KOMMISSIONENS AFGØRELSE (EU) 2022/640

af 7. april 2022

om gennemførelsesbestemmelser for de vigtigste sikkerhedsaktørers roller og ansvarsområder

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 249,

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen ([1]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer ([2]) og

ud fra følgende betragtninger:

(1) Afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444 gælder for alle Kommissionens tjenestegrene og bygninger.

(2) Om nødvendigt skal der vedtages gennemførelsesbestemmelser til at supplere eller understøtte afgørelse (EU, Euratom) 2015/444 i overensstemmelse med afgørelsens artikel 60.

(3) De sikkerhedsforanstaltninger, der træffes for at beskytte EU-klassificerede informationer, skal gennem hele livscyklussen svare til informationernes sikkerhedsklassifikation.

(4) Sikkerhedsforanstaltninger til beskyttelse af kommunikations- og informationssystemer i Kommissionen er fastsat i Kommissionens afgørelse (EU, Euratom) 2017/46 ([3]), navnlig artikel 3 om principper for IT-sikkerhed i Kommissionen og artikel 9 om systemejere.

(5) Formålet med gennemførelsesbestemmelserne om de vigtigste sikkerhedsaktørers roller og ansvarsområder er at vejlede om de forudsætninger og pligter, der er fastsat for disse roller i afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444.

(6) Artikel 36, stk. 7, i afgørelse (EU, Euratom) 2015/444 fastsætter en række yderligere sikkerhedsrelaterede funktioner, som Kommissionens sikkerhedsmyndighed skal påtage sig. Opgaverne i forbindelse med disse funktioner er fastlagt i nævnte afgørelse.

(7) Lokale sikkerhedsansvarlige og arkivansvarlige har et særligt ansvar for beskyttelse af EU's klassificerede informationer i deres tjenestegrene i henhold til afgørelse (EU, Euratom) 2015/444.

(8) Den 4. maj 2016 vedtog Kommissionen en afgørelse ([4]) om bemyndigelse af Kommissionens medlem med ansvar for sikkerhedsanliggender til på Kommissionens vegne og ansvar at vedtage de gennemførelsesbestemmelser, der henvises til i artikel 60 i afgørelse (EU, Euratom) 2015/444; efterfølgende vedtog det medlem af Kommissionen, der er ansvarligt for sikkerhedsspørgsmål, den 13. april 2021 på vegne af Kommissionen og under dennes ansvar en afgørelse ([5]) om videredelegering af disse gennemførelsesbestemmelser til generaldirektøren for Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed —

([1]) EUT L 72 af 17.3.2015, s. 41.
([2]) EUT L 72 af 17.3.2015, s. 53.
([3]) Kommissionens afgørelse (EU, Euratom) 2017/46 af 10. januar 2017 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen (EUT L 6 af 11.1.2017, s. 40).
([4]) Afgørelse C(2016) 2797 final af 4. maj 2016 om bemyndigelse i forbindelse med sikkerhed (findes ikke på dansk).
([5]) Afgørelse C(2021) 2684 final af 13. april 2021 om videredelegering af bemyndigelser, der er tildelt i henhold til Kommissionens afgørelse C(2016) 2797 om bemyndigelse i forbindelse med sikkerhed (findes ikke på dansk).

VEDTAGET DENNE AFGØRELSE:

KAPITEL 1

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. I denne afgørelse fastsættes roller og ansvarsområder for de vigtigste sikkerhedsaktører, der er ansvarlige for beskyttelse af EU's klassificerede informationer (EUCI) i Kommissionen i henhold til afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444.

2. Denne afgørelse finder anvendelse på alle Kommissionens tjenestegrene og på alle Kommissionens lokaliteter.

KAPITEL 2

GENERALDIREKTORATET FOR MENNESKELIGE RESSOURCER OG SIKKERHED

Artikel 2

Kommissionens sikkerhedsmyndighed

1. Direktøren for Sikkerhedsdirektoratet i Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed er Kommissionens sikkerhedsmyndighed (CSA), jf. artikel 7 i afgørelse (EU, Euratom) 2015/444.

2. CSA'en udfører sine opgaver på følgende områder som fastsat i afgørelse (EU, Euratom) 2015/444 i overensstemmelse med artikel 3-7 i denne afgørelse:

a) personelsikkerhed

b) fysisk sikkerhed

c) forvaltning af EUCI

d) akkreditering af ethvert kommunikations- og informationssystem (CIS), der håndterer EUCI

e) industrisikkerhed samt

f) udveksling af klassificerede informationer.

3. CSA'en tilbyder obligatorisk uddannelse af de lokale sikkerhedsansvarlige (LSO'er), stedfortrædende LSO'er, arkivansvarlige (RCO'er) og stedfortrædende RCO'er i deres ansvarsområder og opgaver.

Artikel 3

Informationssikringsmyndighed

Informationssikringsmyndigheden er ansvarlig for følgende aktiviteter i forbindelse med beskyttelse af EUCI:

a) udvikling af sikkerhedspolitikker for informationssikring og sikkerhedsretningslinjer og overvågning af deres effektivitet og relevans

b) beskyttelse og forvaltning af tekniske informationer om kryptoprodukter

c) sikring af, at informationssikkerhedsforanstaltningerne er i overensstemmelse med Kommissionens sikkerheds- og indkøbspolitikker, hvor det er relevant

d) sikring af, at kryptoprodukter udvælges i overensstemmelse med politikkerne for deres egnethed og udvælgelse

e) høring af systemejere, systemleverandører, sikkerhedsaktører og brugerrepræsentanter med hensyn til informationssikkerhedspolitikker og sikkerhedsretningslinjer.

Artikel 4

Sikkerhedsgodkendelsesmyndighed

1. CSA'en er ansvarlig for at akkreditere sikrede områder, der opfylder kravene i artikel 18 i afgørelse 2015/444, og CIS'er til håndtering af EUCI.

2. Kommissionens tjenestegrene hører sikkerhedsgodkendelsesmyndigheden i samarbejde med deres LSO og deres lokale IT-sikkerhedsansvarlige (LISO), alt efter hvad der er relevant, når en afdeling har til hensigt at:

a) opstille et sikret område

b) implementere et CIS til håndtering af EUCI

c) installere eventuelt andet udstyr til håndtering af klassificerede oplysninger, herunder forbindelser til et CIS hos tredjemand.

Sikkerhedsakkrediteringsmyndigheden (SAA) yder rådgivning om disse aktiviteter under både planlægnings- og anlægs- eller udviklingsprocesserne.

3. EUCI må ikke håndteres i et sikret område eller et CIS, før sikkerhedsgodkendelsesmyndigheden har udstedt en godkendelse på det relevante klassifikationsniveau.

4. Kravene til godkendelse af et sikret område omfatter:

a) godkendelse af planerne for det sikrede område

b) godkendelse af kontrakter om arbejder udført af eksterne kontrahenter under hensyntagen til bestemmelserne om industrisikkerhed, f.eks. krav om sikkerhedsgodkendelse af kontrahenterne og deres personale

c) adgang til alle nødvendige erklæringer og typeattester

d) en fysisk inspektion af det sikrede område for at verificere, at byggematerialer og -metoder, adgangskontrol, sikkerhedsudstyr og andre genstande opfylder de krav, der er fastsat af den relevante CSA

e) validering af modforanstaltninger mod elektromagnetisk stråling for ethvert teknisk sikret område

f) godkendelse af de operationelle sikkerhedsprocedurer (SecOP'er) for det sikrede område.

5. Kravene til godkendelse af et CIS, der håndterer EUCI, omfatter:

a) udarbejdelse af en systemakkrediteringsstrategi

b) validering af CIS'ets sikkerhedsplan på grundlag af en risikostyringstilgang

c) validering af SecOP'erne for CIS'et

d) validering af al anden påkrævet sikkerhedsdokumentation, der kræves af sikkerhedsgodkendelsesmyndigheden

e) godkendelse af eventuel anvendelse af krypteringsteknologier

f) validering af modforanstaltningerne mod elektromagnetisk stråling for et CIS, der håndterer informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere

g) en inspektion af CIS'et for at kontrollere, at de dokumenterede sikkerhedsforanstaltninger er gennemført korrekt.

6. Når kravene til akkreditering er opfyldt, udsteder sikkerhedsgodkendelsesmyndigheden en formel autorisation til håndtering af EUCI i det sikrede område eller CIS, til et angivet maksimalt klassifikationsniveau for EUCI og i op til 5 år afhængigt af klassifikationsniveauet af de EUCI, der håndteres, og de involverede risici.

7. Efter underretning om et sikkerhedsbrud eller en væsentlig ændring af udformningen af eller sikkerhedsforanstaltningerne i et sikret område eller CIS gennemgår sikkerhedsgodkendelsesmyndigheden autorisationen til at håndtere EUCI og kan om nødvendigt tilbagekalde denne, indtil eventuelle konstaterede problemer er løst.

Artikel 5

TEMPEST-myndighed

1. TEMPEST-sikkerhedsforanstaltninger gennemføres for at beskytte CIS'er, der håndterer informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, og kan gennemføres for informationer, der er klassificeret på RESTREINT UE/EU RESTRICTED-niveau.

2. TEMPEST-myndigheden er ansvarlig for at godkende de foranstaltninger, der træffes for at beskytte mod kompromittering af EUCI gennem utilsigtede elektroniske emissioner.

3. Efter anmodning fra en ejer af et CIS-system, der håndterer EUCI, udsteder TEMPEST-myndigheden specifikationer for TEMPEST-sikkerhedsforanstaltninger, alt efter hvad der er relevant for informationernes klassifikationsniveau.

4. TEMPEST-myndigheden udfører teknisk afprøvning i forbindelse med akkrediteringen af sikrede områder og CIS'er til håndtering af EUCI, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, og udsteder efter vellykket testning et TEMPEST-certifikat.

5. Et TEMPEST-certifikat skal mindst indeholde følgende oplysninger:

a) datoen for afprøvningen

b) en beskrivelse af TEMPEST-sikkerhedsforanstaltningerne med planer for området

c) certifikatets udløbsdato

d) eventuelle ændringer, som vil ugyldiggøre certificeringen

e) TEMPEST-myndighedens underskrift.

6. En LSO eller en mødearrangør med ansvar for at tilrettelægge et klassificeret møde i samarbejde med LSO'en kan anmode TEMPEST-myndigheden om at teste mødelokaler for at sikre, at de er teknisk sikrede.

Artikel 6

Kryptogodkendelsesmyndighed

1. Kryptogodkendelsesmyndigheden er ansvarlig for at godkende anvendelsen af krypteringsteknologier.

2. Kryptogodkendelsesmyndigheden yder vejledning om kravene til anvendelse og godkendelse af krypteringsteknologier.

3. Kryptogodkendelsesmyndigheden godkender anvendelsen af krypteringsløsninger på grundlag af en anmodning fra systemejeren. Godkendelsen baseres på en tilfredsstillende evaluering af mindst:

a) sikkerhedsbehovene for de oplysninger, der skal beskyttes

b) en oversigt over det CIS, der er involveret i løsningen

c) en vurdering af de iboende risici og restrisikoen

d) en beskrivelse af den planlagte løsning

e) SecOP'er for krypteringsløsningen.

4. Kryptogodkendelsesmyndigheden fører et register over godkendte krypteringsløsninger.

Artikel 7

Kryptodistributionsmyndighed

1. Kryptodistributionsmyndigheden er ansvarlig for distribution af kryptografiske materialer, der anvendes til beskyttelse af EUCI (hovedsagelig krypteringsudstyr, kryptografiske nøgler, certifikater og relaterede autentifikatorer) til følgende:

a) brugere eller afdelinger i Kommissionen til CIS, der administreres af eksterne parter

b) brugere eller organisationer uden for Kommissionen til CIS, der administreres af Kommissionen.

2. Kryptodistributionsmyndigheden kan uddelegere distributionen af kryptografiske materialer til tredjeparter til andre afdelinger i overensstemmelse med artikel 17, stk. 3, i afgørelse 2015/443.

3. Kryptodistributionsmyndigheden sikrer, at alle kryptografiske materialer sendes via sikre kanaler, der beskytter mod og dokumenterer eventuel manipulation, i overensstemmelse med de gældende sikkerhedsregler for klassifikationsgraden for de EUCI, der vil blive beskyttet af disse materialer.

4. Kryptodistributionsmyndigheden skal vejlede LSO'en og, hvor det er relevant, LISO'en i hver af de afdelinger i Kommissionen, der er involveret i produktion, distribution eller brug af kryptografiske materialer.

5. Kryptodistributionsmyndigheden sikrer, at der udarbejdes passende SecOP'er for distributionsprocessen.

KAPITEL 3

KOMMISSIONENS TJENESTEGRENE

Artikel 8

Afdelingschefer

1. Hver afdelingschef udpeger:

a) en LSO og en eller, hvis det er relevant, flere stedfortrædere i afdelingen eller kabinettet

b) en RCO og en eller, hvis det er relevant, flere stedfortrædere i hver afdeling, der driver et EUCI-register

c) en systemejer for hvert CIS, der håndterer EUCI.

2. Afdelingschefen anmoder om godkendelse fra direktøren for Sikkerhedsdirektoratet i Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed forud for udnævnelsen af LSO'er, stedfortrædende LSO'er, RCO'er og stedfortrædende RCO'er.

3. Afdelingschefen identificerer i samråd med LSO'en alle stillinger, der kræver sikkerhedsgodkendelse til at tilgå EUCI. Ansøgere til sådanne stillinger underrettes om kravet om godkendelse under ansættelsesproceduren.

4. Lederen af en afdeling, der ligger inde med EUCI, er ansvarlig for at aktivere nøddestruktionsplaner og evakueringsplaner, når det er nødvendigt. Planerne skal omfatte en alternativ strategi til situationer, hvor afdelingslederen ikke kan kontaktes.

Artikel 9

Ejere af CIS, der håndterer EUCI

1. Systemejeren kontakter sikkerhedsgodkendelsesmyndigheden så tidligt som muligt i et projekt til implementering af et CIS, der håndterer EUCI, med henblik på at fastlægge de relevante sikkerhedsstandarder og -krav og indlede processen med sikkerhedsgodkendelse.

2. Systemejeren sikrer, at sikkerhedsforanstaltningerne opfylder kravene fra sikkerhedsgodkendelsesmyndigheden, og at CIS'et ikke håndterer EUCI, før det er blevet akkrediteret.

3. Systemejeren kontakter kryptogodkendelsesmyndigheden med henblik på godkendelse til at anvende krypteringsteknologier. Systemejere må ikke anvende krypteringsteknologier i produktionssystemer uden forudgående godkendelse.

4. Systemejeren skal rådføre sig med afdelingens LISO om spørgsmål vedrørende CIS'ers sikkerhed.

5. Systemejeren skal mindst en gang om året gennemgå de sikkerhedsforanstaltninger, der gælder for et system, herunder dets sikkerhedsplan.

6. Hvis en sikkerhedshændelse indtræffer i et CIS, som tyder på, at CIS'et ikke længere kan beskytte EUCI i tilstrækkelig grad, underretter systemejeren LSO'en og kontakter straks sikkerhedsgodkendelsesmyndigheden med henblik på rådgivning om det videre forløb. I så fald kan godkendelsen suspenderes, og systemet kan blive taget ud af drift, indtil der er truffet passende korrigerende foranstaltninger.

7. Systemejeren skal til enhver tid give sikkerhedsgodkendelsesmyndigheden fuld støtte i forbindelse med dennes opgaver vedrørende akkreditering af CIS'et.

Artikel 10

Operationel informationssikringsmyndighed

Den operationelle informationssikringsmyndighed for hvert CIS skal:

a) udarbejde sikkerhedsdokumentation i overensstemmelse med sikkerhedspolitikker og -retningslinjer, navnlig sikkerhedsplanen, SecOP'erne vedrørende systemet og den kryptografiske dokumentation som led i CIS-akkrediteringsprocessen

b) deltage i udvælgelse og afprøvning af systemspecifikke tekniske sikkerhedsforanstaltninger, -anordninger og -software for at overvåge deres implementering og sikre, at de installeres, konfigureres og vedligeholdes sikkert i overensstemmelse med den relevante sikkerhedsdokumentation

c) deltage i udvælgelsen af TEMPEST-sikkerhedsforanstaltninger og -anordninger, hvis det kræves i sikkerhedsplanen, og i samarbejde med TEMPEST-myndigheden sikre, at de installeres og vedligeholdes sikkert

d) overvåge gennemførelsen og anvendelsen af SecOP'erne i forbindelse med driften af systemet

e) forvalte og håndtere kryptoprodukter i samarbejde med kryptodistributionsmyndigheden for at sikre korrekt opbevaring af kryptografiske materialer og kontrollerede produkter og om nødvendigt sikre generering af kryptografiske variabler

f) foretage sikkerhedsanalyser, -gennemgange og -test, navnlig med henblik på at udarbejde de relevante risikorapporter som krævet af sikkerhedsgodkendelsesmyndigheden

g) tilbyde CIS-specifik uddannelse i informationssikring

h) implementere og anvende CIS-specifikke sikkerhedsforanstaltninger.

KAPITEL 4

LSO

Artikel 11

Udpegelse af LSO

1. LSO'en og de stedfortrædende LSO'er er tjenestemænd eller midlertidigt ansatte.

2. Alle LSO'er og stedfortrædende LSO'er skal have en gyldig sikkerhedsgodkendelse til at tilgå EUCI op til klassifikationsniveau SECRET UE/EU SECRET og om nødvendigt op til klassifikationsniveau TRES SECRET UE/EU TOP SECRET. LSO'en eller den stedfortrædende LSO skal opnå sikkerhedsgodkendelsen, inden vedkommende udpeges.

3. Kommissionens repræsentationer kan anmode CSA'en om at indrømme en undtagelse fra kravene i stk. 1 og 2.

Artikel 12

Operationelle sikkerhedsprocedurer for sikrede områder

1. LSO'en i den pågældende tjenestegren i Kommissionen udarbejder SecOP'er for hvert sikret område, som hører under deres ansvarsområde.

2. LSO'en skal sikre, at SecOP'erne omfatter følgende krav:

a) kun ansatte med en gyldig sikkerhedsgodkendelse og et konstateret behov for at tilgå dokumenter, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, må have uledsaget adgang til et sikret område i kontortiden

b) uledsaget adgang til et sikret område uden for kontortiden gives kun til LSO'en i afdelingen, RCO(er) i det sikrede område, deres stedfortrædere og autoriseret personale fra sikkerhedsdirektoratet i Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed

c) optageanordninger og kommunikationsudstyr såsom mobiltelefoner, computere, kameraer eller andre intelligente enheder er ikke tilladt i sikrede områder uden forudgående tilladelse fra CSA'en der skal anmodes om eventuel dispensation fra CSA'en på forhånd; LSO'en fungerer som kontaktpunkt

d) alt internt eller eksternt personale, der har brug for adgang til et sikret område, men som ikke opfylder kriterierne under litra a) ovenfor, skal til enhver tid ledsages og overvåges af en behørigt bemyndiget medarbejder; al sådan adgang til et sikret område skal registreres i en logbog, der føres ved indgangen til det sikrede område

e) LSO'en sikrer, at de systemer til detektering af indtrængen, der overvåger et sikret område, er aktive og fungerer korrekt til enhver tid, og forvalter alle relaterede adgangskoder, nøgler, PIN-numre eller andre adgangs- og autentificeringsmekanismer

f) alarmer i et sikret område indberettes til Sikkerhedsdirektoratet i Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed, som straks underretter LSO'en

g) LSO'en i den afdeling, hvor det sikrede område er beliggende, skal føre register over alle interventioner efter en alarm eller en sikringsrelateret hændelse

h) der skal være indført procedurer i tilfælde af en alarm eller en anden nødsituation inden for det sikrede område, herunder evakuering af personale og sikring af en hurtig reaktion fra et beredskabshold under den berørte sikkerhedsmyndigheds og de eksterne beredskabstjenesters myndighed, hvis det er nødvendigt

i) LSO'en skal straks indberette ethvert brud på sikkerheden, der indtræffer inden for eller involverer et sikret område, til CSA'en med henblik på at fastlægge den passende reaktion

j) individuelle kontorer, rum og pengeskabe i et sikret område skal holdes aflåst, når de efterlades uden opsyn

k) personalet skal undgå at drøfte klassificerede oplysninger på gangarealer eller andre fælles områder i det sikrede område, når ikke-autoriserede personer befinder sig i nærheden.

Artikel 13

Sikkerhedsnøgler og -kombinationer

1. LSO'en har det overordnede ansvar for at sikre korrekt håndtering og opbevaring af nøgler og kombinationer, der anvendes i eller til at få adgang til sikrede områder. Nøgler og kombinationer skal opbevares i en sikkerhedscontainer og beskyttes med mindst samme beskyttelsesniveau som det materiale, de giver adgang til.

2. LSO'en fører et register over sikkerhedscontainere og bokslokaler sammen med en ajourført liste over alle medarbejdere, der har uledsaget adgang til dem.

3. LSO'en fører et register over nøgler til sikkerhedscontainere og bokslokaler, herunder de medarbejdere, som har fået dem tildelt. Der skal opbevares et modtagelsesbevis for hver nøgle, der udstedes, herunder nøgleidentifikation, modtager, dato og klokkeslæt.

4. Nøgler og kombinationer udstedes kun til medarbejdere, der har behov for det, og som har fået den relevante autorisation til at tilgå EUCI. LSO'en skal indsamle enhver nøgle i tilfælde, hvor disse betingelser ikke længere er opfyldt.

5. LSO'en opbevarer reservenøgler og en skriftlig fortegnelse over hver kombinationsindstilling i individuelle forseglede, uigennemsigtige, underskrevne og daterede kuverter, som tilvejebringes af den medarbejder, der er ansvarlig for nøglerne. Disse kuverter skal opbevares i en sikkerhedscontainer, der er godkendt til det højeste klassificeringsniveau for materiale, der opbevares i den relevante beholder eller det relevante bokslokale.

6. Hvis en konvolut i forbindelse med en ændring af kombination eller nøglerotation viser tegn på manipulation eller beskadigelse, skal LSO'en behandle dette som en sikkerhedshændelse og straks underrette CSA'en.

7. Ændringer af kombinationsindstillingerne for sikkerhedscontainere i sikrede områder foretages under tilsyn af LSO'en. Kombinationer skal indstilles på ny mindst hver 12. måned, og når:

a) der modtages en ny beholder eller installeres en ny lås (navnlig skal standardkombinationer ændres med det samme)

b) der er mistanke om kompromittering eller en sådan har fundet sted

c) en person, der er i besiddelse af en kombination, ikke længere har behov herfor.

8. LSO'en fører et register over datoerne for de ændringer af kombinationen, der er omhandlet i stk. 7.

Artikel 14

Planer for nødflytning og nøddestruktion af EUCI

1. LSO'en bistår afdelingschefen med at udarbejde planer for nødflytning og nøddestruktion af EUCI på grundlag af vejledning fra HR.DS.

2. LSO'en sikrer, at alt udstyr, der er nødvendigt for driften af de planer, der er omhandlet i stk. 1, er let tilgængeligt og funktionsdygtigt.

3. LSO'en vurderer sammen med de embedsmænd, der er udpeget i de i stk. 1 omhandlede planer, mindst hver 12. måned planernes parathed, og træffer alle nødvendige foranstaltninger for at ajourføre dem.

Artikel 15

Sikkerhedsgodkendelser

1. LSO'en fører en fortegnelse over alle stillinger i afdelingen, der kræver en sikkerhedsgodkendelse fra Kommissionen, og det personale, der varetager disse stillinger. Kravet om en sikkerhedsgodkendelse skal angives i stillingsopslaget i forbindelse med ansættelsesproceduren og meddeles ansøgeren under samtalen.

2. LSO'en fører tilsyn med alle anmodninger om sikkerhedsgodkendelser med henblik på at få adgang til EUCI. LSO'en er kontaktpunkt i den pågældende tjenestegren og samarbejder med CSA'en om sikkerhedsgodkendelserne.

3. LSO'en indgiver anmodningen om at iværksætte sikkerhedsgodkendelsesproceduren for den pågældende medarbejder og sikrer, at medarbejderen straks sender spørgeskemaet om national sikkerhedsgodkendelse tilbage til CSA'en.

4. LSO'en sikrer, at sikkerhedsgodkendte medarbejdere i afdelingen følger den obligatoriske EUCI-briefing for at opnå deres sikkerhedsgodkendelse.

5. LSO'en holder regelmæssigt kontakt med tjenestegrenens personaletjeneste for at informere om alle ændringer i stillinger, der kræver sikkerhedsgodkendelse, og underretter straks CSA'en om eventuelle ændringer.

6. LSO'en underretter CSA'en om ankomsten af nye medarbejdere, der allerede har sikkerhedsgodkendelse til at tiltræde en stilling, der kræver en sikkerhedsgodkendt medarbejder.

7. LSO'en sikrer, at personalet i afdelingen afslutter proceduren for fornyelse af en sikkerhedsgodkendelse inden for den fastsatte frist. Enhver medarbejder, der nægter at gennemføre proceduren, er forpligtet til at lade sig overflytte til en stilling, som ikke kræver en sikkerhedsgodkendt medarbejder.

Artikel 16

EUCI-arkiv

1. Hvis en afdeling driver et EUCI-arkiv, fører LSO'en tilsyn med RCO'ernes aktiviteter vedrørende håndtering af EUCI og overholdelse af reglerne for sikkerhedsbeskyttelse af EUCI.

2. LSO'en udfører følgende kontroller mindst hver 12. måned og ved udskiftning af en RCO eller en stedfortrædende RCO:

a) en kontrol af en stikprøve af dokumenter i EUCI-arkivet for at bekræfte deres status og nøjagtigheden af arkivet over klassificerede dokumenter

b) en kontrol af en stikprøve af kvitteringer og fremsendelsessedler med henblik på distribution af EUCI til og fra EUCI-arkivet

c) kontrol af en stikprøve af destruktionsattester.

3. LSO'en foretager mindst en gang om måneden stikprøvekontrol af arkivet over klassificerede dokumenter og af nyligt modtagne klassificerede dokumenter for at sikre, at dokumenterne registreres korrekt.

4. Alle kontroller registreres i arkivet med klassificerede dokumenter.

Artikel 17

Andre sikkerhedsopgaver

LSO'ens øvrige sikkerhedsansvar fastlægges i en sikkerhedsmeddelelse, der navnlig omfatter den fysiske sikkerhed for personer, bygninger og andre aktiver samt oplysninger.

KAPITEL 5

ARKIVANSVARLIG (RCO)

Artikel 18

Udpegelse af RCO'en

1. RCO'en og de stedfortrædende RCO'er er tjenestemænd eller midlertidigt ansatte.

2. Alle RCO'er og stedfortrædende RCO'er skal have en gyldig sikkerhedsgodkendelse til at tilgå EUCI op til klassifikationsniveau SECRET UE/EU SECRET og om nødvendigt op til klassifikationsniveau TRES SECRET UE/EU TOP SECRET. RCO'en eller den stedfortrædende RCO skal opnå sikkerhedsgodkendelsen, inden vedkommende udpeges.

3. Kommissionens repræsentationer kan anmode CSA'en om at indrømme en undtagelse fra kravene i stk. 1 og 2.

Artikel 19

Opgaver

1. RCO'er registrerer af sikkerhedshensyn oplysninger, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, når:

a) de overføres til eller forlader en af Kommissionens tjenestegrene eller

b) de overføres til eller forlader et CIS.

2. RCO'er registrerer alle hændelser i livscyklussen for alle informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere. RCO'er sikrer også, at alle informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller tilsvarende, og som udveksles med tredjelande og internationale organisationer, registreres. Dette sker i samordning med det EUCI-arkiv, der forvaltes af Generalsekretariatet.

3. RCO'en registrerer dokumenter, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, i registret over klassificerede dokumenter og sikrer, at de opbevares sikkert i EUCI-arkivet.

4. RCO'en bistår Kommissionens personale med at udarbejde og sende informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere.

5. Når dokumenter, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, modtages fra andre afdelinger eller eksterne parter, sikrer RCO'en, at kvitteringen for levering returneres til udstederen.

6. Inden en medarbejder får adgang til et klassificeret dokument, der opbevares i EUCI-arkivet, kontrollerer RCO'en sammen med LSO'en, at medarbejderen er sikkerhedsgodkendt af CSA'en.

7. RCO'en skal logge alt personale, der kommer ind i og forlader EUCI-arkivet, og som ikke har tilladelse til at have uledsaget adgang, og ledsage dem under hele besøget.

8. Når en medarbejder udtager et dokument med henblik på opslag uden for EUCI-arkivet, sikrer RCO'en, at vedkommende er bekendt med de relevante kompenserende sikkerhedsforanstaltninger, og at medarbejderen returnerer dokumentet, så snart det ikke længere skal bruges. RCO'en minder personalet om at returnere sådanne dokumenter så hurtigt som muligt.

9. EUCI-arkivet udsteder et kurercertifikat, hvis klassificerede dokumenter transporteres i hånden uden for det land, hvor arkivet er beliggende.

10. Detaljerede instrukser til RCO'er om registrering af klassificerede dokumenter skal fremgå af en sikkerheds-meddelelse.

Artikel 20

Nedklassificering og afklassificering

RCO'en bistår de udstedende afdelinger i processen med at gennemgå registreret EUCI for at fastslå, om den oprindelige klassifikationsgrad stadig er hensigtsmæssig, eller om dokumentet kan nedklassificeres eller afklassificeres.

Artikel 21

Destruktion

1. RCO'er er ansvarlige for at destruere informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, ved hjælp af godkendte midler, eventuelt under tilstedeværelse af sikkerhedsgodkendte vidner.

2. RCO'er registrerer enhver destruktion af informationer, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, i arkivet med klassificerede dokumenter og opbevarer de tilsvarende destruktions-attester i EUCI-arkivet.

Artikel 22

Supplerende opgaver

1. RCO'en yder al nødvendig bistand til LSO'en, når LSO'en udfører tilsynsaktiviteter i EUCI-arkivet.

2. RCO'en indberetter alle formodede eller faktiske sikkerhedshændelser til LSO'en, som derefter indberetter dem til CSA'en.

3. RCO'en i EUCI-arkivet tilhørende en af Kommissionens tjenestegrene, der afholder et møde, der er klassificeret på CONFIDENTIEL UE/EU CONFIDENTIAL-niveau eller højere, forbereder de EUCI, der vil blive behandlet på mødet, og koordinerer med mødearrangøren med henblik på at sikre, at alle dokumenter og kvitteringer håndteres i overensstemmelse med de relevante regler.

KAPITEL 6

AFSLUTTENDE BESTEMMELSER

Artikel 23

Gennemsigtighed

Denne afgørelse meddeles Kommissionens ansatte og alle personer, som den gælder for, og offentliggøres i *Den Europæiske Unions Tidende*.

Artikel 24

Denne afgørelse træder i kraft dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 7. april 2022.

På Kommissionens vegne
For formanden
Gertrud INGESTAD
Generaldirektør
Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed