionens bestämmelser om informationssäkerhet och it-säkerhet.

8. Generaldirektoratet för personal och säkerhet ska fastställa närmare normer för det ansvar och den verksamhet som avses i punkterna 1–7 i enlighet med artikel 10 nedan.

KAPITEL 4

ÖVRIGA BESTÄMMELSER OCH SLUTBESTÄMMELSER

Artikel 9

Öppenhet

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

Artikel 10

Normer

1. Bestämmelserna i beslutet ska vid behov preciseras närmare i normer och/eller riktlinjer som ska antas i enlighet med beslut (EU, Euratom) 2017/46 och beslut C(2017)7428. Normer och riktlinjer för it-säkerhet ska närmare precisera de här tillämpningsföreskrifterna och beslut (EU, Euratom) 2017/46 med avseende på särskilda säkerhetsområden i enlighet med ISO 27001:2013 Bilaga A. Dessa normer och riktlinjer bygger på bästa branschpraxis och har valts ut för att passa kommissionens it-miljö.

2. Normer ska vid behov utvecklas i enlighet med ISO 27001:2013 Bilaga A på följande områden:

1. Organisation av informationssäkerhet.
2. Personalsäkerhet.
3. Förvaltning av tillgångar.
4. Åtkomstskontroll.
5. Kryptering.
6. Fysisk säkerhet och säkerhet i it-miljön.
7. Driftsäkerhet.
8. Kommunikationssäkerhet.
9. Förvärv, utveckling och underhåll av system.
10. Leverantörsförbindelser.
11. Hantering av informationssäkerhetsrelaterade händelser.
12. Informationssäkerhetsaspekter på hantering av driftskontinuitet.
13. Överensstämmelse.

3. Styrelsen för informationssäkerhet ska godkänna de normer som nämns i punkterna 1 och 2 i denna artikel, innan de antas.

4. Härmed återkallas tillämpningsföreskrifterna till beslut C(2006) 3602 avseende tillämpningsområdet för detta beslut.

5. De normer och riktlinjer som antagits enligt beslut C(2006) 3602 av den 16 augusti 2006 ska, såvida de inte strider mot de här tillämpningsföreskrifterna, fortsatt gälla tills de återkallas eller ersätts av de normer eller riktlinjer som ska antas enligt artikel 13 i beslut (EU, Euratom) 2017/46.

Artikel 11

Ikraftträdande

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

Utfärdat i Bryssel den 6 april 2018.

På kommissionens vägnar
För ordföranden
Günther OETTINGER
Ledamot av kommissionen

BILAGA

ROLLER OCH ANSVAR

RASCI-modellen distribuerar roller och ansvar med hjälp av följande förkortningar:

a) R – Ansvarig

b) A – Ansvarsskyldig

c) S – Stöd

d) C – Hörd

e) I – Informerad

Process \ Roll	Styrelsen för informationssäkerhet	Personalavdelning (DS)	Kommissionens avdelningar	Systemägare	Dataägare	Säkerhetsansvarig för de lokala datasystemen	Generaldirektoratet för informationsteknik	Uppdragstagare
Förenlighet med kommissionens strategi för it-säkerhet		**R/A**	**S**				**S**	
Krypteringsteknik		**C**	**A**	**R**	**I**	**C**		
Inspektioner av it-säkerhet	**I**	**A/R**		**S**	**I**	**I**	**S**	
Tillgång från externa nätverk	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Utlokalisering av kommunikations- och informationssystem		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Styrelsen för informationssäkerhet hörs avseende driften av interna nätverk vid andra kommissionsavdelningar än generaldirektoratet för informationsteknik

[2] Systemägaren av ett utlokaliserat kommunikations- och informationssystem ska vara ansvarig och systemägaren till alla andra kommunikations- och informationssystem till vilka ett utlokaliserat kommunikations- och informationssystem är anslutet ska höras.