KOMMISSIONENS BESLUT (EU) 2022/640

av den 7 april 2022

om genomförandebestämmelser rörande roller och ansvarsområden för huvudaktörerna på säkerhetsområdet

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

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

med beaktande av kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen ([1]),

med beaktande av kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter ([2]),

av följande skäl:

(1) Besluten (EU, Euratom) 2015/443 och (EU, Euratom) 2015/444 är tillämpliga på alla kommissionens avdelningar och lokaler.

(2) Vid behov ska tillämpningsföreskrifter för att komplettera eller understödja beslut (EU, Euratom) 2015/444 antas i enlighet med artikel 60 i det beslutet.

(3) Säkerhetsåtgärder för att skydda säkerhetsskyddsklassificerade EU-uppgifter under hela deras livscykel bör särskilt motsvara deras säkerhetsskyddsklassificeringsnivå.

(4) Säkerhetsåtgärder för att skydda kommissionens kommunikations- och informationssystem fastställs i kommissionens beslut (EU, Euratom) 2017/46 ([3]), särskilt artikel 3 om principerna för it-säkerheten inom kommissionen och artikel 9 om systemägare.

(5) Syftet med genomförandebestämmelserna rörande roller och ansvarsområden för huvudaktörerna på säkerhetsområdet är att ge vägledning om de förutsättningar och uppgifter som fastställs med avseende på dessa roller i besluten (EU, Euratom) 2015/443 och (EU, Euratom) 2015/444.

(6) I artikel 36.7 i beslut (EU, Euratom) 2015/444 fastställs ett antal ytterligare säkerhetsrelaterade funktioner som ska åläggas kommissionens säkerhetsmyndighet. De uppgifter som hör samman med dessa funktioner fastställs i detta beslut.

(7) Lokalt säkerhetsansvariga och kontrolltjänstemän för registreringsenheter har särskilt ansvar för att skydda säkerhetsskyddsklassificerade EU-uppgifter inom sina avdelningar i enlighet med beslut (EU, Euratom) 2015/444.

(8) Den 4 maj 2016 antog kommissionen ett beslut ([4]) om bemyndigande av den ledamot av kommissionen som ansvarar för säkerhetsfrågor för att, på kommissionens vägnar och på dess ansvar, anta de tillämpningsföreskrifter som avses i artikel 60 i beslut (EU, Euratom) 2015/444; därefter antog kommissionsledamoten med ansvar för säkerhetsfrågor, på kommissionens vägnar och på dess ansvar, ett beslut ([5]) den 13 april 2021 om att vidaredelegera dessa tillämpningsföreskrifter till generaldirektören för generaldirektoratet för personal och säkerhet.

([1]) EUT L 72, 17.3.2015, s. 41.
([2]) EUT L 72, 17.3.2015, s. 53.
([3]) Kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem (EUT L 6, 11.1.2017, s. 40).
([4]) Kommissionens beslut C(2016) 2797 final av den 4 maj 2016 om bemyndigande avseende säkerhet.
([5]) Kommissionens beslut C(2021) 2684 final av den 13 april 2021 om beviljande av vidaredelegering av befogenheter enligt kommissionens beslut C(2016) 2797 om bemyndigande avseende säkerhet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

Allmänna bestämmelser

Artikel 1

Innehåll och tillämpningsområde

1. I detta beslut fastställs roller och ansvarsområden för de huvudaktörer på säkerhetsområdet som ansvarar för skyddet av säkerhetsskyddsklassificerade EU-uppgifter inom kommissionen i enlighet med besluten (EU, Euratom) 2015/443 och (EU, Euratom) 2015/444.

2. Detta beslut ska tillämpas på alla kommissionens avdelningar och i alla kommissionslokaler.

KAPITEL 2

Generaldirektoratet för personal och säkerhet

Artikel 2

Kommissionens säkerhetsmyndighet

1. Direktören för direktoratet för säkerhet vid generaldirektoratet för personal och säkerhet ska vara kommissionens säkerhetsmyndighet i den mening som avses i artikel 7 i beslut (EU, Euratom) 2015/444.

2. Kommissionens säkerhetsmyndighet ska utföra sina uppgifter på följande områden enligt beslut (EU, Euratom) 2015/444, i enlighet med artiklarna 3–7 i det här beslutet:

a) Personalsäkerhet.

b) Fysisk säkerhet.

c) Hantering av säkerhetsskyddsklassificerade EU-uppgifter.

d) Ackreditering av alla kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter.

e) Industrisäkerhet.

f) Utbyte av säkerhetsskyddsklassificerade uppgifter.

3. Kommissionens säkerhetsmyndighet ska tillhandahålla obligatorisk utbildning för de lokalt säkerhetsansvariga, ställföreträdande lokalt säkerhetsansvariga, kontrolltjänstemän för registreringsenheter (*kontrolltjänstemän*) och ställföreträdande kontrolltjänstemän för registreringsenheter om deras ansvarsområden och uppgifter.

Artikel 3

Myndighet för informationssäkring

Myndigheten för informationssäkring ska ansvara för följande verksamhet i samband med skyddet av säkerhetsskyddsklassificerade EU-uppgifter:

a) Utveckla säkerhetsstrategier och säkerhetsriktlinjer för informationssäkring och övervaka deras ändamålsenlighet och relevans.

b) Skydda och administrera teknisk information som rör kryptoprodukter.

c) Säkerställa, när så är lämpligt, att åtgärderna för informationssäkring är förenliga med kommissionens strategier för säkerhet och upphandling.

d) Säkerställa att kryptoprodukter väljs ut i överensstämmelse med de strategier som gäller för deras lämplighet och urval.

e) Samråda med systemägare, systemleverantörer, aktörer på säkerhetsområdet och företrädare för användare när det gäller säkerhetsstrategier och säkerhetsriktlinjer för informationssäkring.

Artikel 4

Myndighet för säkerhetsackreditering

1. Kommissionens säkerhetsmyndighet ska ansvara för ackreditering av säkrade utrymmen som uppfyller kraven i artikel 18 i beslut 2015/444 och kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade EU-uppgifter.

2. Kommissionens avdelningar ska samråda med myndigheten för säkerhetsackreditering i samordning med sina lokalt säkerhetsansvariga och, när så är lämpligt, sina säkerhetsansvariga för de lokala datasystemen när en avdelning har för avsikt att

a) bygga ett säkrat utrymme,

b) införa ett kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade EU-uppgifter,

c) installera all annan utrustning för hantering av säkerhetsskyddsklassificerade uppgifter, inbegripet anslutningar till tredje parts kommunikations- och informationssystem.

Myndigheten för säkerhetsackreditering ska ge råd om denna verksamhet under såväl planeringsprocessen som byggnads- eller utvecklingsprocessen.

3. Säkerhetsskyddsklassificerade EU-uppgifter får inte hanteras i ett säkrat utrymme eller ett kommunikations- och informationssystem förrän myndigheten för säkerhetsackreditering har utfärdat en ackreditering på lämplig säkerhetsskyddsklassificeringsnivå.

4. Kraven för ackreditering av ett säkrat utrymme ska omfatta följande:

a) Godkännande av planerna för det säkrade utrymmet.

b) Godkännande av alla kontrakt för arbeten som utförs av externa uppdragstagare, med beaktande av bestämmelserna om industrisäkerhet, t.ex. eventuella krav på säkerhetsgodkännande för uppdragstagarna och deras personal.

c) Tillgång till alla nödvändiga försäkringar och intyg om överensstämmelse.

d) En fysisk inspektion av det säkrade utrymmet för att kontrollera att byggnadsmaterial och byggnadsmetoder, tillträdeskontroller, säkerhetsutrustning och annat material uppfyller de krav som utfärdas av kommissionens säkerhetsmyndighet.

e) Validering av motåtgärder mot elektromagnetisk strålning för alla tekniskt säkrade utrymmen.

f) Godkännande av säkra driftsmetoder (SecOPs) för det säkrade utrymmet.

5. Kraven för ackreditering av ett kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska omfatta följande:

a) Utarbetande av en ackrediteringsstrategi för systemet.

b) Validering av säkerhetsplanen för kommunikations- och informationssystemet, på grundval av en riskhanteringsstrategi.

c) Validering av de säkra driftsmetoderna för kommunikations- och informationssystemen.

d) Validering av all annan säkerhetsdokumentation som krävs, enligt vad som fastställts av myndigheten för säkerhetsackreditering.

e) Godkännande av all användning av krypteringsteknik.

f) Validering av motåtgärder mot elektromagnetisk strålning för ett kommunikations- och informationssystem som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

g) En inspektion av kommunikations- och informationssystemet för att kontrollera att de dokumenterade säkerhetsåtgärderna genomförs korrekt.

6. Efter det att kraven för ackreditering har uppfyllts ska myndigheten för säkerhetsackreditering utfärda ett formellt tillstånd för hantering av säkerhetsskyddsklassificerade EU-uppgifter i det säkrade utrymmet eller kommunikations- och informationssystemet, upp till en angiven högsta säkerhetsskyddsklassificeringsnivå och upp till fem år, beroende på säkerhetsskyddsklassificeringsnivåerna för de EU-uppgifter som hanteras och de risker som föreligger.

7. I fall av en anmälan av en överträdelse av säkerhetsbestämmelserna eller en betydande ändring av utformningen av eller säkerhetsåtgärderna för ett säkrat utrymme eller ett kommunikations- och informationssystem ska myndigheten för säkerhetsackreditering se över och får vid behov återkalla tillståndet att hantera säkerhetsskyddsklassificerade EU-uppgifter till dess att eventuella identifierade problem har lösts.

Artikel 5

Tempestmyndighet

1. För att skydda kommunikations- och informationssystem som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska tempestsäkerhetsåtgärder genomföras, och dessa får även genomföras med avseende på uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

2. Tempestmyndigheten ansvarar för att godkänna de åtgärder som genomförts för skydd mot röjande av säkerhetsskyddsklassificerade EU-uppgifter genom oavsiktliga elektroniska läckor.

3. På begäran av en ägare av ett kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska tempestmyndigheten utfärda specifikationer för tempestsäkerhetsåtgärder som är lämpliga med tanke på uppgifternas säkerhetsskyddsklassificeringsnivå.

4. Tempestmyndigheten ska utföra teknisk testning under ackrediteringen av säkrade utrymmen och kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIAL UE/EU CONFIDENTIAL eller högre och, efter godkänd testning, utfärda ett tempestcertifikat.

5. I ett tempestcertifikat ska minst följande anges:

a) Testdatum.

b) En beskrivning av tempestsäkerhetsåtgärderna, med ritningar av lokalerna.

c) Certifikatets sista giltighetsdag.

d) Eventuella ändringar som innebär att certifieringen blir ogiltig.

e) Underskrift av tempestmyndigheten.

6. En lokalt säkerhetsansvarig eller en mötesarrangör som, i samordning med den lokalt säkerhetsansvarige, ansvarar för att anordna ett säkerhetsskyddsklassificerat möte, får begära att tempestmyndigheten utför testning av möteslokaler för att säkerställa att de är tekniskt säkrade.

Artikel 6

Kryptogodkännande myndighet

1. Den kryptogodkännande myndigheten ska ansvara för att godkänna användningen av krypteringsteknik.

2. Den kryptogodkännande myndigheten ska utfärda riktlinjer om kraven för användning och godkännande av krypteringsteknik.

3. Den kryptogodkännande myndigheten ska godkänna användningen av krypteringslösningar på grundval av en begäran från systemägaren. Godkännandet ska grundas på en tillfredsställande utvärdering av åtminstone följande:

a) Säkerhetsbehoven för den information som ska skyddas.

b) En översikt över de kommunikations- och informationssystem som ingår i lösningen.

c) En bedömning av de inneboende och kvarstående riskerna.

d) En beskrivning av den föreslagna lösningen.

e) De säkra driftsmetoderna för krypteringslösningen.

4. Den kryptogodkännande myndigheten ska föra ett register över godkända krypteringslösningar.

Artikel 7

Kryptodistribueringsmyndighet

1. Kryptodistribueringsmyndigheten ska ansvara för att distribuera kryptoprodukter som används för att skydda säkerhetsskyddsklassificerade EU-uppgifter (främst krypteringsutrustning, krypteringsnycklar, certifikat och tillhörande autentiseringsfunktioner) till följande:

a) Användare eller avdelningar inom kommissionen, för kommunikations- och informationssystem som förvaltas av externa parter.

b) Användare eller organisationer utanför kommissionen, för kommunikations- och informationssystem som förvaltas av kommissionen.

2. Kryptodistribueringsmyndigheten får delegera distributionen av kryptoprodukter för tredje part till andra avdelningar i enlighet med artikel 17.3 i beslut 2015/443.

3. Kryptodistribueringsmyndigheten ska säkerställa att alla kryptoprodukter sänds via säkra kanaler som skyddar mot och ger bevis på eventuell manipulering, i enlighet med de säkerhetsbestämmelser som gäller för säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som skyddas av dessa kryptoprodukter.

4. Kryptodistribueringsmyndigheten ska ge vägledning till den lokalt säkerhetsansvarige och, i förekommande fall, till den säkerhetsansvarige för de lokala datasystemen vid varje avdelning inom kommissionen som deltar i produktionen, distributionen eller användningen av kryptoprodukterna.

5. Kryptodistribueringsmyndigheten ska säkerställa att lämpliga säkra driftsmetoder inrättas för distribueringsprocessen.

KAPITEL 3

Kommissionens avdelningar

Artikel 8

Avdelningschefer

1. Varje avdelningschef ska utnämna följande:

a) En lokalt säkerhetsansvarig och, när så är lämpligt, en eller flera ställföreträdare, för avdelningen eller kansliet.

b) En kontrolltjänsteman för registreringsenheten och, när så är lämpligt, en eller flera ställföreträdare, för varje avdelning som upprätthåller en registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter.

c) En ägare av varje kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter.

2. Avdelningschefen ska begära godkännande av direktören för direktoratet för säkerhet vid generaldirektoratet för personal och säkerhet före utnämningen av lokalt säkerhetsansvariga, ställföreträdande lokalt säkerhetsansvariga, kontrolltjänstemän och ställföreträdande kontrolltjänstemän för registreringsenheten.

3. Avdelningschefen ska i samråd med den lokalt säkerhetsansvarige fastställa alla tjänster som kräver säkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter. Sökande till sådana tjänster ska under rekryteringsprocessen informeras om kravet på säkerhetsgodkännande.

4. Chefen för en avdelning som innehar säkerhetsskyddsklassificerade EU-uppgifter ska, när så är nödvändigt, ansvara för aktivering av planer för förstöring och evakuering i en nödsituation. Planerna ska innehålla ett alternativ för situationer där avdelningschefen inte kan kontaktas.

Artikel 9

Ägare av kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter

1. Systemägaren ska kontakta myndigheten för säkerhetsackreditering så tidigt som möjligt i ett projekt för att införa ett kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter i syfte att fastställa relevanta säkerhetsnormer och säkerhetskrav och för att inleda processen för säkerhetsackreditering.

2. Systemägaren ska säkerställa att säkerhetsåtgärderna uppfyller kraven från myndigheten för säkerhetsackreditering och att kommunikations- och informationssystemet inte hanterar säkerhetsskyddsklassificerade EU-uppgifter förrän det har ackrediterats.

3. Systemägaren ska kontakta den kryptogodkännande myndigheten och begära dess godkännande för att använda krypteringsteknik. Systemägare får inte använda krypteringsteknik i produktionssystem utan förhandsgodkännande.

4. Systemägaren ska samråda med avdelningens säkerhetsansvarige för de lokala datasystemen i frågor som rör säkerheten för kommunikations- och informationssystem.

5. Systemägaren ska minst en gång per år se över de säkerhetsåtgärder som tillämpas på ett system, inbegripet dess säkerhetsplan.

6. Om en säkerhetsincident inträffar i ett kommunikations- och informationssystem och det därvid anges att systemet inte längre kan skydda säkerhetsskyddsklassificerade EU-uppgifter på ett tillfredsställande sätt, ska systemägaren informera den lokalt säkerhetsansvarige och omedelbart kontakta myndigheten för säkerhetsackreditering för att få råd om hur man ska gå tillväga. I detta fall kan ackrediteringen upphävas och systemet tas ur drift till dess att lämpliga korrigerande åtgärder har vidtagits.

7. Systemägaren ska alltid stödja myndigheten för säkerhetsackreditering fullt ut i dess uppgifter i samband med ackreditering av kommunikations- och informationssystem.

Artikel 10

Driftsansvarig myndighet för informationssäkring

Den driftsansvariga myndigheten för informationssäkring för varje kommunikations- och informationssystem ska ha följande uppgifter:

a) Upprätta säkerhetsdokumentation i enlighet med säkerhetsstrategier och säkerhetsriktlinjer, särskilt säkerhetsplanen, de säkra driftsmetoder som rör systemet och krypteringsdokumentationen inom ramen för ackrediteringsprocessen för kommunikations- och informationssystem.

b) Delta i urval och tester av systemspecifika tekniska åtgärder, enheter och program rörande säkerhet, övervaka genomförandet av dessa och säkerställa att de installeras, konfigureras och underhålls på ett säkert sätt och i enlighet med relevant säkerhetsdokumentation.

c) Delta i urvalet av tempestsäkerhetsåtgärder och tempestsäkerhetsutrustning, om så krävs i säkerhetsplanen, och i samarbete med tempestmyndigheten säkerställa att de installeras och underhålls på ett säkert sätt.

d) Övervaka genomförandet och tillämpningen av de säkra driftsmetoder som rör driften av systemet.

e) Förvalta och hantera kryptoprodukter, i samarbete med kryptodistribueringsmyndigheten, för att säkerställa korrekt förvaring av kryptoprodukter och kontrollerat material och, om så krävs, framställningen av kryptografiska variabler.

f) Utföra säkerhetsanalyser, översyner och test, särskilt för att ta fram relevanta riskrapporter, enligt kraven från myndigheten för säkerhetsackreditering.

g) Tillhandahålla systemspecifik utbildning i informationssäkring.

h) Genomföra och svara för driften av systemspecifika säkerhetsåtgärder.

KAPITEL 4

LOKALT SÄKERHETSANSVARIG

Artikel 11

Utnämning av den lokalt säkerhetsansvarige

1. Den lokalt säkerhetsansvarige och de ställföreträdande lokala säkerhetsansvariga ska vara tjänstemän eller tillfälligt anställda.

2. Alla lokalt säkerhetsansvariga och ställföreträdande lokalt säkerhetsansvariga ska ha giltigt säkerhetsbemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till nivån SECRET UE/EU SECRET och vid behov upp till nivån TRES SECRET UE/EU TOP SECRET. Den lokalt säkerhetsansvarige eller ställföreträdande lokalt säkerhetsansvarige ska erhålla säkerhetsbemyndigandet innan denne utnämns.

3. Kommissionens representationer får begära att kommissionens säkerhetsmyndighet beviljar ett undantag från kraven i punkterna 1 och 2.

Artikel 12

Säkra driftsmetoder för säkrade utrymmen

1. Den lokalt säkerhetsansvarige vid den berörda kommissionsavdelningen ska utarbeta säkra driftsmetoder för varje säkrat utrymme som de ansvarar för.

2. Den lokalt säkerhetsansvarige ska säkerställa att de säkra driftsmetoderna inbegriper följande krav:

a) Endast personal med giltigt säkerhetsbemyndigande och konstaterad behovsenlig behörighet att tillgå handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska ges obeledsagat tillträde till ett säkrat utrymme under kontorstid.

b) Utanför kontorstid ska obeledsagat tillträde till ett säkrat utrymme endast beviljas den lokalt säkerhetsansvarige inom avdelningen, kontrolltjänstemannen eller kontrolltjänstemännen för det säkrade utrymmet, dennes eller dessas ställföreträdare och bemyndigad personal från direktoratet för säkerhet vid generaldirektoratet för personal och säkerhet.

c) Inspelnings- och kommunikationsutrustning såsom mobiltelefoner, datorer, kameror eller andra smarta enheter ska inte vara tillåtna i säkrade utrymmen utan förhandstillstånd från kommissionens säkerhetsmyndighet. Eventuella undantag ska begäras från kommissionens säkerhetsmyndighet i förväg. Den lokalt säkerhetsansvarige ska fungera som kontaktpunkt.

d) All intern eller extern personal som behöver tillträde till ett säkrat utrymme men som inte uppfyller kriterierna i led a ska alltid ledsagas och övervakas av en vederbörligen bemyndigad anställd. Allt sådant tillträde till ett säkrat utrymme ska registreras i en loggbok vid ingången till det säkrade utrymmet.

e) Den lokalt säkerhetsansvarige ska säkerställa att de system för upptäckt av intrång som övervakar ett säkrat utrymme alltid är aktiva och fungerar korrekt, och ska hantera alla därmed sammanhörande lösenord, nycklar, PIN-koder eller andra åtkomst- och autentiseringsmekanismer.

f) Larm i ett säkrat utrymme ska rapporteras till direktoratet för säkerhet vid generaldirektoratet för personal och säkerhet, som omedelbart ska underrätta den lokalt säkerhetsansvarige.

g) Den lokalt säkerhetsansvarige vid den avdelning där det säkrade utrymmet är beläget ska föra ett register över alla ingripanden till följd av ett larm eller en säkerhetsincident.

h) Det ska finnas förfaranden för att reagera på ett larm eller en annan nödsituation i det säkrade utrymmet, inbegripet att evakuera personal och säkerställa snabba insatser av en incidenthanteringsgrupp under ledning av kommissionens säkerhetsmyndighet, och vid behov, av externa räddningstjänster.

i) Den lokalt säkerhetsansvarige ska till kommissionens säkerhetsmyndighet omedelbart rapportera alla överträdelser av säkerhetsbestämmelserna som inträffar i eller som berör ett säkrat utrymme, i syfte att fastställa lämpliga åtgärder.

j) Enskilda kontor, rum och kassaskåp inom ett säkrat utrymme ska hållas låsta närhelst de lämnas obevakade.

k) Personalen ska undvika att diskutera säkerhetsskyddsklassificerade uppgifter i korridorer eller andra gemensamma utrymmen i det säkrade utrymmet när obehöriga personer befinner sig i närheten.

Artikel 13

Säkerhetsnycklar och kombinationer

1. Den lokalt säkerhetsansvarige ska ha det övergripande ansvaret för att säkerställa korrekt hantering och lagring av nycklar och kombinationer som används i eller för tillträde till säkrade utrymmen. Nycklar och kombinationer ska lagras i ett säkerhetsskåp och skyddas på minst samma nivå som det material som de ger tillgång till.

2. Den lokalt säkerhetsansvarige ska föra ett register över säkerhetsskåp och valv, tillsammans med en uppdaterad förteckning över all personal som har obeledsagat tillträde till dem.

3. Den lokalt säkerhetsansvarige ska föra ett register över nycklar till säkerhetsskåp och valv, inbegripet den personal som tilldelats nycklarna. Ett kvitto ska bevaras för varje nyckel som givits ut, och av det ska framgå identifieringsuppgifter för nyckeln, mottagare, datum och tidpunkt.

4. Nycklar och kombinationer får endast ges ut till personal som har behovsenlig behörighet att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter och har bemyndigats till detta. Den lokalt säkerhetsansvarige ska ta tillbaka nyckeln när dessa villkor inte längre är uppfyllda.

5. Den lokalt säkerhetsansvarige ska förvara reservnycklar och en skriftlig uppgift om varje kombination i separata förseglade, ogenomskinliga, undertecknade och daterade kuvert som ska tillhandahållas av den anställde som har ansvaret för nycklarna. Dessa kuvert ska förvaras i ett säkerhetsskåp som motsvarar den högsta säkerhetsskyddsklassificeringsnivån för det material som lagras i det berörda säkerhetsskåpet eller valvet.

6. Om ett kuvert efter en ändring av en kombination eller nyckelrotation visar tecken på manipulering eller skada ska den lokalt säkerhetsansvarige behandla detta som en säkerhetsincident och omedelbart informera kommissionens säkerhetsmyndighet.

7. Ändringar av kombinationerna för säkerhetsskåp i säkrade utrymmen ska göras under övervakning av den lokalt säkerhetsansvarige. Kombinationer ska återställas minst var tolfte månad och alltid i följande fall:

a) Ett nytt säkerhetsskåp tas emot eller ett nytt lås installeras (särskilt standardkombinationer ska ändras omedelbart).

b) Uppgifter har röjts eller det finns misstankar om att så har skett.

c) En person som innehar en kombination behöver inte längre tillgång.

8. Den lokalt säkerhetsansvarige ska föra ett register över datum för de kombinationsändringar som avses i punkt 7.

Artikel 14

Planer för evakuering och förstöring av säkerhetsskyddsklassificerade EU-uppgifter i en nödsituation

1. Den lokalt säkerhetsansvarige ska bistå avdelningschefen vid upprättandet av planer för evakuering och förstöring av säkerhetsskyddsklassificerade EU-uppgifter i en nödsituation, på grundval av vägledning från direktoratet för säkerhet vid GD Personal och säkerhet.

2. Den lokalt säkerhetsansvarige ska säkerställa att all utrustning som är nödvändig för att genomföra de planer som avses i punkt 1 är lätt tillgänglig och hålls i gott skick.

3. Den lokalt säkerhetsansvarige ska, tillsammans med de tjänstemän som utsetts i de planer som avses i punkt 1, se över beredskapsnivån i fråga om planerna minst var tolfte månad och vidta alla nödvändiga åtgärder för att uppdatera dem.

Artikel 15

Säkerhetsbemyndigande

1. Den lokalt säkerhetsansvarige ska föra ett register över alla tjänster inom avdelningen för vilka det krävs ett säkerhetsbemyndigande av kommissionen och över den personal som innehar dessa tjänster. Kravet på säkerhetsbemyndigande måste under rekryteringsprocessen anges i meddelandet om ledig tjänst och meddelas sökanden vid intervjun.

2. Den lokalt säkerhetsansvarige ska övervaka alla begäranden om säkerhetsbemyndiganden för tillgång till säkerhetsskyddsklassificerade EU-uppgifter. Den lokalt säkerhetsansvarige ska fungera som kontaktpunkt inom avdelningen och stå i kontakt med kommissionens säkerhetsmyndighet angående säkerhetsbemyndigandena.

3. Den lokalt säkerhetsansvarige ska göra begäran om inledande av förfarandet för säkerhetsbemyndigande för den berörda anställde och säkerställa att den anställde utan dröjsmål återsänder frågeformuläret för nationellt säkerhetsgodkännande till kommissionens säkerhetsmyndighet.

4. Den lokalt säkerhetsansvarige ska säkerställa att personal inom avdelningen som har fått säkerhetsgodkännande deltar i den obligatoriska genomgången rörande säkerhetsskyddsklassificerade EU-uppgifter för att erhålla sitt säkerhetsbemyndigande.

5. Den lokalt säkerhetsansvarige ska regelbundet stå i kontakt med avdelningens personalförvaltning för att hålla sig underrättad om alla ändringar i fråga om tjänster som kräver säkerhetsbemyndigande och ska omedelbart informera kommissionens säkerhetsmyndighet om varje sådan ändring.

6. Den lokalt säkerhetsansvarige ska informera kommissionens säkerhetsmyndighet när en ny anställd som har ett befintligt säkerhetsgodkännande tillträder en tjänst vars innehavare måste ha ett säkerhetsbemyndigande.

7. Den lokalt säkerhetsansvarige ska säkerställa att de anställda inom avdelningen slutför förfarandet för förnyelse av sitt säkerhetsgodkännande inom den föreskrivna tidsfristen. Varje anställd som vägrar att slutföra förfarandet ska vara skyldig att flytta över till en tjänst vars innehavare inte behöver ha ett säkerhetsbemyndigande.

Artikel 16

Registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter

1. Om en avdelning driver en registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter ska den lokalt säkerhetsansvarige övervaka kontrolltjänstemännens verksamhet när det gäller hanteringen av säkerhetsskyddsklassificerade EU-uppgifter och efterlevnaden av säkerhetsbestämmelserna i fråga om skydd av säkerhetsskyddsklassificerade EU-uppgifter.

2. Den lokalt säkerhetsansvarige ska utföra följande kontroller minst var tolfte månad och vid byte av kontrolltjänsteman eller ställföreträdande kontrolltjänsteman:

a) Kontroll av ett urval av handlingar i registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter för att bekräfta deras status och att registret över säkerhetsskyddsklassificerade handlingar är korrekt.

b) Kontroll av ett urval av kvitton och bevis rörande överföringen av säkerhetsskyddsklassificerade EU-uppgifter till och från registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter.

c) Kontroll av ett urval av förstöringsintyg.

3. Den lokalt säkerhetsansvarige ska minst en gång i månaden utföra stickprovskontroller av registret över säkerhetsskyddsklassificerade handlingar och av nyligen mottagna säkerhetsskyddsklassificerade handlingar för att säkerställa att handlingarna registreras korrekt.

4. Alla kontroller ska registreras i loggen för registret över säkerhetsskyddsklassificerade handlingar.

Artikel 17

Övrigt säkerhetsansvar

Den lokalt säkerhetsansvariges övriga säkerhetsansvar ska anges i ett säkerhetsmeddelande som särskilt omfattar den fysiska säkerheten för personer, lokaler och andra tillgångar samt uppgifter.

KAPITEL 5

KONTROLLTJÄNSTEMAN FÖR REGISTRERINGSENHETEN

Artikel 18

Utnämning av kontrolltjänstemannen för registreringsenheten

1. Kontrolltjänstemän för registreringsenheten och ställföreträdande kontrolltjänstemän för registreringsenheten ska vara tjänstemän eller tillfälligt anställda.

2. Alla kontrolltjänstemän för registreringsenheten och ställföreträdande kontrolltjänstemän för registreringsenheten ska ha giltigt säkerhetsbemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till nivån SECRET UE/EU SECRET och vid behov upp till nivån TRES SECRET UE/EU TOP SECRET. Kontrolltjänstemannen för registreringsenheten eller den ställföreträdande kontrolltjänstemannen för registreringsenheten ska erhålla säkerhetsbemyndigandet innan denne utnämns.

3. Kommissionens representationer får begära att kommissionens säkerhetsmyndighet beviljar ett undantag från kraven i punkterna 1 och 2.

Artikel 19

Ansvarsområden

1. Kontrolltjänstemän för registreringsenheter ska för säkerhetsändamål registrera uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre när uppgifterna

a) anländer till eller lämnar en avdelning inom kommissionen, eller

b) anländer till eller lämnar ett informations- och kommunikationssystem.

2. Kontrolltjänstemän för registreringsenheter ska registrera alla händelser under livscykeln för alla uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre. Kontrolltjänstemän för registreringsenheter ska också säkerställa att alla uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande som utbyts med tredjeländer och internationella organisationer registreras. Detta ska ske i samordning med den registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter som förvaltas av generalsekretariatet.

3. Kontrolltjänstemannen för registreringsenheten ska registrera handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre i registret över säkerhetsskyddsklassificerade handlingar och säkerställa att de förvaras säkert i registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter.

4. Kontrolltjänstemannen för registreringsenheten ska bistå kommissionens personal med att utarbeta och översända uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

5. När handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre tas emot från andra avdelningar eller externa parter ska kontrolltjänstemannen för registreringsenheten säkerställa att ett leveranskvittot vederbörligen lämnas till upphovsmannen.

6. Innan en anställd ges tillgång till en säkerhetsskyddsklassificerad handling som innehas av registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter ska kontrolltjänstemannen kontrollera med den lokalt säkerhetsansvarige att den anställde har fått säkerhetsbemyndigande av kommissionens säkerhetsmyndighet.

7. Kontrolltjänstemannen för registreringsenheten ska logga all personal som kommer till och lämnar registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter och som inte har bemyndigande för obeledsagat tillträde och följa dem under hela besöket.

8. När en anställd tar en handling i syfte att konsultera den utanför registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter ska kontrolltjänstemannen säkerställa att vederbörande känner till relevanta kompensationsåtgärder rörande säkerheten och att den anställde återlämnar handlingen så snart den inte längre behövs. Kontrolltjänstemannen för registreringsenheten ska påminna de anställda om att återlämna sådana dokument så snart som möjligt.

9. Om säkerhetsskyddsklassificerade handlingar transporteras personligen utanför det land där registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter är belägen ska registreringsenheten utfärda ett kuririntyg.

10. Detaljerade instruktioner för kontrolltjänstemannen för registreringsenheten om registrering av säkerhetsskyddsklassificerade handlingar ska anges i ett säkerhetsmeddelande.

Artikel 20

Inplacering på lägre säkerhetsskyddsklassificeringsnivå och beslut om att uppgifter inte längre ska vara säkerhetsskyddsklassificerade

Kontrolltjänstemannen för registreringsenheten ska bistå de ansvariga avdelningarna vid översynen av säkerhetsskyddsklassificerade EU-uppgifter för att förvissa sig om huruvida den ursprungliga säkerhetsskyddsklassificeringsnivån fortfarande är lämplig, eller handlingen kan placeras in på en lägre säkerhetsskyddsklassificeringsnivå eller den inte längre ska vara säkerhetsskyddsklassificerad.

Artikel 21

Förstöring

1. Kontrolltjänstemannen för registreringsenheten ska vara ansvarig för att förstöra uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre på godkända sätt, i förekommande fall i närvaro av vittnen som har säkerhetsgodkännande.

2. Kontrolltjänstemannen för registreringsenheten ska registrera all förstöring av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre i registret över säkerhetsskyddsklassificerade handlingar och bevara motsvarande förstöringsintyg i registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter.

Artikel 22

Ytterligare uppgifter

1. Kontrolltjänstemannen för registreringsenheten ska ge all nödvändig hjälp till den lokalt säkerhetsansvarige när denne utför tillsynsverksamhet i registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter.

2. Kontrolltjänstemannen för registreringsenheten ska rapportera alla misstänkta eller faktiska säkerhetsincidenter till den lokalt säkerhetsansvarige, som i sin tur ska rapportera dem till kommissionens säkerhetsmyndighet.

3. Kontrolltjänstemannen för registreringsenheten vid en kommissionsavdelning som anordnar ett möte på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska förbereda de säkerhetsskyddsklassificerade EU-uppgifter som kommer att behandlas under mötet och ska samordna med mötesarrangören för att säkerställa att alla handlingar och kvitton hanteras i enlighet med relevanta bestämmelser.

KAPITEL 6

SLUTBESTÄMMELSER

Artikel 23

Öppenhet

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

Artikel 24

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

Utfärdat i Bryssel den 7 april 2022.

På kommissionens vägnar
För ordföranden
Gertrud INGESTAD
Generaldirektör
Generaldirektoratet för personal och säkerhet