IV

(Oplysninger)

OPLYSNINGER FRA DEN EUROPÆISKE UNIONS INSTITUTIONER, ORGANER, KONTORER OG AGENTURER

TJENESTEN FOR EU'S OPTRÆDEN UDADTIL

AFGØRELSE TRUFFET AF UNIONENS HØJTSTÅENDE REPRÆSENTANT FOR UDENRIGSANLIGGENDER OG SIKKERHEDSPOLITIK

af 19. april 2013

om sikkerhedsbestemmelserne for Tjenesten for EU's Optræden Udadtil

(2013/C 190/01)

UNIONENS HØJTSTÅENDE REPRÆSENTANT FOR UDENRIGSANLIGGENDER OG SIKKERHEDSPOLITIK HAR —

under henvisning til Rådets afgørelse af 26. juli 2010 om, hvordan Tjenesten for EU's Optræden Udadtil ("EU-Udenrigstjenesten") skal tilrettelægges og fungere [1] (2010/427/EU),

under henvisning til udtalelse fra det udvalg, der er omhandlet i artikel 9, stk. 6, i afgørelsen truffet af den højtstående repræsentant af 15. juni 2011 om sikkerhedsbestemmelserne for Tjenesten for EU's Optræden Udadtil [2],

under henvisning til udtalelse fra det udvalg, der er omhandlet i artikel 10, stk. 1, i Rådets afgørelse af 26. juli 2010 om, hvordan EU-Udenrigstjenesten skal tilrettelægges og fungere (2010/427/EU), og

ud fra følgende betragtninger:

(1) EU-Udenrigstjenesten bør som et uafhængigt fungerende EU-organ have sikkerhedsbestemmelser som anført i artikel 10, stk. 1, i Rådets afgørelse 2010/427/EU.

(2) Den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik (i det følgende benævnt "den højtstående repræsentant" eller "HR") bør fastsætte sikkerhedsbestemmelser for EU-Udenrigstjenesten, der omfatter alle sikkerhedsaspekter vedrørende EU-Udenrigstjenestens drift, således at den effektivt kan styre risici for sit personale, sine fysiske aktiver, informationer og besøgende og opfylde sin pligt til at udvise rettidig omhu ("diligenspligt") i denne henseende.

(3) Navnlig bør personale under EU-Udenrigstjenestens ansvar, dens fysiske aktiver, herunder kommunikations- og informationssystemer, samt besøgende sikres et beskyttelsesniveau, der ligger på linje med bedste praksis i Rådet, Kommissionen, medlemsstaterne og om relevant internationale organisationer.

(4) Sikkerhedsbestemmelserne for EU-Udenrigstjenesten bør bidrage til at opnå en mere sammenhængende generel EU-ramme for beskyttelse af EU's klassificerede informationer (i det følgende benævnt "EUCI") og bør bygge på og være i størst mulig overensstemmelse med sikkerhedsreglerne for Rådet for den Europæiske Union (i det følgende benævnt "Rådet") og sikkerhedsbestemmelserne for Europa-Kommissionen.

(5) EU-Udenrigstjenesten, Rådet og Kommissionen er fast besluttet på at anvende ækvivalente sikkerhedsstandarder for beskyttelse af EUCI.

(6) Denne afgørelse gælder med forbehold af artikel 15 og 16 i traktaten om Den Europæiske Unions funktionsmåde og retsakter til gennemførelse heraf.

(7) Det er nødvendigt at tilrettelægge sikkerheden i EU-Udenrigstjenesten og fordelingen af sikkerhedsopgaver inden for EU-Udenrigstjenestens strukturer.

[1] EUT L 201 af 3.8.2010, s. 30.
[2] EUT C 304 af 15.10.2011, s. 5.

(8) Den højtstående repræsentant bør trække på relevant ekspertise i medlemsstaterne, i Generalsekretariatet for Rådet og i Kommissionen efter behov.

(9) Den højtstående repræsentant bør træffe alle passende foranstaltninger, der er nødvendige for gennemførelsen af disse bestemmelser med støtte fra medlemsstaterne, Generalsekretariatet for Rådet og Kommissionen —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Formål og anvendelsesområde

I denne afgørelse fastsættes sikkerhedsbestemmelserne for Tjenesten for EU's Optræden Udadtil (i det følgende benævnt "EU-Udenrigstjenestens sikkerhedsbestemmelser").

I henhold til artikel 10, stk. 1, i Rådets afgørelse af 26. juli 2010 om, hvordan EU-Udenrigstjenesten skal tilrettelægges og fungere (2010/427/EU), finder bestemmelserne anvendelse på hele EU-Udenrigstjenestens personale og alle Unionens delegationer uanset deres administrative status eller oprindelse, og de udgør den generelle lovramme for effektiv styring af de risici, som personale under EU-Udenrigstjenestens ansvar, jf. artikel 2, EU-Udenrigstjenestens lokaliteter, fysiske aktiver, informationer og besøgende udsættes for.

Artikel 2

Definitioner

I denne afgørelse forstås ved:

a) "personale i EU-Udenrigstjenesten": tjenestemænd og øvrige ansatte i EU-Udenrigstjenesten, herunder midlertidigt ansatte i medlemsstaternes diplomatiske tjenester, udstationerede nationale eksperter, jf. definitionen i artikel 6 i Rådets afgørelse af 26. juli 2010 om, hvordan Tjenesten for EU's Optræden Udadtil skal tilrettelægges og fungere (2010/427/EU)

b) "personale under EU-Udenrigstjenestens ansvar": EU-Udenrigstjenestens personale og alt personale i EU-delegationer, uanset deres administrative status eller oprindelse, samt, for så vidt angår denne afgørelse, den højtstående repræsentant og alt efter omstændighederne andet personale fra EU-Udenrigstjenestens hovedkontor

c) "pårørende": familiemedlemmer til personalet under EU-Udenrigstjenestens ansvar i EU-delegationer, og som udgør en del af deres respektive husstand, jf. underretning til udenrigsministeriet i modtagerstaten

d) "EU-Udenrigstjenestens lokaliteter": alle EU-Udenrigstjenestens lokaliteter, herunder bygninger, kontorer, lokaler og andre områder samt områder, der rummer kommunikations- og informationssystemer (herunder systemer til håndtering af EUCI), hvor EU-Udenrigstjenesten permanent eller midlertidigt gennemfører aktiviteter

e) "EU-Udenrigstjenestens sikkerhedsinteresser": personale under EU-Udenrigstjenestens ansvar, EU-Udenrigstjenestens lokaliteter, pårørende, fysiske aktiver, herunder kommunikations- og informationssystemer, informationer og besøgende

f) "EUCI": informationer eller materiale, der er mærket med en EU-klassifikationsgrad, og hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes interesser skade i forskellig grad.

Øvrige definitioner fremgår af de relevante bilag og tillæg A.

Artikel 3

Diligenspligt

1. EU-Udenrigstjenestens sikkerhedsbestemmelser har til formål at opfylde EU-Udenrigstjenestens diligenspligt.

2. EU-Udenrigstjenestens diligenspligt omfatter diligens med hensyn til at iværksætte alle rimelige tiltag til gennemførelse af sikkerhedsforanstaltninger for at forhindre den skadeforvoldelse på EU-Udenrigstjenestens sikkerhedsinteresser, der med rimelighed kan forudses.

Pligten omfatter diverse sikkerhedskomponenter, herunder som følge af nødsituationer eller kriser, uanset karakter.

3. På baggrund af den diligenspligt, der påhviler medlemsstaterne, EU's institutioner eller organer og øvrige parter med personale i EU-delegationer og/eller i EU-delegationslokaliteter, eller EU-Udenrigstjenestens pligt, når EU-delegationer har til huse i ovennævnte øvrige parters lokaliteter, skal EU-Udenrigstjenesten indgå administrative ordninger med hver enkelt af ovenstående enheder med henblik på at afklare de respektive roller og ansvarsområder, opgaver og samarbejdsordninger.

Artikel 4

Fysisk sikkerhed og infrastruktursikkerhed

1. EU-Udenrigstjenesten iværksætter alle relevante fysiske sikkerhedsforanstaltninger (det være sig af permanent eller midlertidig karakter), herunder adgangskontrolordninger, for alle EU-Udenrigstjenestens lokaliteter med henblik på at beskytte EU-Udenrigstjenestens sikkerhedsinteresser. Der skal tages højde for disse foranstaltninger ved tegningen og planlægningen af nye lokaliteter eller inden leje af eksisterende lokaliteter.

2. I tredjelande iværksætter EU-Udenrigstjenesten også alle relevante supplerende fysiske sikkerhedsforanstaltninger, det være sig af permanent eller midlertidig karakter, med henblik på at beskytte sine sikkerhedsinteresser.

Med dette formål for øje kan personalet under EU-Udenrigstjenestens ansvar og de pårørende af sikkerhedsmæssige grunde og i en specifik periode samt i specifikke områder pålægges særlige forpligtelser eller restriktioner.

3. De i stk. 1 og 2 omhandlede foranstaltninger skal stå i et rimeligt forhold til den vurderede risiko.

Artikel 5

Beskyttelse af klassificerede informationer

1. Beskyttelsen af EUCI skal underlægges de krav, der er fastsat i denne afgørelse, og især i bilag A. Den, der er i besiddelse af enhver form for EUCI, bærer ansvaret for at beskytte de pågældende informationer i henhold hertil.

2. EU-Udenrigstjenesten sikrer, at der kun gives adgang til klassificerede informationer til personer, der opfylder betingelserne som fastsat i bilag A, artikel 5.

3. De betingelser, hvorunder lokalt ansatte kan få adgang til EUCI, fastsættes også af den højtstående repræsentant, jf. bestemmelserne om beskyttelse af EUCI i bilag A til denne afgørelse.

4. Sikkerhedsdirektoratet i EU-Udenrigstjenesten forvalter en database vedrørende sikkerhedsgodkendelsesstatus for alt personale under EU-Udenrigstjenestens ansvar og for EU-Udenrigstjenestens kontrahenter.

5. Hvis medlemsstaterne bringer klassificerede informationer med en national klassifikationsmærkning ind i EU-Udenrigstjenestens strukturer eller netværk, beskytter EU-Udenrigstjenesten disse informationer i overensstemmelse med de krav, der gælder for EUCI med en tilsvarende klassifikationsgrad, jf. de gældende bestemmelser i bilag A til denne afgørelse.

6. Områder i EU-Udenrigstjenesten, hvor informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere eller tilsvarende, opbevares, afgrænses som sikrede områder i overensstemmelse med bilag A til denne afgørelse og godkendes af EU-Udenrigstjenestens sikkerhedsmyndighed.

7. Procedurer for den højtstående repræsentants ansvar inden for rammerne af de aftaler eller administrative ordninger, der findes for udvekslingen af EUCI med tredjelande eller internationale organisationer, er beskrevet i bilag A og A VI til denne afgørelse.

Artikel 6

Sikkerhedsrelaterede hændelser og nødsituationer

1. For at sikre en rettidig og effektiv reaktion på sikkerhedsrelaterede hændelser udarbejder EU-Udenrigstjenesten et system til indberetning af sådanne hændelser og nødsituationer, som skal fungere i døgndrift alle ugens dage og omfatte enhver form for sikkerhedsrelaterede hændelser eller trusler mod EU-Udenrigstjenestens sikkerhedsinteresser (f.eks. ulykker, konflikter, ondsindede handlinger, kriminelle handlinger, kidnapnings- og gidselsituationer, lægelige nødsituationer, hændelser med kommunikations- og informationssystemer, cyberangreb osv.).

2. Der etableres nødsituationsforbindelseskanaler mellem EU-Udenrigstjenestens hovedkontor, EU-delegationer, Rådet, Kommissionen, EU's særlige repræsentanter og medlemsstaterne for at støtte dem med at håndtere sikkerhedsrelaterede hændelser, der involverer personale, og konsekvenserne deraf, herunder beredskabsplaner.

3. Denne håndtering af sikkerhedsrelaterede hændelser skal bl.a. omfatte:

— procedurer for effektiv støtte i forbindelse med beslutningsprocessen vedrørende en sikkerhedshændelse, der involverer personale, herunder beslutninger vedrørende tilbagetrækning eller afbrydelse af en tjenesterejse

— en politik og procedurer for genfinding af personale – f.eks. i tilfælde af forsvundne medarbejdere eller kidnapnings- og gidselsituationer – under hensyntagen til medlemsstaternes, EU-institutionernes og EU-Udenrigstjenestens særlige ansvar desangående. Behovet for specifikke kompetencer vedrørende forvaltning af disse aktiviteter i denne sammenhæng skal overvejes under hensyntagen til de ressourcer, som medlemsstaterne kan tilvejebringe.

4. EU-Udenrigstjenesten indfører relevante administrative ordninger til indberetning af sikkerhedsrelaterede hændelser i EU-delegationer. Medlemsstaterne, Kommissionen, eventuelle andre relevante myndigheder samt de relevante sikkerhedsudvalg informeres.

5. Hændelseshåndteringsprocesserne bør udøves og revideres regelmæssigt.

Artikel 7

Kommunikations- og informationssystemernes sikkerhed

1. EU-Udenrigstjenesten skal beskytte informationer, der håndteres i kommunikations- og informationssystemer ("CIS'er"), mod trusler mod fortrolighed, integritet, tilgængelighed, autenticitet og uafviselighed.

2. EU-Udenrigstjenestens sikkerhedsmyndighed, jf. definitionen i artikel 12, afsnit 1, stk. 1, skal vedtage bestemmelser, en sikkerhedspolitik og et sikkerhedsprogram til beskyttelse af alle CIS'er, der ejes eller drives af EU-Udenrigstjenesten.

3. Bestemmelserne, politikken og programmet skal være i overensstemmelse med - og gennemførelsen deraf koordineres nøje med - Rådets og Kommissionens tilsvarende bestemmelser/politik/program og alt efter omstændighederne med de sikkerhedspolitikker, medlemsstaterne gør brug af.

4. Alle kommunikations- og informationssystemer, der håndterer klassificerede informationer, skal undergå en godkendelsesproces. EU-Udenrigstjenesten anvender en ordning for sikkerhedsgodkendelse i samråd med Generalsekretariatet for Rådet og Europa-Kommissionen.

5. Hvis beskyttelsen af EUCI, der håndteres af EU-Udenrigstjenesten, sker ved hjælp af kryptoprodukter, skal sådanne produkter være godkendt af EU-Udenrigstjenestens kryptogodkendelsesmyndighed på anbefaling fra Rådets Sikkerhedsudvalg.

6. EU-Udenrigstjenestens sikkerhedsmyndighed etablerer efter behov følgende informationssikringsfunktioner:

a) en informationssikringsmyndighed

b) en Tempestmyndighed

c) en kryptogodkendelsesmyndighed

d) en kryptodistributionsmyndighed.

7. For hvert system fastsætter EU-Udenrigstjenestens sikkerhedsmyndighed følgende funktioner:

a) en sikkerhedsakkrediteringsmyndighed

b) en operationel informationssikringsmyndighed.

8. Bestemmelser om gennemførelse af denne artikel med hensyn til beskyttelse af EUCI findes i bilag A og A IV.

Artikel 8

Brud på sikkerheden og kompromittering af klassificerede informationer

1. Der er tale om brud på sikkerheden, når en person foretager eller undlader at foretage en handling, og dette er i strid med sikkerhedsbestemmelserne i denne afgørelse og/eller sikkerhedspolitikkerne eller retningslinjerne om alle nødvendige foranstaltninger til gennemførelse deraf som vedtaget i henhold til artikel 20, stk. 1.

2. Der er tale om kompromittering af klassificerede informationer, når de helt eller delvist er blevet videregivet til uautoriserede personer eller enheder.

3. Ethvert brud eller formodet brud på sikkerheden og enhver kompromittering eller formodet kompromittering af klassificerede informationer indberettes straks til EU-Udenrigstjenestens Sikkerhedsdirektorat, der vil træffe passende foranstaltninger, jf. bilag A.

4. Enhver, der er ansvarlig for et brud på sikkerhedsbestemmelserne som fastlagt i denne afgørelse eller for kompromittering af klassificerede informationer, kan gøres til genstand for disciplinære foranstaltninger og/eller retsforfølges i overensstemmelse med gældende love, regler og bestemmelser, jf. i bilag A, artikel 11, stk. 3.

Artikel 9

Efterforskning af sikkerhedsrelaterede hændelser, brud og/eller kompromittering og afhjælpende foranstaltninger

1. EU-Udenrigstjenestens Sikkerhedsdirektorat skal bistået af eksperter fra medlemsstaterne og/eller eventuelt fra andre EU-institutioner og alt efter omstændighederne efter godkendelse fra den administrerende direktør:

a) foretage undersøgelser eller kontroller alt efter omstændighederne:

   i) hvis det konstateres, eller hvis der er rimelig grund til at formode, at klassificerede informationer, som er relevante for EU-Udenrigstjenesten, er blevet kompromitteret eller bortkommet

   ii) ved ethvert reelt eller formodet brud på sikkerheden eller andre sikkerhedsrelaterede hændelser eller trusler rettet mod EU-Udenrigstjenestens sikkerhedsinteresser

b) gennemføre eventuelle nødvendige afhjælpende foranstaltninger som følge af undersøgelser, når det efter omstændighederne er passende.

2. Undersøgelsespersonalet skal have adgang til samtlige informationer, der er nødvendige til udførelse af sådanne undersøgelser, og skal i den sammenhæng støttes fuldt ud af alle EU-Udenrigstjenestens tjenester.

Undersøgelsespersonalet kan iværksætte relevante tiltag for at sikre bevismaterialet på en måde, der står i et rimeligt forhold til den efterforskede sags alvor.

3. Hvis der er tale om adgang til informationer vedrørende personoplysninger, herunder oplysninger i kommunikations- og informationssystemer, skal denne adgang være i overensstemmelse med forordning (EF) nr. 45/2001.

4. Hvis det er nødvendigt at oprette en efterforskningsdatabase, der indeholder personoplysninger, underrettes Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) som angivet i ovennævnte forordning.

Artikel 10

Sikkerhedsrisikostyring

1. Med henblik på at fastslå sine behov for sikkerhedsforanstaltninger udarbejder EU-Udenrigstjenesten i snævert samarbejde med Kommissionens Sikkerhedsdirektorat og alt efter omstændighederne med Sikkerhedskontoret ved Generalsekretariatet for Rådet en omfattende metode til vurdering af sikkerhedsrisikoen.

2. Risici for EU-Udenrigstjenestens sikkerhedsinteresser forvaltes som en proces. Denne proces sigter mod at bestemme kendte sikkerhedsrisici, definere sikkerhedsforanstaltninger for at begrænse sådanne risici til et acceptabelt niveau og anvende foranstaltninger i overensstemmelse med begrebet forsvar i dybden. Effektiviteten af sådanne foranstaltninger samt risikoniveauet vurderes løbende.

3. De roller, ansvarsområder og opgaver, der er fastsat i denne afgørelse, berører ikke det ansvar, der påhviler hver enkelt medarbejder under EU-Udenrigstjenestens ansvar. Især skal særlige EU-medarbejdere, der er på tjenesterejse i tredjelande, udvise almindelig sund fornuft og god dømmekraft med hensyn til deres egen sikkerhed samt leve op til alle gældende sikkerhedsbestemmelser, forordninger, procedurer og instruktioner.

4. EU-Udenrigstjenesten træffer alle rimelige foranstaltninger for at sikre, at dens sikkerhedsinteresser beskyttes, og for at forhindre med rimelighed forudseelige skader herpå.

5. Sikkerhedsforanstaltningerne i EU-Udenrigstjenesten til beskyttelse af klassificerede informationer i hele deres levetid skal stå i et rimeligt forhold til især sikkerhedsklassificeringen, formen og omfanget af informationerne eller materialet, placeringen og konstruktionen af faciliteter, der indeholder klassificerede informationer, og den pågældende trussel, herunder den lokalt vurderede trussel, om ondsindede og/eller kriminelle aktiviteter, herunder spionage, sabotage og terrorisme.

Artikel 11

Sikkerhedsbevidsthed og -uddannelse

1. EU-Udenrigstjenestens sikkerhedsmyndighed sikrer, at der udarbejdes og gennemføres relevante sikkerhedsbevidstheds- og sikkerhedsuddannelsesprogrammer, og at personale under EU-Udenrigstjenestens ansvar samt, hvor det er relevant, deres pårørende får den fornødne bevidsthedsorientering og -uddannelse, der svarer til de risici, som er dér, hvor de arbejder eller bor.

2. Inden de får adgang til EUCI og med jævne mellemrum derefter, skal medarbejdere gøres bekendt med og erkende deres pligter med hensyn til at beskytte EUCI som angivet i bestemmelserne i henhold til artikel 5.

Artikel 12

Tilrettelæggelse af sikkerheden i EU-Udenrigstjenesten

Afsnit 1

Almene bestemmelser

1. Den administrerende direktør (COO) er sikkerhedsmyndigheden for EU-Udenrigstjenesten. I denne egenskab sørger COO'en for, at:

a) sikkerhedsforanstaltningerne i nødvendigt omfang koordineres med de kompetente myndigheder i medlemsstaterne, Generalsekretariatet for Rådet og Europa-Kommissionen og, hvis det er relevant, med tredjelande eller internationale organisationer i alle sikkerhedsspørgsmål, der er relevante for EU-Udenrigstjenestens aktiviteter, herunder med hensyn til arten af trusler mod sikkerheden for personale, fysiske aktiver og informationer og beskyttelsesforanstaltningerne over for disse trusler

b) der fra starten fuldt ud tages hensyn til sikkerhedsaspekterne i forbindelse med alle EU-Udenrigstjenestens aktiviteter

c) der kun gives adgang til klassificerede informationer til personer, der opfylder betingelserne som fastsat i bilag A, artikel 5

d) der etableres et registreringssystem, som sikrer, at oplysninger, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, håndteres i overensstemmelse med denne afgørelse i EU-Udenrigstjenesten, og når oplysningerne videregives til EU's medlemsstater, EU-institutioner, -organer eller -agenturer eller andre godkendte modtagere. Der føres et separat register over samtlige EUCI, EU-Udenrigstjenesten videregiver til tredjelande og internationale organisationer, og over samtlige klassificerede informationer, der modtages fra tredjelande eller internationale organisationer

e) der foretages sikkerhedsinspektioner, jf. artikel 15

f) der gennemføres undersøgelser af alle brud på eller mistanker om brud på sikkerheden, herunder kompromittering eller bortkomst af klassificerede informationer, som EU-Udenrigstjenesten er i besiddelse af eller har udarbejdet, og at de relevante sikkerhedsmyndigheder anmodes om at bistå med sådanne undersøgelser

g) der for at give et rettidigt og effektivt svar på sikkerhedshændelser etableres passende forvaltningsplaner og -mekanismer for hændelser og konsekvenser

h) der træffes relevante foranstaltninger, hvis en person ikke overholder denne afgørelse

i) der indføres relevante fysiske og organisatoriske foranstaltninger til beskyttelse af EU-Udenrigstjenestens sikkerhedsinteresser.

I den forbindelse skal COO'en efter samråd med den administrerende generalsekretær:

— fastsætte sikkerhedskategorien for delegationerne efter samråd med Kommissionen

— efter samråd med HR beslutte, hvornår delegationspersonale bør evakueres, hvis sikkerhedssituationen kræver det

— beslutte hvilke foranstaltninger, der skal finde anvendelse til beskyttelse af pårørende, hvis dette er aktuelt, under hensyntagen til de ordninger med EU-institutioner, der henvises til i artikel 3, stk. 3

— godkende kryptokommunikationspolitikken, især programmet til installering af kryptoprodukter og mekanismer.

2. COO'en skal i dette hverv bistås af direktøren for finansielle og administrative anliggender, af lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat og eventuelt af den administrerende direktør for krisestyring og operationel koordinator.

3. COO'en kan som EU-Udenrigstjenestens sikkerhedsmyndighed og alt efter omstændighederne uddelegere opgaver i så henseende.

4. Hver afdelings- og divisionsleder er ansvarlig for at gennemføre bestemmelser til beskyttelse af EUCI i vedkommendes afdeling eller division.

Hver afdelings- eller divisionsleder er ansvarlig som angivet ovenfor og udpeger medarbejdere til en afdelingssikkerhedskoordinatorfunktion, hvis ressourcer skal stå i et rimeligt forhold til mængden af EUCI, der håndteres af den pågældende afdeling eller division.

Afdelingssikkerhedskoordinatorer skal alt efter omstændighederne bistå og støtte deres afdelings- eller divisionsleder med at udføre sikkerhedsrelaterede opgaver som f.eks.:

a) udarbejdelse af eventuelle yderligere sikkerhedskrav, der er relevante for de specifikke behov i afdelingen eller divisionen

b) periodisk sikkerhedsorientering af afdelingens eller divisionens medarbejdere

c) sikring af, at "need-to-know"-princippet overholdes i deres afdeling eller division

d) vedligeholdelse af en opdateret liste over sikkerhedskoder og nøgler

e) vedligeholdelse af sikkerhedsbestemmelser og sikkerhedsforanstaltninger

f) indberetning af eventuelle brud på sikkerheden og/eller kompromittering af EUCI både til vedkommendes leder og sikkerhedsdirektoratet

g) debriefing af medarbejdere, der fratræder EU-Udenrigstjenesten

h) udarbejdelse af regelmæssige rapporter via organisationens hierarki om afdelingens eller divisionens sikkerhedsanliggender

i) tæt samarbejde med EU-Udenrigstjenestens Sikkerhedsdirektorat om sikkerhedsanliggender.

Alle aktiviteter eller spørgsmål, som kan få indvirkning på sikkerheden, skal i rette tid indrapporteres til EU-Udenrigstjenestens Sikkerhedsdirektorat.

5. Hver leder af en EU-delegation er ansvarlig for at gennemføre alle foranstaltninger vedrørende sikkerheden i EU-delegationen.

Afsnit 2

EU-Udenrigstjenestens Sikkerhedsdirektorat

1. EU-Udenrigstjenesten skal have et sikkerhedsdirektorat. Dets opgave er at:

a) forvalte, koordinere, overvåge og/eller gennemføre alle sikkerhedsforanstaltninger i alle lokaliteter, som EU-Udenrigstjenesten har ansvaret for, i hovedkontoret, i EU og i tredjelande

b) sikre sammenhæng og overensstemmelse med denne afgørelse og med gennemførelsesbestemmelser for enhver aktivitet, som kan have en indvirkning på beskyttelse af EU-Udenrigstjenestens sikkerhedsinteresser

c) være den primære rådgiver for HR, den administrerende generalsekretær og COO'en vedrørende alle sikkerhedsrelaterede anliggender

d) modtage bistand fra de kompetente tjenester i medlemsstaterne i henhold til artikel 10, stk. 3, i Rådets afgørelse 2010/427/EU om, hvordan Tjenesten for EU's Optræden Udadtil skal tilrettelægges og fungere,

e) støtte aktiviteterne i EU-Udenrigstjenestens sikkerhedsakkrediteringsmyndighed ved at foretage fysiske sikkerhedsvurderinger af det generelle sikkerhedsmiljø (GSE)/lokale sikkerhedsmiljø (LSE) ved kommunikations- og informationssystemer til håndtering af EUCI og af lokaliteter, der skal godkendes til håndtering og opbevaring af EUCI.

2. Lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat har ansvaret for at:

a) sikre den overordnede beskyttelse af EU-Udenrigstjenestens sikkerhedsinteresser

b) udarbejde, gennemgå og opdatere sikkerhedsbestemmelserne og koordinere sikkerhedsforanstaltninger med de kompetente myndigheder i medlemsstaterne og efter omstændighederne de kompetente myndigheder i tredjelande og internationale organisationer, der har tilknytning til EU i kraft af sikkerhedsaftaler og/eller -ordninger

c) støtte arbejdet i EU-Udenrigstjenestens Sikkerhedsudvalg, jf. artikel 14, stk. 1, i denne afgørelse

d) samarbejde med andre parter eller myndigheder end de i b) ovenfor omtalte om sikkerhedsanliggender, når dette er hensigtsmæssigt

e) prioritere og fremsætte forslag til styring af budgettet for sikkerhed på hovedkontoret og i EU-delegationer.

3. Lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat skal:

a) sikre, at brud på sikkerheden og kompromitteringer registreres, og at der om nødvendigt iværksættes og foretages undersøgelser

b) mødes regelmæssigt – og når det måtte anses for nødvendigt – for at drøfte områder af fælles interesse med sikkerhedsdirektøren for Generalsekretariatet for Rådet og direktøren for Kommissionens Sikkerhedsdirektorat.

4. EU-Udenrigstjenestens Sikkerhedsdirektorat etablerer kontakt og opretholder tæt samarbejde med:

— de afdelinger, der har ansvaret for sikkerhed i udenrigsministerierne i medlemsstaterne

— de nationale sikkerhedsmyndigheder (NSA'er) og/eller de andre kompetente sikkerhedsmyndigheder i medlemsstaterne for at få hjælp til at tilvejebringe de nødvendige informationer for at kunne vurdere de farer og trusler, som EU-Udenrigstjenesten, dens medarbejdere, dens aktiviteter, dens aktiver og ressourcer og dens klassificerede informationer måtte stå over for på den sædvanlige forretningsadresse

— de kompetente sikkerhedsmyndigheder i medlemsstaterne eller værtsstaterne i det område, hvor EU-Udenrigstjenesten kan udøve sin aktivitet, for så vidt angår alle spørgsmål vedrørende beskyttelse af dens medarbejdere, dens aktivitet, dens aktiver og ressourcer samt dens klassificerede informationer på deres område

— Sikkerhedskontoret ved Generalsekretariatet for Rådet og Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed samt alt efter omstændighederne sikkerhedsafdelingerne i de andre EU-institutioner, -organer og -agenturer

— sikkerhedsafdelingerne i tredjelande eller internationale organisationer med henblik på eventuel nyttig koordinering

— medlemsstaternes NSA'er vedrørende alle sager i forbindelse med beskyttelse af EUCI.

Afsnit 3

EU-delegationer

1. Hver leder af en EU-delegation har ansvaret for lokalt at gennemføre og forvalte alle foranstaltninger vedrørende beskyttelse af EU-Udenrigstjenestens sikkerhedsinteresser i EU-delegationers lokaliteter og inden for deres kompetenceområde.

I samråd med de kompetente myndigheder i værtsstaten, når dette er nødvendigt, træffer vedkommende alle rimeligt gennemførlige foranstaltninger for at sikre, at der indføres relevante fysiske og organisatoriske foranstaltninger med henblik på at nå dette mål.

Delegationslederen udarbejder sikkerhedsbestemmelser til beskyttelse af de pårørende som fastlagt i artikel 2, litra c), om fornødent under hensyntagen til eventuelle administrative ordninger, jf. artikel 3, stk. 3. Delegationslederen aflægger en årlig beretning om alle sikkerhedsrelaterede spørgsmål inden for vedkommendes kompetenceområde til lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat.

Vedkommende skal i disse hverv bistås af EU-Udenrigstjenestens Sikkerhedsdirektorat, personalet i EU-Udenrigstjenesten i den delegation, der udøver dedikerede sikkerhedsopgaver og -funktioner og dedikeret sikkerhedspersonale, som er placeret, hvor der måtte vise sig behov.

2. Desuden skal delegationslederen:

— udarbejde detaljerede sikkerheds- og beredskabsplaner for delegationen på grundlag af overordnede standarddriftsprocedurer

— drive et effektivt system, der fungerer døgnet rundt, til håndtering af sikkerhedsrelaterede hændelser og nødsituationer inden for delegationens aktivitetsområde

— sikre, at alle medarbejdere tilknyttet delegationen er omfattet af en forsikring som krævet af omstændighederne i området

— sørge for, at sikkerhed indgår i den oplæring i arbejdsopgaver, som EU-delegationen giver alle medarbejdere, der indsættes i delegationen, inden eller efter de kommer til delegationen

— sikre, at eventuelle anbefalinger som følge af sikkerhedsvurderinger gennemføres, og med jævne mellemrum udarbejde skriftlige rapporter om gennemførelsen og om andre sikkerhedsanliggender til EU-Udenrigstjenestens sikkerhedsmyndighed.

3. Samtidig med at delegationslederen har ansvaret for at beskytte sikkerhedsforvaltningen samt sikre virksomhedsmæssig fleksibilitet, kan vedkommende uddelegere gennemførelsen af vedkommendes sikkerhedsopgaver til delegationens sikkerhedskoordinator ("DSC"), som kan være souschefen i delegationen eller, hvis der ikke er udnævnt nogen, en anden passende person.

Navnlig kan følgende ansvarsområder overdrages til DSC:

— at have tæt kontakt vedrørende sikkerhedsanliggender med kompetente myndigheder i værtsnationen og de relevante tilsvarende myndigheder ved medlemsstaternes ambassader og diplomatiske missioner

— at gennemføre relevante sikkerhedsforvaltningsprocedurer i forbindelse med EU-Udenrigstjenestens sikkerhedsinteresser, herunder beskyttelse af EUCI

— at gøre medarbejderne bekendt med de sikkerhedsbestemmelser, som er gældende for dem, og om de specifikke risici i værtslandet

— at forelægge anmodninger for EU-Udenrigstjenestens Sikkerhedsdirektorat vedrørende de stillinger, der kræver en personelsikkerhedsgodkendelse (PSC)

— at holde lederen af delegationen, den regionale sikkerhedsansvarlige (RSO) og EU-Udenrigstjenestens Sikkerhedsdirektorat løbende orienteret om hændelser eller udviklingstendenser i området, som har indflydelse på beskyttelsen af EU-Udenrigstjenestens sikkerhedsinteresser.

4. Delegationslederen kan uddelegere sikkerhedsopgaver af administrativ eller teknisk karakter til administrationslederen og andre delegationsmedarbejdere.

5. EU-delegationen bistås af en regional sikkerhedsansvarlig (RSO). RSO'erne påtager sig de nedenfor fastlagte roller i delegationerne inden for deres respektive geografiske ansvarsområder.

Under visse omstændigheder kan en dedikeret RSO, hvis de fremherskende sikkerhedsforhold dikterer det, afsættes til en specifik delegation som fuldtidsmedarbejder.

En RSO kan blive bedt om at flytte væk fra vedkommendes nuværende ansvarsområde, herunder hovedkontoret i Bruxelles, eller endda påtage sig en stilling med bopælspligt alt efter den aktuelle sikkerhedssituation i et givet land og som foreskrevet af EU-Udenrigstjenestens Sikkerhedsdirektorat.

6. RSO'erne er hierarkisk direkte underordnet EU-Udenrigstjenestens Sikkerhedsdirektorat, men under direkte funktionsmæssig og administrativ kontrol af den pågældende delegationsleder. De skal bistå delegationslederen og delegationsmedarbejderne med at arrangere og gennemføre alle fysiske, organisatoriske og proceduremæssige foranstaltninger i forbindelse med sikkerheden for alle delegationsmedarbejdere uanset deres administrative oprindelse.

7. RSO'er giver delegationslederen og delegationsmedarbejderne vejledning og støtte. Hvor det er relevant, og især hvis en dedikeret RSO er fuldtidsmedarbejder, kan vedkommende bistå en EU-delegation med sikkerhedsforvaltning og -gennemførelse, herunder udarbejdelse af sikkerhedskontrakter og forvaltning af sikkerhedsakkrediteringer og -godkendelser.

Artikel 13

FSFP-operationer og EU's særlige repræsentanter

EU-Udenrigstjenestens Sikkerhedsdirektorat bistår og rådgiver direktøren for Direktoratet for Krisestyring og Planlægning (CMPD), generaldirektøren for EU's' Militærstab (EUMS), den civile operationschef, der leder Den Civile Planlægnings- og Gennemførelseskapacitet (CPCC) og EU's øverstbefalende for militæroperationer vedrørende sikkerhedsaspekter ved FSFP-operationer og EU's særlige repræsentanter vedrørende sikkerhedsaspekter ved deres mandat som supplement til de specifikke bestemmelser, der findes i så henseende i de relevante politikker, der er vedtaget af Rådet.

Artikel 14

EU-Udenrigstjenestens Sikkerhedsudvalg

1. Der nedsættes hermed et sikkerhedsudvalg i EU-Udenrigstjenesten.

Det har COO'en eller en udpeget repræsentant som formand og skal afholde møder som pålagt af formanden eller på anmodning fra et af udvalgsmedlemmerne. EU-Udenrigstjenestens Sikkerhedsdirektorat skal støtte formanden i dennes funktion og alt efter omstændighederne yde administrativ bistand i forbindelse med udvalgets arbejde.

2. EU-Udenrigstjenestens Sikkerhedsudvalg består af repræsentanter fra:

— hver enkelt medlemsstat

— Sikkerhedskontoret ved Generalsekretariatet for Rådet

— Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed.

En medlemsstatsdelegation til EU-Udenrigstjenestens Sikkerhedsudvalg kan bestå af medlemmer af:

— den nationale sikkerhedsmyndighed og/eller den udpegede sikkerhedsmyndighed

— de afdelinger, der har sikkerhedsansvaret i udenrigsministerierne.

3. Udvalgets repræsentanter kan ledsages og rådgives af eksperter, således som repræsentanterne anser det for nødvendigt. Repræsentanter fra andre EU-institutioner, -agenturer eller -organer kan anmodes om at deltage, når der drøftes spørgsmål, som er relevante for deres sikkerhed.

4. Med forbehold af stk. 5 nedenfor bistår EU-Udenrigstjenestens Sikkerhedsudvalg ved hjælp af høringer EU-Udenrigstjenesten vedrørende alle sikkerhedsspørgsmål, der er relevante for EU-Udenrigstjenestens aktiviteter, hovedkontoret og EU-delegationerne.

Navnlig med forbehold af stk. 5 nedenfor gælder følgende:

a) EU-Udenrigstjenestens Sikkerhedsudvalg skal høres i forbindelse med:

   — sikkerhedspolitikker, retningslinjer, koncepter eller andre dokumenter om metoderne i forbindelse med sikkerhed, især med hensyn til beskyttelse af klassificerede informationer og de foranstaltninger, der skal træffes i tilfælde af, at personale i EU-Udenrigstjenesten ikke overholder sikkerhedsbestemmelserne

   — tekniske sikkerhedsaspekter, der kan påvirke HR's afgørelser om at fremsætte en henstilling til Rådet om at indlede forhandlinger vedrørende informationssikkerhedsaftaler, jf. bilag A, artikel 10, stk. 1, litra a)

   — eventuelle ændringer af denne afgørelse.

b) EU-Udenrigstjenestens Sikkerhedsudvalg kan alt efter omstændighederne høres eller orienteres om spørgsmål vedrørende sikkerheden for medarbejdere og aktiver i EU-Udenrigstjenestens hovedkontor og EU-delegationer, med forbehold af artikel 3, stk. 3

c) EU-Udenrigstjenesten skal orienteres om alle tilfælde af kompromittering eller bortkomst af EUCI i EU-Udenrigstjenesten.

5. Enhver ændring af reglerne om beskyttelse af EUCI, der er indeholdt i denne afgørelse og bilag A, kræver en enstemmig positiv udtalelse fra medlemsstaterne som repræsenteret i EU-Udenrigstjenestens Sikkerhedsudvalg. En sådan enstemmig positiv udtalelse er også påkrævet inden:

— **indgåelse af forhandlinger af administrative ordninger, jf. bilag A, artikel 10, stk. 1,** litra b)

— videregivelse af klassificerede informationer under ekstraordinære omstændigheder, jf. bilag A VI, stk. 9, 11 og 12

— overtagelse af informationsudstederens ansvar i de tilfælde, der er omtalt i bilag A VI, artikel 10, stk. 4, sidste punktum.

Hvis der kræves en enstemmig positiv udtalelse, er denne betingelse opfyldt, når medlemsstaternes delegationer ikke kommer med nogen indvendinger under udvalgsarbejdet.

6. EU-Udenrigstjenestens Sikkerhedsudvalg skal tage fuld højde for de sikkerhedspolitikker og retningslinjer, der er gældende i Rådet og Kommissionen.

7. EU-Udenrigstjenestens Sikkerhedsudvalg får udleveret listen over EU-Udenrigstjenestens årlige inspektioner og inspektionsrapporterne, når disse er færdige.

8. Tilrettelæggelse af møderne:

— EU-Udenrigstjenestens Sikkerhedsudvalg mødes mindst to gange om året. Der kan arrangeres yderligere møder, enten i fuldt omfang eller i NSA/DSA- eller i MFA-sikkerhedsformat, af formanden eller efter anmodning fra udvalgsmedlemmerne.

— EU-Udenrigstjenestens Sikkerhedsudvalg tilrettelægger sine aktiviteter, så det kan fremsætte henstillinger om specifikke sikkerhedsområder. Det kan om nødvendigt etablere andre ekspertunderområder. Det udarbejder et kommissorium for sådanne ekspertunderområder og får rapporter fra dem om deres aktiviteter.

— EU-Udenrigstjenestens Sikkerhedsdirektorat er ansvarligt for at forberede de emner, der skal drøftes. Formanden opstiller en foreløbig dagsorden for hvert møde. Udvalgsmedlemmerne kan fremsætte forslag til yderligere emner, der skal drøftes.

Artikel 15

Sikkerhedsinspektioner

1. EU-Udenrigstjenestens sikkerhedsmyndighed sikrer, at der regelmæssigt foretages sikkerhedsinspektioner på EU-Udenrigstjenestens hovedkontor og i EU-delegationerne for at kunne vurdere, om sikkerhedsforanstaltningerne er tilstrækkelige, og kontrollere, om de overholder denne afgørelse. EU-Udenrigstjenestens Sikkerhedsdirektorat kan om nødvendigt udpege eksperter til at deltage i sikkerhedsinspektioner i EU-agenturer og -organer, der er oprettet i henhold til afsnit V, kapitel 2, i TEU.

2. EU-Udenrigstjenestens sikkerhedsinspektioner foretages i henhold til bemyndigelsen hos EU-Udenrigstjenestens Sikkerhedsdirektorat og om fornødent med støtte fra sikkerhedseksperter, der repræsenterer andre EU-institutioner eller medlemsstaterne, især i forbindelse med de ordninger, der er omtalt i artikel 3, stk. 3.

3. EU-Udenrigstjenesten kan i fornødent omfang trække på ekspertise i medlemsstaterne, i Generalsekretariatet for Rådet og i Kommissionen.

Om nødvendigt kan relevante sikkerhedseksperter, der hører til i medlemsstaternes missioner i tredjelandene, og/eller repræsentanter fra de diplomatiske sikkerhedsafdelinger i medlemsstaterne anmodes om at deltage i sikkerhedsinspektionen af EU-delegationen.

4. Bestemmelser vedrørende gennemførelse af denne artikel med hensyn til beskyttelse af EUCI findes i bilag A III.

Artikel 16

Vurderingsbesøg

Der arrangeres vurderingsbesøg for at sikre, at de sikkerhedsforanstaltninger, der er indført i et tredjeland eller en international organisation, er effektive til beskyttelse af EUCI, som udveksles i henhold til en administrativ ordning, jf. bilag A VI, artikel 10, stk. 1, litra b).

EU-Udenrigstjenestens Sikkerhedsdirektorat kan udpege eksperter til at deltage i vurderingsbesøg i tredjelande eller internationale organisationer, med hvilke EU har indgået en informationssikkerhedsaftale, jf. bilag A VI, artikel 10, stk. 1, litra a).

Artikel 17

Kontinuitetsplanlægning

EU-Udenrigstjenestens Sikkerhedsdirektorat bistår COO'en med at forvalte de sikkerhedsrelaterede aspekter af EU-Udenrigstjenestens kontinuitetsprocesser som led i EU-Udenrigstjenestens overordnede kontinuitetsplanlægning.

Artikel 18

Rejsevejledninger for tjenesterejser uden for EU

EU-Udenrigstjenestens Sikkerhedsdirektorat sikrer, at der findes rejsevejledninger vedrørende tjenesterejser uden for EU for personalet under EU-Udenrigstjenestens ansvar, idet der trækkes på ressourcerne i samtlige relevante tjenester i EU-Udenrigstjenesten – især SITROOM, INTCEN, de geografiske afdelinger og EU-delegationerne.

EU-Udenrigstjenestens Sikkerhedsdirektorat tilvejebringer efter anmodning og ved at trække på ovennævnte ressourcer specifikke rejsevejledninger vedrørende tjenesterejser til tredjelande, hvor risikoniveauet er højt eller fornøjet, for personale under EU-Udenrigstjenestens ansvar.

Artikel 19

Arbejdsmiljø

EU-Udenrigstjenestens sikkerhedsbestemmelser supplerer EU-Udenrigstjenestens bestemmelser vedrørende arbejdsmiljøet som vedtaget af den højtstående repræsentant.

Artikel 20

Gennemførelse og revision

1. EU-Udenrigstjenestens sikkerhedsmyndighed godkender efter høringer af EU-Udenrigstjenestens Sikkerhedsudvalg, når dette er hensigtsmæssigt, sikkerhedspolitikker eller retningslinjer, der fastsætter eventuelle foranstaltninger, som er nødvendige for at gennemføre disse bestemmelser i EU-Udenrigstjenesten, og opbygger den nødvendige kapacitet, der dækker samtlige sikkerhedsaspekter, i snævert samarbejde med medlemsstaternes kompetente sikkerhedsmyndigheder og med støtte fra de relevante tjenester i EU-institutionerne.

2. I henhold til artikel 4, stk. 5, i Rådets afgørelse 2010/427/EU af 26. juli 2010 om, hvordan Tjenesten for EU's Optræden Udadtil skal tilrettelægges og fungere, kan der i fornødent omfang anvendes overgangsordninger ved hjælp af serviceniveauaftaler med de relevante tjenester i Generalsekretariatet for Rådet og i Kommissionen.

3. HR sikrer overordnet sammenhæng med hensyn til anvendelse af denne afgørelse og tager disse sikkerhedsbestemmelser op til revision.

4. EU-Udenrigstjenestens sikkerhedsbestemmelser skal gennemføres i snævert samarbejde med medlemsstaternes kompetente sikkerhedsmyndigheder, med Sikkerhedskontoret ved Generalsekretariatet for Rådet og med Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed.

5. EU-Udenrigstjenesten sikrer, at der tages højde for alle aspekter af sikkerhedsprocessen i EU-Udenrigstjenestens krisestyringssystem.

6. COO'en som sikkerhedsmyndighed og lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat sikrer, at denne afgørelse gennemføres.

Artikel 21

Ophævelse af tidligere afgørelser

1. Denne afgørelse ophæver og træder i stedet for afgørelsen truffet af Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik den 15. juni 2011 om sikkerhedsbestemmelserne for Tjenesten for EU's Optræden Udadtil [1].

2. Denne afgørelse ophæver afgørelsen truffet af Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik den 23. februar 2011 om betegnelsen og opgaverne for den delegerede sikkerhedsmyndighed ved Tjenesten for EU's Optræden Udadtil.

Artikel 22

Afsluttende bestemmelser

Denne afgørelse træder i kraft på datoen for dens undertegnelse.

Den offentliggøres i *Den Europæiske Unions Tidende*.

De kompetente myndigheder i EU-Udenrigstjenesten skal på behørig og rettidig vis underrette samtlige medarbejdere, der er omfattet af denne afgørelse og bilagene dertil, om indholdet, ikrafttrædelsesdatoen og eventuelle efterfølgende ændringer deraf.

Udfærdiget i Bruxelles, den 19. april 2013.

Den højtstående repræsentant

C. ASHTON

[1] EUT C 304 af 15.10.2011, s. 5.

BILAG A

PRINCIPPER OG STANDARDER FOR BESKYTTELSE AF EUCI

Artikel 1

Formål, anvendelsesområde og definitioner

1. I dette bilag fastsættes grundprincipperne og minimumsstandarderne for sikkerhedsbeskyttelse af EUCI.

2. Disse grundprincipper og minimumsstandarder gælder for EU-Udenrigstjenesten og personale under EU-Udenrigstjenestens ansvar som omtalt og defineret i artikel 1 og 2 i denne afgørelse.

Artikel 2

Definition af EUCI, sikkerhedsklassifikationer og mærkninger

1. Ved "EU's klassificerede informationer" (EUCI) forstås informationer eller materiale mærket med en EU-sikkerhedsklassifikation, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes interesser skade i forskellig grad.

2. EUCI klassificeres efter en af følgende grader:

a) TRÈS SECRET UE/EU TOP SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser overordentlig alvorlig skade.

b) SECRET UE/EU SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser alvorlig skade.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser skade.

d) RESTREINT UE/EU RESTRICTED: informationer og materiale, hvis uautoriserede videregivelse kunne have negativ indvirkning på Den Europæiske Unions eller en eller flere af medlemsstaternes interesser.

3. EUCI skal være mærket med en klassifikationsgrad, jf. stk. 2. EUCI kan forsynes med yderligere mærkninger for at angive de aktivitetsområder, de vedrører, identificere udstederen, begrænse distributionen eller anvendelsen eller angive mulighederne for videregivelse.

Artikel 3

Klassifikationsstyring

1. EU-Udenrigstjenesten sikrer, at EUCI er hensigtsmæssigt klassificeret, klart identificeret som klassificerede informationer og kun bevarer sin klassifikationsgrad så længe som nødvendigt.

2. EUCI må ikke nedklassificeres eller afklassificeres, og ingen af mærkningerne ifølge artikel 2, stk. 3, må ændres eller fjernes uden forudgående skriftligt samtykke fra udstederen.

3. EU-Udenrigstjenestens sikkerhedsmyndighed godkender efter høring af EU-Udenrigstjenestens Sikkerhedsudvalg i henhold til artikel 14, stk. 5, i denne afgørelse, en sikkerhedspolitik om etablering af EUCI, som skal omfatte en praktisk klassificeringsvejledning.

Artikel 4

Beskyttelse af klassificerede informationer

1. EUCI beskyttes i overensstemmelse med denne afgørelse.

2. Den, der er i besiddelse af EUCI, er ansvarlig for beskyttelse heraf i overensstemmelse med denne afgørelse.

3. Hvis medlemsstaterne bringer klassificerede informationer med en national klassifikationsmærkning ind i EU-Udenrigstjenestens strukturer eller netværk, beskytter EU-Udenrigstjenesten disse informationer i overensstemmelse med de krav, der gælder for EUCI med en tilsvarende klassifikationsgrad, jf. den sammenlignende oversigt over sikkerhedsklassifikationer i tillæg B til Rådets afgørelse 2011/292/EU af 31. marts 2011 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer.

EU-Udenrigstjenesten etablerer passende procedurer for at holde nøjagtig rede på, hvem der er udstederen af

— de klassificerede informationer, EU-Udenrigstjenesten modtager

— det kildemateriale, der indgår i de klassificerede informationer, som EU-Udenrigstjenesten udsteder.

EU-Udenrigstjenestens Sikkerhedsudvalg skal underrettes om disse procedurer.

4. Større mængder eller en samling af EUCI kan berettige til et beskyttelsesgrad, der svarer til en højere klassificering, end de enkelte elementer gør.

Artikel 5

Personelsikkerhed ved håndtering af EU's klassificerede informationer

1. Ved personelsikkerhed forstås anvendelse af foranstaltninger for at sikre, at adgang til EUCI kun gives til personer, som:

— har "need-to-know"

— i forbindelse med adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, er blevet sikkerhedsgodkendt til den relevante klassifikationsgrad eller på anden måde er behørigt autoriseret i kraft af deres funktioner i overensstemmelse med nationale love og bestemmelser

— er blevet gjort bekendt med deres ansvar.

2. I procedurerne for personelsikkerhedsgodkendelse (PSC) fastsættes det, om en person under hensyn til vedkommendes loyalitet, troværdighed og pålidelighed kan autoriseres til at få adgang til EUCI.

3. Alle personer skal gøres bekendt med og skriftligt erkende deres ansvar for at beskytte EUCI i overensstemmelse med denne afgørelse, inden de får adgang til EUCI og med jævne mellemrum derefter.

4. Bestemmelser til gennemførelse af denne artikel findes i bilag A I.

Artikel 6

Fysisk sikkerhed for EU's klassificerede informationer

1. Ved fysisk sikkerhed forstås anvendelse af fysiske og tekniske beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til EUCI.

2. De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre, at en indtrænger skaffer sig hemmelig adgang eller tiltvinger sig adgang, på at afskrække fra, vanskeliggøre og afsløre uautoriserede handlinger samt på at muliggøre personalemæssig adskillelse, for så vidt angår adgang til EUCI på "need-to-know"-basis. Sådanne foranstaltninger fastlægges på basis af en risikostyringsproces.

3. Fysiske sikkerhedsforanstaltninger indføres for alle lokaliteter, bygninger, kontorer, lokaler og andre områder, hvor EUCI håndteres eller opbevares, herunder områder, der huser kommunikations- og informationssystemer, jf. artikel 8, stk. 2.

4. Områder, hvor EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, opbevares, skal etableres som sikrede områder i overensstemmelse med bilag A II og godkendes af EU-Udenrigstjenestens sikkerhedsmyndighed.

5. Der må kun anvendes godkendt udstyr eller godkendte anordninger til beskyttelse af EUCI, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere.

6. Bestemmelser til gennemførelse af denne artikel findes i bilag A II.

Artikel 7

Forvaltning af klassificerede informationer

1. Ved forvaltning af klassificerede informationer forstås anvendelse af administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus for at supplere foranstaltningerne i artikel 5, 6 og 8 og derved bidrage til at afskrække fra, afsløre og udbedre skade forårsaget af forsætlig eller uagtsom kompromittering eller bortkomst af sådanne informationer. Sådanne foranstaltninger omfatter bl.a. udarbejdelse, registrering, kopiering, oversættelse, transport, håndtering, opbevaring og destruktion af EUCI.

2. Informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, sikkerhedsregistreres forud for distributionen og ved modtagelsen. De kompetente myndigheder i EU-Udenrigstjenesten etablerer en registraturordning med henblik herpå. Informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, registreres i dertil oprettede registraturer.

3. Tjenester og lokaliteter, hvor EUCI håndteres eller opbevares, underkastes regelmæssig inspektion foretaget af EU-Udenrigstjenestens sikkerhedsmyndighed.

4. EUCI transporteres på følgende måde mellem tjenester og lokaliteter uden for fysisk beskyttede områder:

a) generelt transmitteres EUCI via elektroniske midler beskyttet af kryptoprodukter, der er godkendt i henhold til artikel 7, stk. 5, i denne afgørelse og i henhold til klart definerede operationelle procedurer (SecOP'er)

b) når de i litra a) omhandlede midler ikke anvendes, transporteres EUCI enten:

   i) via elektroniske medier (f.eks. USB-nøgler, cd'er og harddiske) beskyttet af kryptoprodukter, der er godkendt i overensstemmelse med artikel 7, stk. 5, i denne afgørelse, eller

   ii) i alle andre tilfælde som foreskrevet af EU-Udenrigstjenestens sikkerhedsmyndighed i overensstemmelse med de relevante beskyttelsesforanstaltninger i bilag A III, afsnit V.

5. Bestemmelser til gennemførelse af denne artikel findes i bilag A III.

Artikel 8

Beskyttelse af EUCI, der håndteres i kommunikations- og informationssystemer

1. Ved informationssikring (IA) i forbindelse med kommunikations- og informationssystemer forstås tilliden til, at disse systemer beskytter de informationer, der håndteres, og at de fungerer, som de skal, når de skal, under de legitime brugeres kontrol. Effektiv IA sikrer et passende niveau af fortrolighed, integritet, tilgængelighed, uafviselighed og autenticitet. IA baseres på en risikostyringsproces.

2. Ved "kommunikations- og informationssystem" (CIS) forstås et system, der muliggør håndtering af informationer i elektronisk form. Et kommunikations- og informationssystem omfatter alle de aktiver, der er nødvendige for dets drift, herunder infrastrukturer, organisation, personale og informationsressourcer. Dette bilag finder anvendelse på al håndtering af EUCI i EU-Udenrigstjenestens CIS'er.

3. EUCI håndteres i CIS'er i overensstemmelse med begrebet IA.

4. Al håndtering af EUCI i CIS'er skal gennem en akkrediteringsproces. Akkrediteringen har til formål at sikre, at alle passende sikkerhedsforanstaltninger er blevet gennemført, og at der er opnået en tilstrækkelig grad af beskyttelse af EUCI og af CIS'et i overensstemmelse med denne afgørelse. Akkrediteringsudredningen skal fastsætte den højeste klassifikationsgrad af de informationer, der kan håndteres i et CIS, samt de betingelser og vilkår, der svarer hertil.

5. Al håndtering af informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, i CIS'er skal sikkerhedsbeskyttes, således at informationerne ikke kan kompromitteres gennem utilsigtede elektromagnetiske emissioner (Tempestsikkerhedsforanstaltninger).

6. Hvis beskyttelsen af EUCI sker ved hjælp af kryptoprodukter, skal sådanne produkter være godkendt i henhold til artikel 7, stk. 5, i denne afgørelse.

7. Ved elektronisk transmission af EUCI skal der anvendes godkendte kryptoprodukter. Uanset dette krav kan der i nødsituationer følges specifikke procedurer eller anvendes specifikke tekniske konfigurationer, jf. bilag A IV.

8. I henhold til artikel 7, stk. 6, i denne afgørelse oprettes i nødvendigt omfang følgende IA-funktioner:

a) en IA-myndighed (IAA)

b) en Tempestmyndighed (TA)

c) en kryptogodkendelsesmyndighed (CAA)

d) en kryptodistributionsmyndighed (CDA).

9. I henhold til artikel 7, stk. 7, i denne afgørelse skal der for hvert enkelt system oprettes:

a) en sikkerhedsakkrediteringsmyndighed (SAA)

b) en operativ IA-myndighed.

10. Bestemmelser til gennemførelse af denne artikel findes i bilag A IV.

Artikel 9

Industrisikkerhed

1. Ved industrisikkerhed forstås anvendelse af foranstaltninger for at sikre, at kontrahenter eller underkontrahenter beskytter EUCI under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter. Generelt må sådanne kontrakter ikke indebære adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET.

2. EU-Udenrigstjenesten kan ved aftale overdrage opgaver, som indebærer eller medfører adgang til eller håndtering eller opbevaring af EUCI, til industrivirksomheder eller andre enheder, som er registreret i en medlemsstat eller i et tredjeland, der har indgået en aftale om informationssikkerhed eller en administrativ ordning, jf. bilag A, artikel 10, stk. 1.

3. EU-Udenrigstjenesten sikrer som kontraherende myndighed, at minimumsstandarderne for industrisikkerhed som fastlagt i denne afgørelse og omhandlet i kontrakten overholdes, når der tildeles klassificerede kontrakter til industrivirksomheder eller andre enheder. Den sikrer ved hjælp af den relevante NSA/DSA, at sådanne minimumsstandarder overholdes.

4. Kontrahenter eller underkontrahenter, der er registreret i en medlemsstat, og som deltager i klassificerede kontrakter eller underkontrakter, der kræver håndtering og opbevaring af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, inden for deres faciliteter, enten i forbindelse med opfyldelsen af kontrakterne eller i perioden forud for indgåelsen af kontrakterne, skal være i besiddelse af en facilitetssikkerhedsgodkendelse (FSC) til den krævede klassifikationsgrad, som er udstedt af NSA'en, DSA'en eller en anden kompetent sikkerhedsmyndighed i den pågældende medlemsstat.

5. En kontrahents eller underkontrahents personale, der med henblik på opfyldelse af en klassificeret kontrakt har brug for adgang til informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal tildeles en PSC af den pågældende nationale sikkerhedsmyndighed (NSA), udpegede sikkerhedsmyndighed (DSA) eller en anden kompetent sikkerhedsmyndighed i overensstemmelse med nationale love og bestemmelser og de minimumsstandarder, der er fastslået i bilag A I.

6. Bestemmelserne til gennemførelse af denne artikel findes i bilag A V.

Artikel 10

Udveksling af klassificerede informationer med tredjelande og internationale organisationer

1. EU-Udenrigstjenesten kan kun udveksle EUCI med et tredjeland eller en international organisation, hvis:

a) der findes en informationssikkerhedsaftale mellem EU og tredjelandet eller den internationale organisation, som er indgået i henhold til artikel 37 i TEU og artikel 218 i TEUF, eller

b) en administrativ ordning mellem HR og de kompetente sikkerhedsmyndigheder i tredjelandet eller den internationale organisation vedrørende udveksling af oplysninger, der i princippet ikke er klassificeret højere end RESTREINT UE/EU RESTRICTED, og hvor ordningen er indgået i overensstemmelse med proceduren i artikel 14, stk. 5, i denne afgørelse, er trådt i kraft, eller

c) der gælder en rammeaftale eller en aftale om ad-hoc-deltagelse mellem EU og tredjelandet i forbindelse med en FSFP-krisestyringsoperation, der er indgået i henhold til artikel 37 i TEU og artikel 218 i TEUF,

og betingelserne som fastsat i dette dokument er blevet opfyldt.

Undtagelser til ovennævnte hovedregel fremgår af bilag A VI, afsnit V.

2. Administrative ordninger som omhandlet i stk. 1, litra b), skal indeholde bestemmelser, der sikrer, at tredjelande eller internationale organisationer, når de modtager EUCI, sikkerhedsbeskytter sådanne informationer i overensstemmelse med informationernes klassifikationsgrad og efter minimumsstandarder, som mindst svarer til de standarder, der er fastslået i denne afgørelse.

Informationer, der udveksles på grundlag af aftaler som omhandlet i stk. 1, litra c), skal begrænses til oplysninger om FSFP-operationer, hvor det pågældende tredjeland deltager på grundlag af disse aftaler og i overensstemmelse med bestemmelserne deri.

3. Der skal arrangeres vurderingsbesøg i tredjelande eller internationale organisationer, jf. artikel 16 i denne afgørelse, for at sikre, at sikkerhedsforanstaltningerne til beskyttelse af udvekslede EUCI er effektive.

4. Afgørelsen om at videregive EUCI, som EU-Udenrigstjenesten er i besiddelse af, til et tredjeland eller en international organisation, træffes fra sag til sag på grundlag af informationernes art og indhold, modtagerens "need-to-know" og EU's interesse i videregivelsen.

EU-Udenrigstjenesten skal indhente skriftligt samtykke fra alle enheder, der har leveret klassificerede informationer som kildemateriale til EUCI, som EU-Udenrigstjenesten er udsteder af, for at fastslå, at der ikke er nogen indvendinger mod videregivelse.

Hvis udstederen af de klassificerede informationer, der ønskes videregivet, ikke er EU-Udenrigstjenesten, skal EU-Udenrigstjenesten først indhente udstederens skriftlige samtykke til videregivelsen.

Hvis EU-Udenrigstjenesten imidlertid ikke kan fastslå, hvem der er udstederen, skal EU-Udenrigstjenestens sikkerhedsmyndighed påtage sig udstederens ansvar efter at have indhentet enstemmig positiv udtalelse fra medlemsstaterne som repræsenteret i EU-Udenrigstjenestens Sikkerhedsudvalg.

5. Bestemmelser til gennemførelse af denne artikel findes i bilag A VI.

Artikel 11

Brud på sikkerheden og kompromittering af klassificerede informationer

1. Et eventuelt brud på eller en eventuel mistanke om brud på sikkerheden eller en eventuel kompromittering eller en eventuel mistanke om kompromittering af klassificerede informationer skal straks indberettes til EU-Udenrigstjenestens Sikkerhedsdirektorat, der i nødvendigt omfang skal underrette Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed og Sikkerhedskontoret ved Generalsekretariatet for Rådet, den eller de pågældende medlemsstater eller andre berørte enheder.

2. Hvis det konstateres, eller hvis der er rimelig grund til at formode, at klassificerede informationer er kompromitteret eller bortkommet, skal EU-Udenrigstjenestens Sikkerhedsdirektorat alt efter omstændighederne underrette Sikkerhedsdirektoratet ved Kommissionen, Sikkerhedskontoret ved Generalsekretariatet for Rådet eller NSA'en i den eller de pågældende medlemsstater eller andre berørte enheder og skal træffe alle passende foranstaltninger i overensstemmelse med de relevante love og bestemmelser for at:

a) vurdere den potentielle skade for EU's eller medlemsstaternes interesser

b) træffe passende foranstaltninger til at forebygge en gentagelse

c) sikre bevismaterialet

d) sikre, at sagen undersøges af personale, der ikke er direkte involveret i bruddet på sikkerheden, for at fastslå de faktiske omstændigheder

e) underrette de relevante myndigheder om konsekvenserne af hændelsen og de foranstaltninger, der er truffet

f) orientere udstederen.

3. Enhver medarbejder under EU-Udenrigstjenestens ansvar, som er ansvarlig for brud på sikkerhedsreglerne i denne afgørelse, kan pålægges disciplinære foranstaltninger i overensstemmelse med gældende regler og bestemmelser.

Enhver, der er ansvarlig for kompromittering eller bortkomst af klassificerede informationer, pålægges disciplinære foranstaltninger og/eller retsforfølges i overensstemmelse med gældende love, regler og bestemmelser.

Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed, Sikkerhedskontoret ved Generalsekretariatet for Rådet eller NSA'en i den eller de pågældende medlemsstater eller andre berørte enheder skal alt efter omstændighederne straks orienteres.

4. Mens der pågår en efterforskning af brud og/eller kompromittering, kan lederen af EU-Udenrigstjenestens Sikkerhedsdirektorat suspendere den pågældende persons adgang til EUCI og til EU-Udenrigstjenestens lokaliteter. Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed, Sikkerhedskontoret ved Generalsekretariatet for Rådet eller NSA'en i den eller de pågældende medlemsstater eller andre berørte enheder skal straks orienteres om denne afgørelse.

BILAG A I

PERSONELSIKKERHED

I. **INDLEDNING**

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 5 i bilag A. Det fastsætter navnlig de kriterier, som EU-Udenrigstjenesten skal gøre brug af til fastlæggelse af, om en person under hensyntagen til vedkommendes loyalitet, troværdighed og pålidelighed kan autoriseres til at få adgang til EUCI, samt de undersøgelsesmæssige og administrative procedurer, der skal følges i den forbindelse.

2. "Personelsikkerhedsgodkendelse" (PSC) for adgang til EUCI er en udredning fra en kompetent myndighed i en medlemsstat, der udarbejdes efter gennemførelse af en sikkerhedsundersøgelse foretaget af de kompetente myndigheder i en medlemsstat, og som bekræfter, at en person, forudsat at vedkommendes "need-to-know" er fastslået, kan tildeles adgang til EUCI op til en nærmere bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en nærmere bestemt dato, og den pågældende betegnes som "sikkerhedsgodkendt".

3. "Certifikat for personelsikkerhedsgodkendelse" (PSCC) er et certifikat fra EU-Udenrigstjenestens sikkerhedsmyndighed om, at en person er sikkerhedsgodkendt, og som viser den klassifikationsgrad for EUCI, som personen kan få adgang til, gyldighedsdatoen for den relevante PSC og certifikatets udløbsdato.

4. "Autorisation til adgang til EUCI" er en autorisation fra EU-Udenrigstjenestens sikkerhedsmyndighed, som udstedes i overensstemmelse med denne afgørelse, efter at der er udstedt en PSC af de kompetente myndigheder i en medlemsstat, og som bekræfter, at en person, forudsat at vedkommendes "need-to-know" er fastslået, kan tildeles adgang til EUCI op til en nærmere bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en nærmere bestemt dato, og den pågældende person betegnes som "sikkerhedsgodkendt".

II. **AUTORISATION TIL AT FÅ ADGANG TIL EUCI**

5. Adgang til informationer klassificeret RESTREINT UE/EU RESTRICTED kræver ikke nogen sikkerhedsgodkendelse og tildeles, efter at:

   a) vedkommendes lovbestemte eller kontraktlige forbindelse til EU-Udenrigstjenesten er fastslået

   b) vedkommendes "need-to-know" er fastslået

   c) vedkommende er gjort bekendt med sikkerhedsbestemmelserne og bestemmelser til beskyttelse af EUCI og skriftligt har anerkendt sit ansvar for at beskytte EUCI i overensstemmelse med denne afgørelse.

6. En person kan kun autoriseres til at få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, efter at:

   a) vedkommendes "need-to-know" er fastslået

   b) den pågældende har fået en PSC op til det relevante niveau eller på anden vis i kraft af sine funktioner er behørigt autoriseret i overensstemmelse med nationale love og bestemmelser

   c) vedkommende er blevet gjort bekendt med sikkerhedsbestemmelserne og bestemmelserne til beskyttelse af EUCI og skriftligt har anerkendt sit ansvar for at beskytte sådanne informationer.

7. EU-Udenrigstjenesten skal identificere de stillinger i sin organisation, hvor der er brug for information klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, og hvor der derfor er brug for en PSC til den relevante klassifikationsgrad, jf. artikel 4 ovenfor.

8. Personale i EU-Udenrigstjenesten skal erklære, om de har statsborgerskab i mere end ét land.

PSC-anmodningsprocedurer i EU-Udenrigstjenesten

9. For personale i EU-Udenrigstjenesten skal ansættelsesmyndigheden i EU-Udenrigstjenesten fremsende det udfyldte spørgeskema vedrørende personelsikkerhed til NSA'en i den medlemsstat, hvor personen er statsborger, med anmodning om at der foretages en sikkerhedsundersøgelse for den EUCI-klassifikationsgrad, hvortil personen har brug for adgang.

10. Hvis en person har statsborgerskab i mere end ét land, fremsendes anmodningen om en sikkerhedsundersøgelse til NSA'en i det land, hvorfra personen er blevet rekrutteret.

11. Hvis EU-Udenrigstjenesten får kendskab til oplysninger, der er relevante for en sikkerhedsundersøgelse, om en person, der har ansøgt om en PSC, underretter EU-Udenrigstjenesten den relevante NSA herom i overensstemmelse med de relevante regler og bestemmelser.

12. Efter gennemførelsen af sikkerhedsundersøgelsen underretter den relevante NSA EU-Udenrigstjenestens Sikkerhedsdirektorat om resultatet af en sådan undersøgelse.

    a) Hvis sikkerhedsundersøgelsen fører til den konklusion, at der ikke er konstateret negative forhold, som kan rejse tvivl om personens loyalitet, troværdighed og pålidelighed, kan EU-Udenrigstjenestens sikkerhedsmyndighed tildele den pågældende adgang til EUCI op til den relevante klassifikationsgrad indtil en nærmere bestemt dato.

    b) EU-Udenrigstjenesten træffer alle relevante foranstaltninger for at sikre, at de betingelser eller restriktioner, som NSA'en pålægger, gennemføres på behørig vis. NSA'en skal orienteres om resultatet.

    c) Hvis sikkerhedsundersøgelsen ikke fører til denne konklusion, underretter EU-Udenrigstjenestens sikkerhedsmyndighed den pågældende person, der kan anmode om at blive hørt af EU-Udenrigstjenestens sikkerhedsmyndighed. EU-Udenrigstjenestens sikkerhedsmyndighed kan anmode den kompetente NSA om de nærmere oplysninger, som denne er i stand til at give i henhold til de nationale love og bestemmelser. Såfremt resultatet bekræftes, kan der ikke tildeles tilladelse til adgang til EUCI. I så fald træffer EU-Udenrigstjenesten alle relevante foranstaltninger for at sikre, at den ansøger, der har indgivet en begæring, nægtes enhver adgang til EUCI.

13. Sikkerhedsundersøgelsen samt de opnåede resultater, på hvilke EU-Udenrigstjenesten bygger sin beslutning om, hvorvidt der skal tildeles en tilladelse til adgang til EUCI eller ej, er underlagt de relevante love og bestemmelser, som er gældende i den pågældende medlemsstat, herunder bestemmelser om klageadgang. Der kan indgives klager over afgørelser truffet af EU-Udenrigstjenestens sikkerhedsmyndighed i overensstemmelse med vedtægten for tjenestemænd ved Den Europæiske Union og ansættelsesvilkårene for de øvrige ansatte ved Den Europæiske Union, som fastsat i forordning (EØF, Euratom, EKSF) nr. 259/68 ([1]) (i det følgende benævnt "personalevedtægten").

14. Den sikkerhedskonklusion, som en PSC er baseret på, forudsat at den stadig er gyldig, omfatter alle de arbejdsopgaver, den pågældende person udfører i EU-Udenrigstjenesten, Generalsekretariatet for Rådet eller Kommissionen.

15. Hvis en persons ansættelsesperiode ikke påbegyndes inden for 12 måneder efter meddelelsen af sikkerhedsundersøgelsens resultat til EU-Udenrigstjenestens sikkerhedsmyndighed, eller hvis personens ansættelse afbrydes i en periode på 12 måneder eller mere, uden at der i samme periode sker ansættelse i EU-Udenrigstjenesten, i andre EU-institutioner, -agenturer eller -organer eller i en stilling i en medlemsstats nationale forvaltning, der kræver adgang til klassificerede informationer, skal dette resultat meddeles den relevante NSA med henblik på at få bekræftet, at det fortsat er gyldigt og relevant.

16. Hvis EU-Udenrigstjenesten får kendskab til oplysninger om, at en person, der er i besiddelse af en gyldig PSC, udgør en sikkerhedsrisiko, underretter EU-Udenrigstjenesten den relevante NSA herom i overensstemmelse med de relevante regler og bestemmelser. Når en NSA underretter EU-Udenrigstjenesten om, at den trækker en sikkerhedskonklusion tilbage, der er givet i overensstemmelse med stk. 12, litra a), vedrørende en person, der er i besiddelse af en gyldig tilladelse til adgang til EUCI, kan EU-Udenrigstjenestens sikkerhedsmyndighed anmode NSA'en om de nærmere oplysninger, som denne er i stand til at give i henhold til de nationale love og bestemmelser. Hvis de negative oplysninger bekræftes, inddrages ovennævnte tilladelse, og personen har ikke længere adgang til EUCI eller til stillinger, hvor en sådan adgang er mulig, eller hvor den pågældende ville kunne udgøre en sikkerhedsrisiko.

17. En beslutning om inddragelse af en autorisation til adgang til EUCI fra en medarbejder i EU-Udenrigstjenesten og, når det er relevant, grundene hertil meddeles den pågældende person, som kan anmode om at blive hørt af EU-Udenrigstjenestens sikkerhedsmyndighed. Oplysninger, der videregives af en NSA, er underlagt de relevante love og bestemmelser, som er gældende i den pågældende medlemsstat, herunder bestemmelser om klageadgang. Der kan indgives klager over afgørelser truffet af EU-Udenrigstjenestens sikkerhedsmyndighed i overensstemmelse med personalevedtægten.

18. Nationale eksperter, der udstationeres til EU-Udenrigstjenesten i en stilling, hvortil der kræves adgang til klassificerede informationer CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal fremlægge en gyldig national PSC for adgang til EUCI for den relevante klassifikationsgrad over for EU-Udenrigstjenestens sikkerhedsmyndighed, inden de påbegynder arbejdet. Ovenstående proces skal forvaltes af den udsendende medlemsstat.

Registre over PSC'er

19. EU-Udenrigstjenesten vedligeholder en database over sikkerhedsgodkendelsesstatus for alt personale under EU-Udenrigstjenestens ansvar og for EU-Udenrigstjenestens kontrahenters medarbejdere. Disse registre skal indeholde den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), datoen for tildelingen af PSC'en samt dens gyldighedsperiode.

20. Sammen med medlemsstaterne og andre EU-institutioner, -agenturer og -organer indføres der passende koordineringsprocedurer for at sikre, at EU-Udenrigstjenesten fører et korrekt og omfattende register over sikkerhedsgodkendelsesstatus for alt personale under EU-Udenrigstjenestens ansvar og for EU-Udenrigstjenestens kontrahenters medarbejdere.

([1]) EFT L 56 af 4.3.1968, s. 1.

21. EU-Udenrigstjenestens sikkerhedsmyndighed kan udstede et certifikat for personelsikkerhedsgodkendelse (PSCC) med angivelse af den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), gyldighedsdatoen for den relevante PSC og certifikatets udløbsdato.

Undtagelser fra kravet om PSC

22. Personer, der er behørigt autoriseret til adgang til EUCI i kraft af deres funktioner og i overensstemmelse med nationale love og bestemmelser, skal alt efter omstændighederne af EU-Udenrigstjenestens Sikkerhedsdirektorat gøres bekendt med deres sikkerhedsmæssige forpligtelser med hensyn til beskyttelse af EUCI.

III. UDDANNELSE I OG BEVIDSTGØRELSE OM SIKKERHED

23. Inden der opnås autoriseret adgang til EUCI, skal alle personer skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og de konsekvenser, det kan få, hvis EUCI kompromitteres. EU-Udenrigstjenesten fører et register over sådanne skriftlige bekræftelser.

24. Alle personer, der er autoriseret til at have adgang til eller skal håndtere EUCI, skal indledningsvis gøres opmærksom på og med regelmæssige mellemrum gøres bekendt med sikkerhedsrisici og skal øjeblikkelig indberette enhver henvendelse eller aktivitet, de finder mistænkelig eller usædvanlig, til de relevante sikkerhedsmyndigheder.

25. Alle personer, der har fået tildelt adgang til EUCI, skal være omfattet af løbende personelsikkerhedsforanstaltninger (dvs. opfølgningsforanstaltninger), så længe de håndterer EUCI. Ansvaret for løbende personelsikkerhed påhviler:

a) Personer, der tildeles adgang til EUCI: De er personligt ansvarlige for deres egen sikkerhedsadfærd og skal straks indberette enhver fremgangsmåde eller aktivitet, som de anser for at være mistænkelig eller usædvanlig, og enhver forandring vedrørende deres personlige omstændigheder, der kan have indvirkning på deres PSC eller tilladelse til adgang til EUCI, til de relevante sikkerhedsmyndigheder.

b) Ledere: De er ansvarlige for at sikre, at deres personale er bekendt med sikkerhedsforanstaltningerne og ansvaret for at beskytte EUCI, og for at overvåge deres personales sikkerhedsadfærd og enten tage fat på eventuelle problematiske sikkerhedsanliggender selv eller indberette eventuelle negative oplysninger, der kan have indvirkning på deres medarbejderes PSC eller tilladelse til adgang til EUCI, til de relevante sikkerhedsmyndigheder.

c) Sikkerhedsaktører i EU-Udenrigstjenestens sikkerhedsorganisation, jf. artikel 12 i denne afgørelse: De er ansvarlige for at sørge for orienteringer om sikkerhedsbevidsthed for at sikre, at medarbejderne i deres område regelmæssigt bliver orienteret, for at fremme en stærk sikkerhedskultur inden for deres ansvarsområde og indføre foranstaltninger til overvågning af medarbejdernes sikkerhedsadfærd og for at indberette eventuelle negative oplysninger, der kan have indvirkning på alle personers PSC, til de relevante sikkerhedsmyndigheder.

d) EU-Udenrigstjenesten og medlemsstaterne: De skal etablere de fornødne kanaler til at formidle information, der kan have indvirkning på alle personers PSC eller tilladelse til adgang til EUCI.

26. Alle personer, der ikke længere udfører funktioner, som kræver adgang til EUCI, skal underrettes om og, når det er relevant, skriftligt bekræfte deres forpligtelser med hensyn til fortsat beskyttelse af EUCI.

IV. EKSTRAORDINÆRE OMSTÆNDIGHEDER

27. EU-Udenrigstjenestens sikkerhedsmyndighed kan i hastetilfælde, hvor det er behørigt begrundet i EU-Udenrigstjenestens interesse, og inden en fuldstændig sikkerhedsundersøgelse er afsluttet, efter samråd med NSA'en i den medlemsstat, hvor den pågældende er statsborger, og med forbehold af resultatet af en foreløbig kontrol til undersøgelse af, at der ikke er konstateret negative oplysninger, give tjenestemænd og øvrige ansatte ved EU-Udenrigstjenesten midlertidig autorisation til at få adgang til EUCI med henblik på en specifik opgave. Der bør hurtigst muligt gennemføres en fuldstændig sikkerhedsundersøgelse. Sådanne midlertidige autorisationer er gyldige i en periode, der ikke overstiger seks måneder, og tillader ikke adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET. Alle personer, der har fået en midlertidig autorisation, skal skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og konsekvenserne af en eventuel kompromittering af EUCI. EU-Udenrigstjenesten fører et register over sådanne skriftlige bekræftelser.

28. Når en person skal tiltræde en stilling, hvortil der kræves en PSC med en højere klassifikationsgrad end den, den pågældende allerede har, kan tiltrædelsen ske midlertidigt, forudsat at:

a) den pågældendes foresatte skriftligt dokumenterer, at der er et tvingende behov for adgang til EUCI med en højere klassifikationsgrad

b) adgangen er begrænset til bestemte EUCI til brug for arbejdsopgaverne

c) den pågældende har en gyldig PSC

d) der er iværksat foranstaltninger med henblik på at opnå autorisation til den klassifikationsgrad, som er påkrævet til stillingen

e) den kompetente myndighed i tilstrækkeligt omfang har kontrolleret, at den pågældende ikke har begået alvorlige eller gentagne overtrædelser af sikkerhedsreglerne

f) den pågældendes varetagelse af arbejdsopgaverne godkendes af den kompetente myndighed i EU-Udenrigstjenesten

g) den relevante NSA/DSA, der har udstedt den pågældendes PSC, er blevet hørt, og der ikke er modtaget nogen indvendinger

h) undtagelsen registreres i den ansvarlige registratur eller underregistratur med en beskrivelse af de informationer, der er givet adgang til.

29. Ovennævnte procedure anvendes for engangsadgang til EUCI med en klassifikationsgrad, der er ét trin højere end den, personen er sikkerhedsgodkendt til. Der må ikke gøres tilbagevendende brug af denne procedure.

30. Under ganske særlige omstændigheder, f.eks. i forbindelse med tjenesterejser i fjendtlige miljøer eller under en eskalerende international krise, kan HR, den administrerende generalsekretær eller den administrerende direktør, såfremt det er tvingende nødvendigt, især for at redde menneskeliv, give tilladelse, så vidt muligt skriftligt, til, at personer, der ikke har den krævede PSC, får adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, hvis en sådan tilladelse er absolut nødvendig, og der ikke er rimelige grunde til at betvivle den pågældende persons loyalitet, troværdighed og pålidelighed. Denne tilladelse skal registreres med en beskrivelse af de informationer, der er givet adgang til.

31. Drejer det sig om informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, begrænses denne nødadgang til EU-borgere, som allerede er autoriseret til at have adgang enten til den nationale klassifikationsgrad, der svarer til TRÈS SECRET UE/EU TOP SECRET, eller til informationer, der er klassificeret SECRET UE/EU SECRET.

32. EU-Udenrigstjenestens Sikkerhedsudvalg underrettes om tilfælde, hvor proceduren i stk. 29 og 30 anvendes.

33. EU-Udenrigstjenestens Sikkerhedsudvalg forelægges hvert år en rapport om anvendelsen af procedurerne i dette afsnit.

V. DELTAGELSE I MØDER PÅ EU-UDENRIGSTJENESTENS HOVEDKONTOR OG I EU-DELEGATIONER

34. Når personer skal deltage i møder i EU-Udenrigstjenestens hovedkontor og EU-delegationer, hvor der drøftes informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal deres PSC-status bekræftes. For medlemsstaternes repræsentanter, tjenestemænd fra GSC og Kommissionen fremsender de relevante myndigheder et PSCC eller en anden dokumentation for PSC til EU-Udenrigstjenestens Sikkerhedsdirektorat, EU-delegationens sikkerhedskoordinator, eller dokumenterne forelægges undtagelsesvis af den pågældende person. Der kan eventuelt anvendes en konsolideret navneliste, som indeholder den relevante dokumentation for PSC.

35. Hvis en PSC for adgang til EUCI inddrages fra en person, hvis arbejdsopgaver kræver deltagelse i møder på EU-Udenrigstjenestens hovedkontor eller i en EU-delegation, hvor der drøftes informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, underretter den kompetente myndighed EU-Udenrigstjenesten herom.

VI. POTENTIEL ADGANG TIL EUCI

36. Når personer skal ansættes under forhold, hvor de eventuelt kan få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal de sikkerhedsgodkendes på behørig vis eller skal til stadighed ledsages.

37. Kurerer, vagter og eskorter skal sikkerhedsgodkendes til den relevante klassifikationsgrad eller på anden vis undersøges i passende omfang i overensstemmelse med nationale love og bestemmelser og med jævne mellemrum gøres bekendt med sikkerhedsprocedurer til beskyttelse af EUCI og de forpligtelser, der påhviler dem med hensyn til beskyttelse af de informationer, de får betroet, eller som de uforvarende har adgang til.

BILAG A II

FYSISK SIKKERHED FOR EU'S KLASSIFICEREDE INFORMATIONER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 6 i bilag A. Det fastsætter mindstekrav til den fysiske beskyttelse af lokaliteter, bygninger, kontorer, lokaler og andre områder, hvor EUCI håndteres og opbevares, herunder områder, der huser CIS'er.

2. De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre uautoriseret adgang til EUCI ved:

   a) at sikre, at EUCI håndteres og opbevares hensigtsmæssigt

   b) at muliggøre personalemæssig adskillelse, for så vidt angår adgang til EUCI, på grundlag af personalets "need-to-know" og, når det er relevant, dets sikkerhedsgodkendelse

   c) at afskrække fra, vanskeliggøre og afsløre uautoriserede handlinger

   d) at forhindre eller forsinke, at indtrængere skaffer sig hemmelig adgang eller tiltvinger sig adgang.

II FYSISKE SIKKERHEDSKRAV OG -FORANSTALTNINGER

3. EU-Udenrigstjenesten skal anvende en risikostyringsproces med henblik på sikkerhedsbeskyttelse af EUCI i deres lokaliteter for at sikre, at der anvendes en fysisk beskyttelsesgrad, der svarer til den vurderede risiko. Risikostyringsprocessen skal tage hensyn til alle relevante faktorer, navnlig:

   a) EUCI's klassifikationsgrad

   b) formen og mængden af EUCI under hensyn til, at store mængder eller en samling af EUCI kan kræve, at der skal anvendes strengere beskyttelsesforanstaltninger

   c) omgivelserne og strukturen af de bygninger eller områder, hvor EUCI opbevares,

   d) vurderingen af trusler fra tredjelande som udviklet af INTCEN, især på grundlag af rapporter fra EU-delegationer

   e) den vurderede trussel fra efterretningstjenester, der har EU eller medlemsstaterne som mål, samt fra sabotage, terrorisme og undergravende eller anden kriminel virksomhed.

4. EU-Udenrigstjenestens sikkerhedsmyndighed fastlægger under anvendelse af begrebet dybdeforsvar den rette kombination af de fysiske sikkerhedsforanstaltninger, der skal iværksættes. De kan omfatte en eller flere af følgende foranstaltninger:

   a) en perimeterafspærring: en fysisk afspærring, der afgrænser et område, som kræver sikkerhedsbeskyttelse

   b) system til afsløring af indtrængen (IDS): et IDS kan anvendes for at øge det sikkerhedsniveau, en perimeterafspærring giver, eller anvendes i rum og bygninger i stedet for sikkerhedspersonale eller for at bistå dette personale

   c) adgangskontrol: der kan foretages adgangskontrol ved et anlæg, en bygning eller flere bygninger i et anlæg eller i forbindelse med områder eller rum inde i en bygning. Kontrollen kan foretages elektronisk, elektromekanisk, udføres af sikkerhedspersonale og/eller en receptionist eller ved hjælp af andre fysiske metoder

   d) sikkerhedspersonale: der kan ansættes sikkerhedspersonale, der er uddannet, er under tilsyn og, når det er nødvendigt, har en relevant sikkerhedsgodkendelse, bl.a. for at afskrække personer, der planlægger hemmelig indtrængen

   e) intern tv-overvågning (CCTV): sikkerhedspersonalet kan anvende CCTV for at kontrollere hændelser og IDS-alarmer på store anlæg eller langs perimetre

   f) sikkerhedsbelysning: der kan anvendes sikkerhedsbelysning for at afskrække en potentiel indtrænger og for at skaffe den belysning, der er nødvendig for en effektiv overvågning foretaget direkte af sikkerhedspersonalet eller indirekte ved hjælp af et CCTV-system

g) eventuelle andre passende fysiske foranstaltninger, der skal afskrække fra eller afsløre uautoriseret adgang eller forhindre bortkomst af eller skade på EUCI.

5. EU-Udenrigstjenestens Sikkerhedsdirektorat kan foretage visitation ved ind- og udgang som afskrækkelse mod uautoriseret indførelse af materiale eller uautoriseret fjernelse af EUCI fra lokaliteter eller bygninger.

6. Når der er risiko for indblik i EUCI, selv uforsætligt, skal der træffes passende foranstaltninger til at imødegå denne risiko.

7. I forbindelse med nye faciliteter skal der defineres fysiske sikkerhedskrav og funktionelle specifikationer som en del af planlægningen og udformningen af faciliteterne. I forbindelse med eksisterende faciliteter skal de fysiske sikkerhedskrav opfyldes i videst mulig udstrækning.

III. **UDSTYR TIL FYSISK BESKYTTELSE AF EUCI**

8. Når der skal anskaffes udstyr (f.eks. sikkerhedscontainere, makulatorer, dørlåse, elektroniske adgangskontrolsystemer, IDS, alarmsystemer) til fysisk beskyttelse af EUCI, skal den kompetente sikkerhedsmyndighed sikre, at udstyret opfylder de godkendte tekniske standarder og minimumskrav.

9. De tekniske specifikationer for udstyr, der skal anvendes til fysisk beskyttelse af EUCI, fastsættes i sikkerhedsretningslinjer, der skal godkendes af sikkerhedsudvalget.

10. Sikkerhedssystemer skal inspiceres med jævne mellemrum, og udstyret skal vedligeholdes regelmæssigt. Vedligeholdelsesarbejdet skal tage hensyn til resultatet af inspektionerne for at sikre, at udstyret fortsat fungerer optimalt.

11. Effektiviteten af de individuelle sikkerhedsforanstaltninger og af det samlede sikkerhedssystem skal reevalueres ved hver inspektion.

IV. **FYSISK BESKYTTEDE OMRÅDER**

12. Der etableres to typer fysisk beskyttede områder eller nationale pendanter hertil med henblik på den fysiske beskyttelse af EUCI:

a) administrative områder

b) sikrede områder (herunder teknisk sikrede områder).

13. Den kompetente sikkerhedsmyndighed bestemmer, at et område opfylder kravene til at blive betegnet som et administrativt område, et sikret område eller et teknisk sikret område.

14. For så vidt angår administrative områder:

a) der etableres en synligt afgrænset perimeter, der muliggør kontrol af personer og, når det er muligt, af køretøjer

b) uledsaget adgang tillades kun for personer, der er behørigt autoriseret af EU-Udenrigstjenestens Sikkerhedsdirektorat

c) alle andre personer skal til stadighed ledsages eller underkastes tilsvarende kontrol.

15. For så vidt angår sikrede områder:

a) der etableres en synligt afgrænset og beskyttet perimeter, hvor al ind- og udgang kontrolleres ved hjælp af et adgangskort eller et persongenkendelsessystem

b) uledsaget adgang tillades kun for personer, der er sikkerhedsgodkendt til en passende klassifikationsgrad og specifikt bemyndiget til at komme ind på området på grundlag af deres "need-to-know"

c) alle andre personer skal til stadighed ledsages eller underkastes tilsvarende kontrol.

16. Hvis adgang til et sikret område i praksis indebærer direkte adgang til de klassificerede informationer, der opbevares deri, gælder følgende yderligere krav:

a) den højeste klassifikationsgradsgrad for de informationer, der normalt opbevares i området, skal klart angives

b) alle besøgende skal have en specifik autorisation til at få adgang til området, skal til stadighed ledsages og skal være passende sikkerhedsgodkendt, medmindre der træffes foranstaltninger, der sikrer, at der ikke er mulighed for adgang til EUCI

c) elektronisk udstyr må ikke bringes med ind på området.

17. Sikrede områder, der er beskyttet mod aflytning, udpeges som teknisk sikrede områder. Følgende yderligere krav gælder:

a) sådanne områder skal udstyres med IDS, være aflåst, når de ikke er i brug, og være bevogtet, når de er i brug. Eventuelle nøgler skal kontrolleres i overensstemmelse med afsnit VI i dette bilag

b) alle personer og alt materiel, der kommer ind i disse områder, skal kontrolleres

c) områderne skal underkastes regelmæssige fysiske og/eller tekniske inspektioner som krævet af EU-Udenrigstjenestens sikkerhedsmyndighed. Inspektionerne skal desuden foretages efter en eventuel uautoriseret adgang eller ved mistanke om, at en sådan adgang har fundet sted

d) områderne må ikke indeholde uautoriserede kommunikationslinjer, uautoriserede telefoner eller andre uautoriserede kommunikationsanordninger og uautoriseret elektrisk eller elektronisk udstyr.

18. Inden der skal anvendes kommunikationsanordninger og elektrisk eller elektronisk udstyr af enhver art i områder, hvor der afholdes møder om eller arbejdes med informationer, der er klassificeret SECRET UE/EU SECRET eller højere, og når truslen for EUCI vurderes som værende stor, skal dette udstyr uanset stk. 17, litra d), først undersøges af EU-Udenrigstjenestens sikkerhedsmyndighed for at sikre, at ingen forståelige informationer uagtsomt eller ulovligt transmitteres ud af det sikrede områdes perimeter ved hjælp af sådant udstyr.

19. Sikrede områder, hvor der ikke er vagtpersonale døgnet rundt, skal, når det er relevant, inspiceres ved afslutningen af normal arbejdstid og med tilfældige intervaller uden for normal arbejdstid, medmindre der findes et IDS.

20. Sikrede områder og teknisk sikrede områder kan etableres midlertidigt inden for et administrativt område med henblik på at afholde et klassificeret møde eller til et andet lignende formål.

21. Der skal for hvert sikret område udarbejdes operationelle sikkerhedsprocedurer, som indeholder bestemmelser om:

a) klassifikationsgraden for de EUCI, der kan håndteres og opbevares i området

b) de overvågnings- og beskyttelsesforanstaltninger, der skal opretholdes

c) de personer, der er autoriseret til at have uledsaget adgang til området i kraft af deres "need-to-know" og sikkerhedsgodkendelse

d) når det er relevant, procedurerne for ledsagelse eller for sikkerhedsbeskyttelse af EUCI, når andre personer autoriseres til at få adgang til området

e) andre relevante foranstaltninger og procedurer.

22. Der skal bygges bokslokaler inden for sikrede områder. Vægge, gulve, lofter, vinduer og låsbare døre skal godkendes af EU-Udenrigstjenestens sikkerhedsmyndighed og yde tilsvarende beskyttelse som den, en sikkerhedscontainer, der er godkendt til opbevaring af EUCI med samme klassifikationsgrad, yder.

V. FYSISKE BESKYTTELSESFORANSTALTNINGER MED HENBLIK PÅ HÅNDTERING OG OPBEVARING AF EUCI

23. EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, kan håndteres:

a) i et sikret område

b) i et administrativt område, forudsat at EUCI er beskyttet mod uautoriserede personers adgang, eller

c) uden for et sikret område eller et administrativt område, forudsat at den, der er i besiddelse af informationerne, transporterer EUCI i overensstemmelse med bilag A III, stk. 30-42 og har lovet at overholde kompenserende foranstaltninger, der er fastslået i sikkerhedsinstruktioner udstedt af EU-Udenrigstjenestens sikkerhedsmyndighed, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang.

24. EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, skal opbevares i passende aflåste kontormøbler i et administrativt område eller et sikret område. De kan opbevares midlertidigt uden for et sikret område eller et administrativt område forudsat at den, der er i besiddelse af informationerne, har lovet at overholde kompenserende foranstaltninger, der er fastslået i sikkerhedsinstruktioner udstedt af EU-Udenrigstjenestens sikkerhedsmyndighed.

25. EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, kan håndteres:

a) i et sikret område

b) i et administrativt område, forudsat at EUCI er beskyttet mod uautoriserede personers adgang, eller

c) uden for et sikret område eller et administrativt område, forudsat at den, der er i besiddelse af informationerne:

i) transporterer EUCI i overensstemmelse med bilag A III, stk. 30-42

ii) har lovet at overholde kompenserende foranstaltninger, der er fastslået i sikkerhedsinstruktioner udstedt af EU-Udenrigstjenestens sikkerhedsmyndighed, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang

iii) til enhver tid har EUCI under personlig kontrol

iv) i tilfælde af dokumenter i papirform har underrettet den relevante registratur om situationen.

26. EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, skal opbevares i et sikret område i en sikkerhedscontainer eller et bokslokale.

27. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal håndteres i et sikret område.

28. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal opbevares i et sikret område på hovedkontoret under et af følgende forhold:

a) i en sikkerhedscontainer, jf. stk. 8, med en eller flere af følgende former for supplerende kontrol:

i) permanent beskyttelse eller kontrol foretaget af sikkerhedsgodkendt sikkerhedspersonale eller vagtpersonale

ii) et godkendt IDS kombineret med indsatssikkerhedspersonale

eller

b) i et bokslokale udstyret med IDS og kombineret med indsatssikkerhedspersonale.

29. Regler for transport af EUCI uden for fysisk beskyttede områder findes i bilag A III.

VI. **KONTROL MED NØGLER OG KODER, DER ANVENDES TIL SIKKERHEDSBESKYTTELSE AF EUCI**

30. EU-Udenrigstjenestens sikkerhedsmyndighed fastsætter procedurer for forvaltning af nøgler og koder til kontorer, rum, bokslokaler og sikkerhedscontainere. Sådanne procedurer skal beskytte mod uautoriseret adgang.

31. Koder skal læres udenad af det mindst mulige antal personer, der har behov for at kende dem. Koder til sikkerhedscontainere og bokslokaler, hvor der opbevares EUCI, skal ændres:

a) hver gang der modtages et nyt penge- eller stålskab m.v.

b) når der sker en ændring i det personale, der kender koden

c) når der er konstateret en kompromittering, eller der er mistanke herom

d) når der er foretaget vedligeholdelse eller reparation af en lås

e) mindst hver 12. måned.

BILAG A III

FORVALTNING AF KLASSIFICEREDE INFORMATIONER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 7 i bilag A. Det fastsætter de administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus for at bidrage til at afskrække fra, afsløre og udbedre skade forårsaget af forsætlig eller uagtsom kompromittering eller bortkomst af sådanne informationer.

II. KLASSIFIKATIONSSTYRING

Klassifikation og mærkning

2. Informationer klassificeres, hvis de kræver beskyttelse med hensyn til fortroligheden.

3. Det er udstederen af EUCI, der er ansvarlig for at fastlægge klassifikationsgraden i overensstemmelse med de relevante klassifikationsretningslinjer og for udbredelse af informationerne.

4. EUCI's klassifikationsgrad fastlægges i overensstemmelse med bilag A, artikel 2, stk. 2, og ved henvisning til den sikkerhedspolitik, der skal godkendes i henhold til bilag A, artikel 3, stk. 3.

5. Klassificerede informationer fra medlemsstaterne, der udveksles med EU-Udenrigstjenesten, skal tildeles den samme beskyttelsesgrad som EUCI og have en tilsvarende klassifikationsgrad. I tillæg B til Rådets afgørelse 2011/292/EU af 31. marts 2011 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer findes der en sammenlignende oversigt.

6. Klassifikationsgraden og, hvor dette er relevant, datoen eller den specifikke hændelse, hvorefter de kan nedklassificeres eller afklassificeres, skal fremgå klart og korrekt, uanset om EUCI forekommer i papirform eller i mundtlig, elektronisk eller en hvilken som helst anden form.

7. De enkelte dele af et givet dokument (dvs. sider, afsnit og punkter i et dokument samt bilag, tillæg og vedhæftet materiale) kan kræve forskellig klassifikationsgrad og skal mærkes i overensstemmelse hermed, også ved lagring i elektronisk form.

8. I videst muligt omfang skal dokumenter, der indeholder dele med forskellig klassifikationsgrad, struktureres, så dele med en anden klassifikationsgrad let kan identificeres og udskilles, hvis det er nødvendigt.

9. Et dokuments eller dossiers samlede klassifikationsgrad skal mindst være den samme som den del, der har den højeste klassifikationsgrad. Når informationer er indsamlet fra forskellige kilder, skal det endelige produkt tages op til revision for at fastlægge dets samlede klassifikationsgrad, da det kan tilsige en højere klassifikationsgrad end de enkelte dele.

10. En følgeskrivelse klassificeres lige så højt som bilagenes højeste klassifikationsgrad. Udstederen skal klart ved hjælp af en passende mærkning angive, på hvilket niveau følgeskrivelsen skal klassificeres, hvis den adskilles fra sine bilag, f.eks.

CONFIDENTIEL UE/EU CONFIDENTIAL

Uden vedhæftet materiale RESTREINT UE/EU RESTRICTED

Mærkning

11. Ud over en af de klassifikationsmærkninger, der er nævnt i bilag A, artikel 2, stk. 2, kan EUCI forsynes med yderligere mærkninger, f.eks. med:

    a) en identifikator for at angive udstederen

    b) eventuelle særlige påtegninger, kodeord eller akronymer, der angiver det aktivitetsområde, som dokumentet omhandler, en særlig distribution på "need-to-know"-basis eller begrænset anvendelse

    c) videregivelsespåtegninger.

12. Hvis det besluttes at videregive EUCI et tredjeland eller en international organisation, fremsender EU-Udenrigstjenestens Sikkerhedsdirektorat de pågældende klassificerede informationer med en videregivelsespåtegning, der angiver det tredjeland eller den internationale organisation, som informationerne er videregivet til.

13. EU-Udenrigstjenestens sikkerhedsmyndighed vedtager en liste over godkendte mærkninger.

Forkortede klassifikationsmærkninger

14. Standardiserede forkortede klassifikationsmærkninger kan anvendes for at angive klassifikationsgraden for de enkelte afsnit i en tekst. Forkortelserne erstatter ikke den uforkortede klassifikationsmærkning.

15. Følgende standardforkortelser kan anvendes i EU's klassificerede dokumenter for at angive afsnits eller tekstdeles klassifikationsgrad, hvis teksten er kortere end en enkelt side:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Udarbejdelse af EUCI

16. Når der udarbejdes et klassificeret EU-dokument,

a) skal hver side være tydeligt mærket med klassifikationsgraden

b) skal hver side nummereres

c) skal dokumentet være forsynet med et referencenummer og et emne, der ikke i sig selv er en klassificeret information, medmindre det er mærket som sådan

d) skal dokumentet være forsynet med dato

e) skal dokumenter, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, have et eksemplarnummer på hver side, hvis de skal udsendes i flere eksemplarer.

17. Hvis punkt 15 ikke kan finde anvendelse på EUCI, træffes der andre passende foranstaltninger i overensstemmelse med de sikkerhedsretningslinjer, der skal fastlægges i medfør af denne afgørelse.

Nedklassificering og afklassificering af EUCI

18. På det tidspunkt, hvor informationerne udarbejdes, angiver udstederen så vidt muligt og især i forbindelse med informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, om EUCI kan nedklassificeres eller afklassificeres på en nærmere bestemt dato eller efter en specifik begivenhed.

19. EU-Udenrigstjenesten tager regelmæssigt EUCI i dets besiddelse op til revision for at vurdere, om klassifikationsgraden fortsat skal finde anvendelse. EU-Udenrigstjenesten opretter et system, således at klassifikationsgraden af registrerede EUCI, som den har udfærdiget, tages op til revision mindst hvert femte år. En sådan revision er ikke nødvendig, hvis udstederen fra begyndelsen har angivet, at informationerne automatisk på et nærmere bestemt tidspunkt nedklassificeres eller afklassificeres, og informationerne er mærket i overensstemmelse hermed.

III. SIKKERHEDSREGISTRERING AF EUCI

20. Der oprettes en central registratur på hovedkontoret. For hver organisatorisk enhed i EU-Udenrigstjenesten, hvor EUCI håndteres, skal der oprettes en ansvarlig registratur, som er underordnet den centrale registratur, for at sikre, at EUCI håndteres i overensstemmelse med denne afgørelse. Registraturerne oprettes som sikrede områder som defineret i bilag A.

Hver EU-delegation opretter sin egen EUCI-registratur.

EU-Udenrigstjenestens sikkerhedsmyndighed udpeger en hovedregistratur for disse registraturer.

21. I denne afgørelse forstås ved sikkerhedsregistrering (i det følgende benævnt "registrering") anvendelse af procedurer, som registrerer informationernes livscyklus, inklusive deres udbredelse og destruktion. I forbindelse med et CIS kan registreringsprocedurerne gennemføres ved processer i selve CIS'et.

22. Alt materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal registreres, når det ankommer til eller forlader en organisatorisk enhed, herunder EU-delegationer. Informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, registreres i dertil oprettede registraturer.

23. Den centrale registratur skal på EU-Udenrigstjenestens hovedkontor være den vigtigste ind- og udgang ved udveksling af klassificerede informationer med tredjelande og internationale organisationer. Den skal føre register over alle disse udvekslinger.

24. HR godkender en sikkerhedspolitik vedrørende sikkerhedsregistrering af EUCI i henhold til artikel 14 i denne afgørelse.

Très secret UE/EU top secret-registraturer

25. Den centrale registratur skal på EU-Udenrigstjenestens hovedkontor udpeges til at fungere som den centrale modtagelses- og afsendelsesmyndighed for informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET. Der kan i nødvendigt omfang oprettes underregistraturer, der håndterer disse informationer i registreringsøjemed.

26. Underregistraturer må ikke sende TRÈS SECRET UE/EU TOP SECRET-dokumenter direkte til andre underregistraturer under samme centrale TRÈS SECRET UE/EU TOP SECRET-registratur eller til anden side uden sidstnævntes udtrykkelige skriftlige godkendelse.

IV. KOPIERING OG OVERSÆTTELSE AF EU's KLASSIFICEREDE DOKUMENTER

27. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, må kun kopieres eller oversættes med udstederens forudgående skriftlige samtykke.

28. Hvis udstederen af dokumenter, der er klassificeret SECRET UE/EU SECRET eller lavere, ikke har stillet særlige betingelser for kopiering eller oversættelse af dem, kan sådanne dokumenter kopieres eller oversættes efter instruks fra den, der er i besiddelse af dem.

29. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, gælder også for kopier og oversættelser af det. Der må kun tages kopier af dokumenter, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, af en relevant (under-)registratur og med en sikret kopimaskine. Kopierne skal registreres.

V. TRANSPORT AF EUCI

30. Transport af EUCI er omfattet af beskyttelsesforanstaltningerne i punkt 31-41. Ved transport af EUCI via elektroniske medier kan nedennævnte sikkerhedsforanstaltninger uanset artikel 7, stk. 4, suppleres med de relevante tekniske modforanstaltninger som foreskrevet af EU-Udenrigstjenestens sikkerhedsmyndighed med henblik på at minimere risikoen for bortkomst eller kompromittering.

31. EU-Udenrigstjenestens sikkerhedsmyndighed udfærdiger instruktioner for transport af EUCI i overensstemmelse med denne afgørelse.

I en bygning eller en selvstændig gruppe af bygninger

32. EUCI, der transporteres i en bygning eller en selvstændig gruppe af bygninger, skal tildækkes for at forhindre observation af deres indhold.

33. I en bygning eller en selvstændig gruppe af bygninger skal informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, transporteres af hensigtsmæssigt sikkerhedsgodkendte personer i en sikret kuvert, hvorpå kun modtagerens navn er angivet.

Inden for EU

34. EUCI, der transporteres mellem bygninger eller lokaliteter inden for EU, skal pakkes således, at de er beskyttet mod uautoriseret videregivelse.

35. Transport af informationer, der er klassificeret SECRET UE/EU SECRET eller lavere, skal ske på en af følgende måder:

a) militær, officiel eller diplomatisk kurer, alt efter hvad der er hensigtsmæssigt

b) håndbåret under forudsætning af:

i) at EUCI forbliver i bærerens besiddelse, medmindre de opbevares i overensstemmelse med kravene i bilag A II

ii) at EUCI ikke åbnes undervejs eller læses på offentlige steder

iii) at enkeltpersoner er sikkerhedsgodkendt til en passende klassifikationsgrad og gjort bekendt med deres sikkerhedsansvar

iv) at enkeltpersoner om nødvendigt får udstedt et kurercertifikat

c) nationale posttjenester eller kommercielle kurertjenester under forudsætning af:

i) at de er godkendt af den relevante NSA i overensstemmelse med nationale love og bestemmelser

ii) at de anvender passende beskyttelsesforanstaltninger i overensstemmelse med de minimumskrav, der skal fastsættes i sikkerhedsretningslinjerne i medfør af artikel 20, stk. 1, i denne afgørelse.

Ved transport fra en medlemsstat til en anden finder bestemmelserne i litra c) kun anvendelse på informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller lavere.

36. Materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET (f.eks. udstyr eller maskiner), og som ikke kan transporteres på de i punkt 34 omhandlede måder, transporteres som fragt af kommercielle fragtfirmaer i overensstemmelse med bilag A V.

37. Transport af informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, mellem bygninger eller lokaliteter inden for EU, skal ske ved hjælp af militær, officiel eller diplomatisk kurer, alt efter hvad der er hensigtsmæssigt.

Fra EU til et tredjelands område eller mellem EU-enheder i tredjelande

38. EUCI, der transporteres fra EU til et tredjelands område eller mellem EU-enheder i tredjelande, skal pakkes således, at de er beskyttet mod uautoriseret videregivelse.

39. Transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, fra EU til et tredjelands område og transport af EUCI, der er klassificeret op til SECRET UE/EU SECRET, mellem EU-enheder i tredjelande skal ske på en af følgende måder:

a) militær eller diplomatisk kurer

b) håndbåret under forudsætning af:

i) at pakken er plomberet med et officielt segl eller er pakket, så det fremgår, at det drejer sig om en officiel forsendelse, som ikke skal underkastes told- eller sikkerhedskontrol

ii) at enkeltpersoner er i besiddelse af et kurercertifikat, der identificerer pakken og autoriserer dem til at transportere den

iii) at EUCI forbliver i bærerens besiddelse, medmindre de opbevares i overensstemmelse med kravene i bilag A II

iv) at EUCI ikke åbnes undervejs eller læses på offentlige steder

v) de pågældende personer er sikkerhedsgodkendt til en passende klassifikationsgrad og gjort bekendt med deres sikkerhedsansvar.

40. Transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, og som videregives af EU til et tredjeland eller en international organisation, skal overholde de relevante bestemmelser i en informationssikkerhedsaftale eller en administrativ ordning i henhold til bilag A, artikel 10, stk. 2.

41. Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, kan også transporteres fra EU til et tredjelands område af posttjenester eller kommercielle kurertjenester.

42. Transport af informationer, der er klassificeret SECRET UE/EU TOP SECRET, fra EU til et tredjelands område eller mellem EU-enheder i tredjelande, skal ske ved hjælp af militær eller diplomatisk kurer.

VI. **DESTRUKTION AF EUCI**

43. EU's klassificerede dokumenter, som der ikke længere er brug for, kan destrueres, jf. dog de relevante regler og bestemmelser om arkivering.

44. Dokumenter, der er omfattet af registrering i henhold til bilag A, artikel 7, stk. 2, destrueres af den ansvarlige registratur efter anvisning fra den, der er i besiddelse af dem, eller fra en kompetent myndighed. Journalerne og andre registreringsinformationer ajourføres i overensstemmelse hermed.

45. For så vidt angår dokumenter, der er klassificeret SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, foretages destruktionen i overværelse af et vidne, der er sikkerhedsgodkendt til mindst den klassifikationsgrad, som det destruerede dokument har.

46. Den registraturansvarlige og vidnet, hvis dettes tilstedeværelse er påkrævet, underskriver en destruktionsattest, der opbevares i registraturen. Registraturen opbevarer destruktionsattester vedrørende dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, i en periode på mindst ti år og vedrørende dokumenter, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, i en periode på mindst fem år.

47. Klassificerede dokumenter, herunder dokumenter, der er klassificeret RESTREINT UE/EU RESTRICTED, destrueres ved metoder, som opfylder de relevante EU-standarder eller tilsvarende standarder eller er godkendt af medlemsstaterne i overensstemmelse med nationale tekniske standarder, for at forhindre hel eller delvis rekonstruktion.

48. Destruktion af edb-lagringsmedier, der anvendes til lagring af EUCI, foregår i overensstemmelse med punkt 36 i bilag A IV.

VII. SIKKERHEDSINSPEKTIONER

EU-Udenrigstjenestens sikkerhedsinspektioner

49. I henhold til artikel 15 i denne afgørelse omfatter EU-Udenrigstjenestens sikkerhedsinspektioner:

a) generelle sikkerhedsinspektioner, der har til formål at vurdere det generelle sikkerhedsniveau for EU-Udenrigstjenestens hovedkontor, EU-delegationer og alle deraf afhængige eller dermed forbundne lokaliteter, især med henblik på at vurdere effektiviteten af de sikkerhedsforanstaltninger, der gennemføres for at beskytte EU-Udenrigstjenestens sikkerhedsinteresser

b) EUCI-sikkerhedsinspektioner, der har til formål at vurdere – generelt med henblik på en akkreditering – hvor effektive de foranstaltninger, der gennemføres for at beskytte EUCI i EU-Udenrigstjenestens hovedkontor og EU-delegationer, er.

Der udføres især bl.a. inspektioner for:

i) at sikre, at de krævede minimumstandarder for beskyttelse af EUCI, der er fastslået i denne afgørelse, overholdes

ii) at understrege betydningen af sikkerhed og effektiv risikostyring i de inspicerede enheder

iii) at anbefale modforanstaltninger for at afbøde de specifikke virkninger i tilfælde af tab af klassificerede informationers fortrolighed, integritet eller tilgængelighed

iv) at styrke sikkerhedsmyndighedernes løbende uddannelses- og bevidstgørelsesprogrammer vedrørende sikkerhed.

Gennemførelse af og indberetning om EU-Udenrigstjenestens sikkerhedsinspektioner

50. EU-Udenrigstjenestens sikkerhedsinspektioner gennemføres af et inspektionshold fra EU-Udenrigstjenestens Sikkerhedsdirektorat og om nødvendigt med støtte fra sikkerhedseksperter fra andre EU-institutioner eller fra medlemsstaterne.

Inspektionsholdet skal have adgang til alle steder, hvor der håndteres EUCI, navnlig de steder, hvor registraturerne og CIS'erne findes.

51. EU-Udenrigstjenestens sikkerhedsinspektioner i EU-delegationer kan, når det måtte anses for nødvendigt, gennemføres med støtte fra de sikkerhedsansvarlige ved medlemsstaternes ambassader, der er lokaliseret i tredjelandene.

52. Inden udgangen af hvert kalenderår vedtager EU-Udenrigstjenestens sikkerhedsmyndighed et sikkerhedsinspektionsprogram for EU-Udenrigstjenesten for det følgende år.

53. Når det måtte anses for nødvendigt, kan EU-Udenrigstjenestens sikkerhedsmyndighed arrangere sikkerhedsinspektioner, som ikke er med i ovennævnte program.

54. Ved afslutningen af sikkerhedsinspektionen forelægges de vigtigste konklusioner og anbefalinger for den inspicerede enhed. Inspektionsholdet udarbejder derefter en inspektionsrapport. Hvis der foreslås korrigerende foranstaltninger, og fremsættes anbefalinger, medtages der tilstrækkelige detaljer i rapporten til at understøtte konklusionerne. Rapporten fremsendes til EU-Udenrigstjenestens sikkerhedsmyndighed og til lederen af den inspicerede enhed.

Der udarbejdes regelmæssigt en rapport under EU-Udenrigstjenestens Sikkerhedsdirektorats ansvar for at fremhæve erfaringerne fra de inspektioner, der er gennemført i en nærmere angivet periode og behandlet af EU-Udenrigstjenestens Sikkerhedsudvalg.

Gennemførelse af og indberetning om sikkerhedsinspektioner i EU-agenturer og -organer, der er oprettet ifølge afsnit V, kapitel 2, i TEU

55. EU-Udenrigstjenestens Sikkerhedsdirektorat kan, når det er hensigtsmæssigt, udpege medvirkende eksperter til at deltage i fælles EU-inspektionshold, som udfører inspektioner i EU-agenturer og -organer, der er oprettet ifølge afsnit V, kapitel 2, i TEU.

Tjekliste for EU-Udenrigstjenestens sikkerhedsinspektioner

56. EU-Udenrigstjenestens Sikkerhedsdirektorat udarbejder og ajourfører en sikkerhedsinspektionstjekliste over de punkter, der skal kontrolleres ved EU-Udenrigstjenestens sikkerhedsinspektion. Denne tjekliste fremsendes til EU-Udenrigstjenestens Sikkerhedsudvalg.

57. Oplysninger til brug for tjeklisten indhentes, navnlig under inspektionen, hos de ledende sikkerhedsansvarlige i den enhed, der inspiceres. Når tjeklisten er udfyldt med de detaljerede svar, klassificeres den efter aftale med den inspicerede enhed. Den indgår ikke i inspektionsrapporten.

BILAG A IV

BESKYTTELSE AF EUCI, DER HÅNDTERES I CIS'ER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 8 i bilag A.

2. Følgende egenskaber og koncepter for informationssikring (IA) er væsentlige for sikkerheden og for, at operationer i kommunikations- og informationssystemer (CIS'er) kan fungere korrekt:

autenticitet:	sikkerhed for, at informationer er ægte og fra bona fide-kilder
tilgængelighed:	det forhold, at informationer er tilgængelige og kan anvendes på anmodning fra en autoriseret enhed
fortrolighed:	det forhold, at informationer ikke videregives til uautoriserede personer, enheder eller processer
integritet:	sikring af informationernes og aktivernes rigtighed og fuldstændighed
uafviselighed:	evnen til at bevise, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes.

II. INFORMATIONSSIKRINGSPRINCIPPER

3. Nedenstående bestemmelser er grundlaget for sikkerhedsbeskyttelse af al håndtering af EUCI i CIS'er. Detaljerede krav til gennemførelse af disse bestemmelser defineres i sikkerhedspolitikker og sikkerhedsretningslinjer for informationssikring.

Sikkerhedsrisikostyring

4. Sikkerhedsrisikostyringen skal være en integrerende del af at fastlægge, udvikle, drive og opretholde CIS'er. Risikostyringen (vurdering, behandling, accept og kommunikation) skal foregå som en gentagelsesproces, der gennemføres i fællesskab af repræsentanter for systemejere, projektmyndigheder, driftsmyndigheder og sikkerhedsakkrediteringsmyndigheder under anvendelse af en gennemprøvet, gennemsigtig og fuldt forståelig risikovurderingsproces. Anvendelsesområdet for CIS'et og dets aktiver skal klart defineres i starten af risikostyringsprocessen.

5. De kompetente myndigheder skal tage de potentielle trusler mod CIS'er op til revision og opretholde ajourførte og præcise trusselvurderinger, der afspejler det aktuelle operative miljø. De skal hele tiden ajourføre deres viden om spørgsmål i forbindelse med sårbarhed og regelmæssigt tage sårbarhedsvurderingen op til revision med afsæt i et informationsteknologimiljø (it-miljø) i stadig forandring.

6. Formålet med sikkerhedsrisikostyringen er at anvende et sæt sikkerhedsforanstaltninger, der giver sig udslag i en tilfredsstillende balance mellem brugerkrav og residualsikkerhedsrisiko.

7. De specifikke krav og det detaljeringsomfang og den detaljeringsgrad, der fastlægges af den relevante sikkerhedsakkrediteringsmyndighed (SAA) ved akkreditering af et CIS, skal svare til den vurderede risiko under hensyntagen til alle relevante faktorer, herunder klassifikationsgraden af de EUCI, der håndteres i CIS'et. Akkreditering skal omfatte en formel udredning om residualrisikoen og en ansvarlig myndigheds accept af residualrisikoen.

Sikkerhed i hele CIS'ets livscyklus

8. Opretholdelse af sikkerheden skal være et krav i den samlede CIS-livscyklus fra startfasen til udtagningen af drift.

9. Den rolle, som hver enkelt aktør i et CIS spiller, og dens interaktion med hensyn til sikkerhed skal fastlægges for hver fase af livscyklussen.

10. Ethvert CIS, herunder dets tekniske og ikke-tekniske sikkerhedsforanstaltninger, er underkastet afprøvning af sikkerheden under akkrediteringsprocessen for at sikre, at det relevante sikkerhedsniveau ved de gennemførte sikkerhedsforanstaltninger er nået, og kontrollere, at de er korrekt gennemført, integreret og konfigureret.

11. Der skal regelmæssigt udføres sikkerhedsvurderinger, -inspektioner og -revisioner under driften og vedligeholdelsen af et CIS, og når der opstår ekstraordinære omstændigheder.

12. Sikkerhedsdokumentationen for et CIS skal udvikles i løbet af dets livscyklus som en integrerende del af ændrings- og konfigurationsstyringsprocessen.

Bedste praksis

13. EU-Udenrigstjenesten samarbejder med GSC, Kommissionen og medlemsstaterne om at udvikle bedste praksis for sikkerhedsbeskyttelse af EUCI, der håndteres i CIS'er. Retningslinjerne for bedste praksis skal omfatte de tekniske, fysiske, organisatoriske og proceduremæssige sikkerhedsforanstaltninger for CIS'er, som bevisligt er effektive med hensyn til imødegåelse af trusler og sårbarheder.

14. Sikkerhedsbeskyttelsen af EUCI, der håndteres i CIS'er, skal trække på de erfaringer, som enheder involveret i IA både inden for og uden for EU har gjort.

15. Udbredelsen og den efterfølgende gennemførelse af bedste praksis skal bidrage til at nå et ækvivalent sikringsniveau for de forskellige CIS'er, der drives af EU-Udenrigstjenesten til håndtering af EUCI.

Dybdeforsvar

16. For at afbøde risikoen i forbindelse med CIS'er skal der gennemføres en række tekniske og ikke-tekniske sikkerhedsforanstaltninger, der er organiseret som en kæde af forsvarsmekanismer. Denne kæde skal omfatte:

a) *afskrækkelse:* sikkerhedsforanstaltninger med det formål at afskrække fjendtlig planlægning af angreb på CIS'er

b) *forebyggelse:* sikkerhedsforanstaltninger med det formål at hindre eller blokere angreb på CIS'er

c) *afsløring:* sikkerhedsforanstaltninger med det formål at opdage angreb på CIS'er

d) *modstandsdygtighed:* sikkerhedsforanstaltninger med det formål at begrænse virkningerne af et angreb til et minimum af informationer eller CIS-aktiver og afværge yderligere skade

e) *genopretning:* sikkerhedsforanstaltninger med det formål at genoprette en sikker situation for CIS'er.

Det skal afgøres ved en risikovurdering, hvor strenge og udbredte disse tekniske sikkerhedsforanstaltninger skal være.

17. De kompetente myndigheder skal sikre, at de kan imødegå hændelser, der kan overskride organisatoriske og nationale grænser, med henblik på at koordinere svar og udveksle informationer om disse hændelser og den hermed forbundne risiko (edb-nødberedskabskapaciteter).

Minimalisme- og "least privilege"-princippet

18. Der implementeres kun de funktioner, det udstyr og de tjenester, der skal til for at opfylde operative behov og undgå unødvendige risici.

19. CIS-brugere og automatiserede processer skal kun tildeles den adgang, de privilegier eller de autorisationer, der er behov for til at udføre opgaverne, for at begrænse enhver skade, der kan opstå ved uheld, fejl eller uautoriseret brug af CIS-ressourcer.

20. De registreringsprocedurer, der udføres af et CIS, skal, hvor det er nødvendigt, kontrolleres som led i akkrediteringsprocessen.

Bevidsthed om informationssikring (IA)

21. Den første forsvarslinje for CIS'ers sikkerhed er, at der er bevidsthed om risiciene og de tilgængelige sikkerhedsforanstaltninger. Det er navnlig nødvendigt, at alt det personale, der er involveret i CIS'ers livscyklus, herunder brugerne, forstår:

a) at sikkerhedssvigt i betydelig grad kan skade CIS'er og hele organisationen

b) den potentielle skade mod andre, som kan opstå på grund af sammenkobling og indbyrdes afhængighed

c) at de hver især har et ansvar og ansvarliggøres for CIS'ers sikkerhed afhængigt af deres roller inden for systemerne og processerne.

22. For at sikre, at sikkerhedsansvaret forstås, skal IA-uddannelse og –bevidstgørelse være obligatorisk for alt berørt personale, herunder ledere og CIS-brugere.

Evaluering og godkendelse af it-sikkerhedsprodukter

23. Den nødvendige grad af tillid til sikkerhedsforanstaltningerne, defineret som et sikringsniveau, fastlægges i overensstemmelse med resultatet af risikostyringsprocessen og med de relevante sikkerhedspolitikker og sikkerhedsretningslinjer.

24. Sikringsniveauet efterprøves ved at anvende internationalt anerkendte eller nationalt godkendte processer og metoder. Dette omfatter primært evaluering, kontrol og revision.

25. Kryptoprodukter til sikkerhedsbeskyttelse af EUCI skal først evalueres og godkendes af en national kryptogodkendelsesmyndighed (CAA) i en medlemsstat.

26. Inden de kan anbefales til godkendelse af EU-Udenrigstjenestens CAA i overensstemmelse med artikel 7, stk. 5, i denne afgørelse, skal sådanne kryptoprodukter gennemgå en andenpartsevaluering med positivt resultat foretaget af en kvalificeret evalueringsmyndighed (AQUA) i en medlemsstat, der ikke medvirker til at designe eller fremstille udstyret. Hvor detaljeret andenpartsevalueringen skal være, afhænger af den planlagte højeste klassifikationsgrad for de EUCI, der skal beskyttes ved hjælp af disse produkter.

27. Hvis det er berettiget af specifikke operative grunde, kan EU-Udenrigstjenestens CAA efter henstilling fra Rådets Sikkerhedsudvalg dispensere fra kravene ifølge punkt 25 eller 26 og udstede en midlertidig godkendelse for en specifik periode efter proceduren i artikel 7, stk. 5, i denne afgørelse.

28. En AQUA skal være en CAA i en medlemsstat, der på grundlag af kriterier, som er fastsat af Rådet, er blevet akkrediteret til at foretage andenpartsevalueringen af kryptoprodukter til beskyttelse af EUCI.

29. Den højtstående repræsentant skal godkende en sikkerhedspolitik for kvalifikation og godkendelse af ikke-kryptografiske it-sikkerhedsprodukter.

Transmission inden for sikrede områder

30. Ved transmission af EUCI inden for sikrede områder kan ukrypteret distribution eller kryptering på et lavere niveau anvendes på grundlag af resultatet af en risikostyringsproces og med forbehold af godkendelse fra SAA'en, jf. dog bestemmelserne i denne afgørelse.

Sikker sammenkobling af CIS'er

31. I denne afgørelse forstås ved systemsammenkobling direkte kobling af to eller flere it-systemer med henblik på udveksling af data og andre informationsressourcer (f.eks. kommunikation) i en eller flere retninger.

32. Et CIS skal behandle et tilkoblet it-system som upålideligt og gennemføre beskyttelsesforanstaltninger for at kontrollere udvekslingen af klassificerede informationer.

33. For alle sammenkoblinger af et CIS med et andet it-system skal følgende grundlæggende krav opfyldes:

a) de forretningsmæssige eller operative krav til sådanne sammenkoblinger skal fastlægges og godkendes af de kompetente myndigheder

b) sammenkoblingen skal gennemgå en risikostyrings- og akkrediteringsproces og godkendes af de kompetente SAA'er

c) der skal oprettes grænsebeskyttelsestjenester (BPS) rundt om alle CIS'er.

34. Der må ikke være nogen sammenkobling mellem et akkrediteret CIS og et ubeskyttet eller offentligt netværk, medmindre CIS'et har godkendt den BPS, der er installeret til dette formål mellem CIS'et og det ubeskyttede eller offentlige netværk. Sikkerhedsforanstaltningerne for sådanne sammenkoblinger skal tages op til revision af den kompetente informationssikringsmyndighed (IAA) og godkendes af den kompetente SAA.

Hvis det ubeskyttede eller offentlige netværk udelukkende anvendes som bærer, og dataene er krypteret ved hjælp af et kryptoprodukt, som er godkendt i overensstemmelse med artikel 7, stk. 5, i denne afgørelse, anses forbindelsen ikke for at være en sammenkobling.

35. Direkte sammenkobling eller kaskadekobling mellem et CIS, som er akkrediteret til at håndtere informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, og et ubeskyttet eller offentligt netværk er forbudt.

Edb-lagringsmedier

36. Edb-lagringsmedier skal destrueres i overensstemmelse med procedurer, der er godkendt af EU-Udenrigstjenestens sikkerhedsmyndighed.

37. Edb-lagringsmedier skal genanvendes, nedklassificeres eller afklassificeres i overensstemmelse med en sikkerhedspolitik, der skal fastlægges i henhold til artikel 7, stk. 2, i denne afgørelse.

Nødsituationer

38. Uanset bestemmelserne i denne afgørelse kan de særlige procedurer, der er beskrevet i det følgende, anvendes i et begrænset tidsrum i en nødsituation, f.eks. under forestående eller faktiske krise-, konflikt- eller krigssituationer eller under ekstraordinære operative forhold.

39. EUCI kan transmitteres ved hjælp af kryptoprodukter, der er godkendt til en lavere klassifikationsgrad eller endog ukrypteret med den kompetente myndigheds godkendelse, hvis eventuel forsinkelse ville forvolde en skade, der er langt alvorligere end den skade, som videregivelse af det klassificerede materiale ville forvolde, og hvis:

a) afsender og modtager ikke har de krævede krypteringsmidler eller slet ingen krypteringsmidler har

b) det klassificerede materiale ikke kan sendes i tide med andre midler.

40. Klassificerede informationer, der transmitteres under de i stk. 39 nævnte omstændigheder, må ikke bære nogen mærkning eller påtegning, der skiller dem ud fra informationer, der er uklassificeret eller kan beskyttes ved hjælp af et disponibelt kryptoprodukt. Modtagerne skal via andre midler straks underrettes om klassifikationsgraden.

41. Ved anvendelse af punkt 39 aflægges der efterfølgende rapport til EU-Udenrigstjenestens Sikkerhedsdirektorat, som så aflægger rapport til EU-Udenrigstjenestens Sikkerhedsudvalg. Af denne rapport skal som minimum fremgå afsenderen, modtagen og udstederen af hver enkelt EUCI.

III. INFORMATIONSSIKRINGSFUNKTIONER OG -MYNDIGHEDER

42. Der skal oprettes følgende IA-funktioner i medlemsstaterne og i EU-Udenrigstjenesten. Disse funktioner behøver ikke være organiseret i individuelle enheder. De skal have separate mandater. Disse funktioner og det medfølgende ansvar kan dog kombineres eller integreres i samme organisatoriske enhed eller opdeles i forskellige organisatoriske enheder, forudsat at det undgås, at der opstår interne interessekonflikter eller konflikter mellem arbejdsopgaver.

Informationssikringsmyndigheden (IAA)

43. IAA'en er ansvarlig for:

a) udvikling af IA-sikkerhedspolitikker og sikkerhedsretningslinjer og overvågning af deres effektivitet og relevans

b) beskyttelse og forvaltning af tekniske informationer om kryptoprodukter

c) sikring af, at de IA-foranstaltninger, der vælges til sikkerhedsbeskyttelse af EUCI, er i overensstemmelse med de relevante politikker for deres egnethed og udvælgelse

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

e) koordinering af IA-uddannelse og -bevidstgørelse

f) samarbejde med systemleverandøren, sikkerhedsaktørerne og brugerrepræsentanterne med hensyn til IA-sikkerhedspolitikkerne og sikkerhedsretningslinjerne

g) sikring af, at den relevante ekspertise er til rådighed i EU-Udenrigstjenestens Sikkerhedsudvalgs ekspertunderudvalg vedrørende IA-spørgsmål.

Tempestmyndigheden

44. Tempestmyndigheden (TA) er ansvarlig for at sikre, at CIS'er er i overensstemmelse med Tempestpolitikkerne og -retningslinjerne. Den skal godkende Tempestmodforanstaltninger vedrørende anlæg og produkter til beskyttelse af EUCI op til en nærmere bestemt klassifikationsgrad i det operative miljø.

Kryptogodkendelsesmyndighed (CAA)

45. CAA'en er ansvarlig for at sikre, at kryptoprodukter er i overensstemmelse med de respektive kryptopolitikker. Den skal godkende et kryptoprodukt til beskyttelse af EUCI op til en nærmere bestemt klassifikationsgrad i det operative miljø.

Kryptodistributionsmyndighed (CDA)

46. CDA'en er ansvarlig for:

a) at forvalte og stå til regnskab for EU-kryptomateriale

b) at sikre, at der indføres og anvendes relevante procedurer og kanaler med henblik på at kunne stå til regnskab for alt EU-kryptomateriale og sikre håndtering, opbevaring og distribution deraf

c) at sikre overdragelse af EU-kryptomateriale til eller fra enkeltpersoner eller tjenester, der bruger det.

Sikkerhedsakkrediteringsmyndighed (SAA)

47. Sikkerhedsakkrediteringsmyndigheden (SAA) for hvert system er ansvarlig for:

a) at sikre, at CIS'er overholder de relevante sikkerhedspolitikker og sikkerhedsretningslinjer, samt udstede en godkendelse af et CIS til at håndtere EUCI med en nærmere bestemt klassifikationsgrad i det operative miljø og angive betingelserne for akkrediteringen og kriterierne for fornyet godkendelse

b) at etablere en sikkerhedsakkrediteringsproces i overensstemmelse med de relevante politikker, som klart angiver de godkendelsesbetingelser, der gælder for et CIS, den har ansvaret for

c) at definere en sikkerhedsakkrediteringsstrategi, der fastsætter en detaljeringsgrad for akkrediteringsprocessen svarende til det krævede sikringsniveau

d) at gennemgå og godkende sikkerhedsrelateret dokumentation, herunder udredninger om risikostyring og residualrisiko, systemspecifikke sikkerhedskrav (i det følgende benævnt "SSRS'er"), dokumentation for kontrol af sikkerhedsimplementering og operationelle sikkerhedsprocedurer (i det følgende benævnt "SecOP'er"), samt sikre, at den er i overensstemmelse med EU-Udenrigstjenestens sikkerhedsregler og sikkerhedspolitik

e) at kontrollere implementeringen af sikkerhedsforanstaltningerne i forbindelse med CIS'et ved at foretage eller få foretaget sikkerhedsvurderinger, -inspektioner eller -revisioner

f) at fastlægge sikkerhedskrav (f.eks. niveauer for personelsikkerhedsgodkendelse) for CIS-følsomme stillinger

g) at godkende valget af godkendte krypto- og Tempestprodukter, der anvendes med henblik på at sikre et CIS

h) at godkende eller, hvor det er relevant, deltage i den fælles godkendelse af sammenkoblingen af et CIS med andre CIS'er

i) at samarbejde med systemleverandøren, sikkerhedsaktørerne og brugerrepræsentanterne om sikkerhedsrisikostyring, især residualrisikoen, og betingelserne for godkendelseserklæringen.

48. EU-Udenrigstjenestens SAA er ansvarlig for akkreditering af alle CIS'er, der anvendes inden for EU-Udenrigstjenestens kompetenceområde.

Sikkerhedsakkrediteringsudvalg (SAB)

49. Et fælles SAB er ansvarligt for akkreditering af CIS'er, der både henhører under EU-Udenrigstjenestens SAA og medlemsstaternes SAA'er. Det består af en SAA-repræsentant fra hver medlemsstat med deltagelse af en SAA-repræsentant for GSC og Kommissionen. Andre enheder med knudepunkter i et CIS indbydes til at deltage, når det pågældende system drøftes.

SAB har en repræsentant for EU-Udenrigstjenestens SAA som formand. Det træffer afgørelse ved konsensus blandt SAA-repræsentanterne for institutioner, medlemsstater og andre enheder med knudepunkter i CIS'et. Det aflægger regelmæssigt rapport om sine aktiviteter til EU-Udenrigstjenestens Sikkerhedsudvalg og meddeler det alle akkrediteringsudredninger.

Den operative informationssikringsmyndighed

50. Den operative IA-myndighed for hvert system er ansvarlig for:

a) at udvikle sikkerhedsdokumentation i overensstemmelse med sikkerhedspolitikkerne og sikkerhedsretningslinjerne, især systemspecifikke sikkerhedskrav (SSRS), herunder udredningen om residualrisikoen, operationelle sikkerhedsprocedurer (SecOP'er) og kryptoplanen i forbindelse med CIS-akkrediteringsprocessen

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

c) at deltage i udvælgelse af Tempestsikkerhedsforanstaltninger og -anordninger, hvis det kræves i SSRS, og sikre, at de installeres og vedligeholdes sikkert i samarbejde med TA

d) at overvåge gennemførelse og anvendelse af SecOP'er og, hvor det er relevant, uddelegere operationelt sikkerhedsansvar til systemejeren

e) at forvalte og håndtere kryptoprodukter samt sikre opbevaring af kryptomateriale og kontrolleret materiale og om nødvendigt generering af kryptovariabler

f) at gennemføre sikkerhedsanalyserevisioner og -afprøvninger, især for at udarbejde relevante risikorapporter som krævet af SAA'en

g) at tilbyde CIS-specifik IA-uddannelse

h) at implementere og anvende CIS-specifikke sikkerhedsforanstaltninger.

BILAG A V

INDUSTRISIKKERHED

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 9 i bilag A. Det fastsætter generelle sikkerhedsbestemmelser, der er gældende for industrivirksomheder eller andre enheder under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter, der tildeles af EU-Udenrigstjenesten.

2. Den højtstående repræsentant godkender en politik for industrisikkerhed, der navnlig indeholder detaljerede krav vedrørende facilitetssikkerhedsgodkendelser (FSC'er), de særlige sikkerhedsbetingelser (SAL), besøg, transmission og transport af EUCI.

II. SIKKERHEDSELEMENTER I EN KLASSIFICERET KONTRAKT

Klassifikationsvejledning (SCG)

3. Inden der iværksættes et udbud eller tildeles en klassificeret kontrakt, skal EU-Udenrigstjenesten som kontraherende myndighed fastsætte klassifikationsgraden for informationer, som skal videregives til bydende og kontrahenter, samt klassifikationsgraden for informationer, som kontrahenten skal udarbejde. Med henblik herpå udarbejder EU-Udenrigstjenesten en SCG, der skal anvendes ved opfyldelsen af kontrakten.

4. For at fastlægge klassifikationsgraden for de forskellige elementer i en klassificeret kontrakt anvendes følgende principper:

   a) ved udarbejdelsen af en SCG skal EU-Udenrigstjenesten tage hensyn til alle relevante sikkerhedsaspekter, herunder den klassifikationsgrad, der er tildelt informationer, som udstederen af informationerne har videregivet og godkendt til brug for kontrakten

   b) en kontrakts samlede klassifikationsgrad kan ikke være lavere end den højeste klassifikationsgrad for dens elementer

   c) EU-Udenrigstjenesten skal, når det er relevant, samarbejde med medlemsstaternes NSA'er/DSA'er eller en anden berørt kompetent sikkerhedsmyndighed, hvis der skal foretages ændringer i klassifikationen af informationer, der er udarbejdet af eller videregivet til kontrahenter i forbindelse med opfyldelsen af en kontrakt, og når der foretages eventuelle efterfølgende ændringer af SCG.

Særlige sikkerhedsbetingelser (SAL)

5. Sikkerhedskravene for de enkelte kontrakter beskrives i SAL. SAL skal, når det er relevant, indeholde SCG og skal være en integrerende del af en klassificeret kontrakt eller underkontrakt.

6. SAL skal indeholde bestemmelser om, at kontrahenten og/eller underkontrahenten skal opfylde minimumsstandarderne i denne afgørelse. Manglende overholdelse af minimumsstandarderne kan udgøre en tilstrækkelig grund til, at kontrakten ophæves.

Program-/projektsikkerhedsinstruktion (PSI)

7. Afhængigt af omfanget af programmer eller projekter, der kræver adgang til eller håndtering eller opbevaring af EUCI, kan den kontraherende myndighed, der er udpeget til at forvalte programmet eller projektet, udarbejde specifikke program-/projektsikkerhedsinstruktioner (PSI). PSI kræver godkendelse fra medlemsstaternes NSA'er/DSA'er eller en anden berørt kompetent sikkerhedsmyndighed, der deltager i programmet/projektet, og kan indeholde yderligere sikkerhedskrav.

III. FACILITETSSIKKERHEDSGODKENDELSE (FSC)

8. EU-Udenrigstjenestens Sikkerhedsdirektorat beder en NSA eller DSA eller en anden kompetent sikkerhedsmyndighed i medlemsstaten om at tildele en FSC som angivelse af, at en industrivirksomhed eller en anden enhed i overensstemmelse med nationale love og bestemmelser kan sikkerhedsbeskytte EUCI med den relevante klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) inden for sine faciliteter. En kontrahent, underkontrahent eller en potentiel kontrahent eller underkontrahent kan først få rådighed over eller tildeles adgang til EUCI, når beviset for FSC er blevet sendt til EU-Udenrigstjenesten.

9. Når det er relevant, underretter EU-Udenrigstjenesten som kontraherende myndighed den relevante NSA/DSA eller en anden kompetent sikkerhedsmyndighed om, at der er behov for en FSC i perioden forud for indgåelse af en kontrakt eller med henblik på opfyldelsen af en kontrakt. En FSC eller PSC er påkrævet i perioden forud for indgåelsen af en kontrakt, hvis EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal videregives i løbet af udbudsproceduren.

10. EU-Udenrigstjenesten tildeler som kontraherende myndighed ikke en klassificeret kontrakt til en udvalgt bydende, før den fra NSA'en/DSA'en eller en anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor den pågældende kontrahent eller underkontrahent er registreret, har fået bekræftet, at den relevante FSC, hvor det er påkrævet, er udstedt.

11. EU-Udenrigstjenesten anmoder som kontraherende myndighed NSA/DSA eller en anden kompetent sikkerhedsmyndighed, som har udstedt en FSC, om at underrette om eventuelle negative oplysninger, der påvirker FSC'en. I tilfælde af en underkontrakt underrettes NSA'en/DSA'en eller en anden kompetent sikkerhedsmyndighed tilsvarende.

12. Hvis den relevante NSA/DSA eller en anden kompetent sikkerhedsmyndighed inddrager en FSC, er det en tilstrækkelig grund til, at EU-Udenrigstjenesten som kontraherende myndighed ophæver en klassificeret kontrakt eller udelukker en bydende fra udvælgelsen.

IV. PERSONELSIKKERHEDSGODKENDELSER (PSC'ER) FOR KONTRAHENTERS PERSONEL

13. Alt personel, der arbejder for kontrahenter, og som har behov for adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal være hensigtsmæssigt sikkerhedsgodkendt og have "need-to-know" vedrørende adgang til informationerne. Selv om der ikke kræves en PSC for adgang til EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED, gælder "need-to-know"-princippet for en sådan adgang.

14. Ansøgninger om PSC'er for kontrahenters personel skal fremsættes over for den NSA/DSA, der har ansvaret for enheden.

15. EU-Udenrigstjenesten skal understrege over for kontrahenter, der ønsker at ansætte en statsborger fra et tredjeland i en stilling, der kræver adgang til EUCI, at ansvaret for at beslutte, om den pågældende kan tildeles adgang til sådanne informationer, jf. denne afgørelse, og bekræfte at udstederens samtykke skal foreligge, inden der gives en sådan adgang, påhviler NSA/DSA'en i den medlemsstat, hvor den ansættende enhed er lokaliseret og registreret.

V. KLASSIFICEREDE KONTRAKTER OG UNDERKONTRAKTER

16. Hvis EUCI videregives til en bydende i perioden forud for indgåelsen af en kontrakt, skal udbudsbekendtgørelsen indeholde en bestemmelse, der forpligter den bydende, der undlader at afgive bud, eller som ikke udvælges, til at returnere alle klassificerede dokumenter inden for en bestemt tidsfrist.

17. Når der er tildelt en klassificeret kontrakt eller underkontrakt, underretter EU-Udenrigstjenesten som kontraherende myndighed kontrahentens eller underkontrahentens NSA/DSA eller en anden kompetent sikkerhedsmyndighed om sikkerhedsbestemmelserne for den klassificerede kontrakt.

18. Når sådanne kontrakter ophæves eller udløber, underretter EU-Udenrigstjenesten som kontraherende myndighed (og/eller, alt efter hvad der er hensigtsmæssigt, NSA'en/DSA'en eller en anden kompetent sikkerhedsmyndighed i tilfælde af en underkontrakt) straks NSA'en/DSA'en eller en anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor kontrahenten eller underkontrahenten er registreret.

19. Som hovedregel er kontrahenten eller underkontrahenten forpligtet til at returnere EUCI, som vedkommende er i besiddelse af, til den kontraherende myndighed ved ophævelsen eller udløbet af den klassificerede kontrakt eller underkontrakt.

20. De særlige bestemmelser for bortskaffelse af EUCI under opfyldelsen af kontrakten eller ved dens ophævelse eller udløb fastsættes i SAL.

21. Er kontrahenten eller underkontrahenten autoriseret til at beholde EUCI efter kontraktens ophævelse eller udløb, skal minimumsstandarderne i denne afgørelse fortsat opfyldes, og kontrahenten eller underkontrahenten skal beskytte EUCI's fortrolighed.

22. De betingelser, hvorpå kontrahenten kan udbyde dele af kontrakten i underentreprise, skal fastsættes i udbuddet og i kontrakten.

23. En kontrahent skal indhente tilladelse fra EU-Udenrigstjenesten som kontraherende myndighed, inden en del af en klassificeret kontrakt udbydes i underentreprise. En underkontrakt må ikke tildeles industrivirksomheder eller andre enheder, som er registreret i et tredjeland, der ikke har indgået en informationssikkerhedsaftale med EU.

24. Kontrahenten er ansvarlig for at sikre, at alle underkontraheringsaktiviteter gennemføres i overensstemmelse med minimumsstandarderne i denne afgørelse, og må ikke videregive EUCI til en underkontrahent uden forudgående skriftligt samtykke fra den kontraherende myndighed.

25. For så vidt angår EUCI, der udarbejdes eller håndteres af kontrahenten eller underkontrahenten, varetager den kontraherende myndighed udsteders rettigheder.

VI. BESØG I FORBINDELSE MED KLASSIFICEREDE KONTRAKTER

26. Hvis EU-Udenrigstjenesten, kontrahenter eller underkontrahenter skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, i hinandens lokaliteter med henblik på opfyldelse af en klassificeret kontrakt, skal der tilrettelægges besøg i samråd med de pågældende NSA'er/DSA'er eller en anden berørt kompetent sikkerhedsmyndighed. Dette berører ikke NSA'ers/DSA'ers forret til i forbindelse med specifikke projekter at blive enige om en procedure, hvormed disse besøg kan arrangeres straks.

27. Alle besøgende skal være i besiddelse af en relevant PSC og have "need-to-know" med henblik på adgang til EUCI vedrørende kontrakten med EU-Udenrigstjenesten.

28. Besøgende kan kun få adgang til EUCI, der har relation til besøgets formål.

VII. TRANSMISSION OG TRANSPORT AF EUCI

29. For så vidt angår elektronisk transmission af EUCI, finder de relevante bestemmelser i artikel 8 i bilag A og i bilag A IV anvendelse.

30. For så vidt angår transport af EUCI, finder de relevante bestemmelser i bilag A III til denne afgørelse i overensstemmelse med nationale love og bestemmelser anvendelse.

31. For så vidt angår fragttransport af klassificeret materiale, finder følgende principper anvendelse ved fastlæggelsen af sikkerhedsordninger:

a) sikkerheden skal garanteres på alle stadier under transporten fra udgangspunktet til det endelige bestemmelsessted

b) den beskyttelsesgrad, der skal tillægges en forsendelse, bestemmes af den højeste klassifikationsgrad for det materiale, den indeholder

c) transportvirksomhederne skal have en FSC på det rette niveau, hvis den også indebærer, at klassificerede informationer opbevares i kontrahenters faciliteter. Under alle omstændigheder skal medarbejdere, der håndterer forsendelsen, være hensigtsmæssigt sikkerhedsgodkendt i overensstemmelse med bilag A I

d) forud for enhver grænseoverskridende transport af materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, udarbejder afsenderen en transportplan, som godkendes af EU-Udenrigstjenesten og om fornødent i samråd med NSA'er/DSA'er for både afsenderen og modtageren eller andre berørte kompetente sikkerhedsmyndigheder

e) transporten gennemføres så vidt muligt direkte og afsluttes så hurtigt, som forholdene tillader

f) ruterne bør så vidt muligt kun gå gennem medlemsstater. Der bør kun benyttes ruter gennem andre lande end medlemsstater, hvis EU-Udenrigstjenesten eller en anden kompetent sikkerhedsmyndighed i såvel afsenderens som modtagerens stat har givet tilladelse hertil.

VIII. VIDEREGIVELSE AF EUCI TIL KONTRAHENTER I TREDJELANDE

32. EUCI videregives til kontrahenter og underkontrahenter i tredjelande, som har en gældende sikkerhedsaftale med EU i overensstemmelse med de sikkerhedsforanstaltninger, der er aftalt mellem EU-Udenrigstjenesten som kontraherende myndighed og NSA'en/DSA'en i det pågældende tredjeland, hvor kontrahenten er registreret.

IX. HÅNDTERING OG OPBEVARING INFORMATIONER, DER ER KLASSIFICERET RESTREINT UE/EU RESTRICTED

33. Sammen med medlemsstatens NSA/DSA, alt efter hvad der er hensigtsmæssigt, har EU-Udenrigstjenesten som kontraherende myndighed ret til at besøge kontrahenters/underkontrahenters faciliteter på grundlag af kontraktbestemmelser for at kontrollere, at de relevante sikkerhedsforanstaltninger til beskyttelse af EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, er indført som krævet ifølge kontrakten.

34. I det omfang, det er nødvendigt i henhold til nationale love og bestemmelser, underretter EU-Udenrigstjenesten som kontraherende myndighed NSA'er/DSA'er eller en anden kompetent sikkerhedsmyndighed om kontrakter eller underkontrakter, som indeholder informationer, der er klassificeret RESTREINT UE/EU RESTRICTED.

35. En FSC eller en PSC til kontrahenter eller underkontrahenter og deres personale er ikke påkrævet for kontrakter, EU-Udenrigstjenesten tildeler, og som indeholder informationer, der er klassificeret RESTREINT UE/EU RESTRICTED.

36. EU-Udenrigstjenesten undersøger som kontraherende myndighed svarene på udbud vedrørende kontrakter, der kræver adgang til informationer, som er klassificeret RESTREINT UE/EU RESTRICTED, uanset de krav med hensyn til FSC eller PSC, der måtte findes i nationale love og bestemmelser.

37. De betingelser, hvorpå kontrahenten kan udbyde dele af kontrakten i underentreprise, skal være i overensstemmelse med punkt 22-24.

38. Hvis en kontrakt omfatter håndtering af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, i et CIS, som drives af en kontrahent, sikrer EU-Udenrigstjenesten som kontraherende myndighed, at kontrakten eller underkontrakten nærmere beskriver de nødvendige tekniske og administrative krav for akkreditering af CIS'et, som svarer til den vurderede risiko, under hensyntagen til alle relevante faktorer. Omfanget af akkrediteringen af et CIS aftales mellem den kontraherende myndighed og den relevante NSA/DSA.

BILAG A VI

UDVEKSLING AF KLASSIFICEREDE INFORMATIONER MED TREDJELANDE OG INTERNATIONALE ORGANISATIONER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 10 i bilag A.

II. RAMMER FOR UDVEKSLING AF KLASSIFICEREDE INFORMATIONER

2. EU-Udenrigstjenesten kan udveksle EUCI med tredjelande eller internationale organisationer i henhold til bilag A, artikel 10, stk. 1.

For at støtte HR med at udføre opgaverne som fastsat i artikel 218 i TEUF skal:

a) den relevante geografiske eller tematiske afdeling i EU-Udenrigstjenesten i samråd med EU-Udenrigstjenestens Sikkerhedsdirektorat, når det er hensigtsmæssigt, identificere behovet for langtidsudveksling af EUCI med det pågældende tredjeland eller den pågældende internationale organisation

b) EU-Udenrigstjenestens Sikkerhedsdirektorat i samråd med den relevante geografiske afdeling i EU-Udenrigstjenesten, når det er hensigtsmæssigt, præsentere HR for de tekstforslag, der skal fremlægges for Rådet i medfør af artikel 218, stk. 3, 5, og 6, i TEUF

c) EU-Udenrigstjenestens Sikkerhedsdirektorat støtte HR med at føre forhandlinger i samarbejde med de relevante tjenester i Kommissionen og Generalsekretariatet for Rådet

d) EU-Udenrigstjenestens Krisestyrings- og Planlægningsdirektorat i samråd med de relevante tjenester i EU-Udenrigstjenesten i forbindelse med aftaler eller ordninger med tredjelande om deres deltagelse i FSFP-krisestyringsoperationer, jf. bilag A, artikel 10, stk. 1, litra c), når det er hensigtsmæssigt, præsentere HR for de tekstforslag, som skal fremlægges for Rådet i medfør af TEUF, artikel 218, stk. 3, 5 og 6, og støtte HR med at føre forhandlinger i samarbejde med de relevante tjenester i EU-Udenrigstjenesten og i Generalsekretariatet for Rådet.

3. Hvis informationssikkerhedsaftaler indeholder en bestemmelse om, at der skal indgås aftale om tekniske gennemførelsesordninger mellem EU-Udenrigstjenestens Sikkerhedsdirektorat – i samarbejde med Sikkerhedsdirektoratet ved Kommissionens Generaldirektorat for Menneskelige Ressourcer og Sikkerhed og Sikkerhedskontoret ved Generalsekretariatet for Rådet – og den kompetente sikkerhedsmyndighed i det pågældende tredjeland eller den pågældende internationale organisation, skal der i disse ordninger tages højde for den beskyttelsesgrad samt de sikkerhedsbestemmelser, -strukturer og -procedurer, der er indført i det pågældende tredjeland eller den pågældende internationale organisation.

4. Hvis der er et langsigtet behov for, at EU-Udenrigstjenesten udveksler oplysninger, der ikke er klassificeret højere end RESTREINT UE/EU RESTRICTED, med et tredjeland eller en international organisation, og hvis det er konstateret, at den pågældende part ikke i tilstrækkelig grad har fået udarbejdet et sikkerhedssystem, der gør det muligt at indgå en informationssikkerhedsaftale, kan HR efter at have opnået en enstemmig positiv udtalelse fra EU-Udenrigstjenestens Sikkerhedsudvalg i henhold til artikel 14, stk. 5, i denne afgørelse indgå en administrativ ordning med de kompetente sikkerhedsmyndigheder i det pågældende tredjeland eller den pågældende internationale organisation.

5. Der må ikke ske nogen elektronisk udveksling af EUCI med et tredjeland eller en international organisation, medmindre dette udtrykkeligt er omtalt i informationssikkerhedsaftalen eller den administrative ordning.

6. I henhold til en administrativ ordning om udveksling af klassificerede informationer udpeger EU-Udenrigstjenesten og tredjelandet eller den internationale organisation hver især en registratur som det primære indgangs- og udgangspunkt for udvekslede klassificerede informationer. For EU-Udenrigstjenestens vedkommende vil dette være EU-Udenrigstjenestens centrale registratur.

7. Administrative ordninger skal som hovedregel have form af en brevveksling.

III VURDERINGSBESØG

8. Vurderingsbesøg, jf. artikel 16 i denne afgørelse, gennemføres efter gensidig aftale med det pågældende tredjeland eller den pågældende internationale organisation, og følgende evalueres:

a) lovrammerne for sikkerhedsbeskyttelsen af klassificerede informationer

b) særlige kendetegn ved sikkerhedslovene, -bestemmelserne, -politikkerne eller -procedurerne i tredjelandet eller den internationale organisation, der kan få indflydelse på den maksimale klassifikationsgrad for de informationer, der kan udveksles

c) de sikkerhedsforanstaltninger og -procedurer, der reelt er indført til beskyttelse af klassificerede informationer

d) sikkerhedsgodkendelsesprocedurerne i forbindelse med klassifikationsgraden for de EUCI, der skal videregives.

9. Der må ikke udveksles EUCI, inden der er gennemført et vurderingsbesøg, og det på baggrund af ækvivalensen for den beskyttelsesgrad, der vil blive givet, er besluttet i hvilken grad, der må udveksles klassificerede informationer mellem parterne.

Hvis der endnu ikke er gennemført et sådant vurderingsbesøg, og HR får kendskab til ekstraordinære eller presserende grunde til at udveksle klassificerede informationer, skal EU-Udenrigstjenesten:

a) først indhente udstederens skriftlige samtykke for at fastslå, at der ikke er nogen indvendinger mod videregivelse

b) henvise til EU-Udenrigstjenestens sikkerhedsmyndighed, der kan beslutte at videregive informationerne, forudsat at der er indhentet en enstemmig positiv udtalelse fra medlemsstaterne som repræsenteret i EU-Udenrigstjenestens Sikkerhedsudvalg.

Hvis EU-Udenrigstjenesten ikke kan identificere udstederen, påtager EU-Udenrigstjenestens sikkerhedsmyndighed sig udstederens ansvar efter at have indhentet en enstemmig positiv udtalelse fra EU-Udenrigstjenestens Sikkerhedsudvalg.

IV. BEMYNDIGELSE TIL AT VIDEREGIVE EUCI TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

10. Hvis der findes en ramme som omhandlet i bilag A, artikel 10, stk. 1, for udveksling af klassificerede informationer med et tredjeland eller en international organisation, træffer EU-Udenrigstjenestens sikkerhedsmyndighed en afgørelse om at videregive EUCI fra EU-Udenrigstjenesten til et tredjeland eller en international organisation, idet EU-Udenrigstjenestens sikkerhedsmyndighed kan uddelegere en sådan tilladelse til ledende tjenestemænd i EU-Udenrigstjenesten eller andre personer under dens myndighed.

11. Hvis udstederen af de klassificerede informationer, der skal videregives, herunder udstederne af det kildemateriale, de måtte indeholde, ikke er EU-Udenrigstjenesten, skal EU-Udenrigstjenesten først indhente udstederens skriftlige samtykke for at fastslå, at der ikke er nogen indvendinger mod videregivelse. Hvis EU-Udenrigstjenesten ikke kan identificere udstederen, påtager EU-Udenrigstjenestens sikkerhedsmyndighed sig udstederens ansvar efter at have indhentet en enstemmig positiv udtalelse fra medlemsstaterne som repræsenteret i EU-Udenrigstjenestens Sikkerhedsudvalg.

V. EKSTRAORDINÆR AD HOC-VIDEREGIVELSE AF EUCI

12. Hvis der ikke er etableret en ramme i overensstemmelse med bilag A, artikel 10, stk. 1, og når EU's eller en eller flere af medlemsstaternes interesser kræver videregivelse af EUCI af politiske, operationelle eller presserende grunde, kan EUCI undtagelsesvis videregives til et tredjeland eller en international organisation, når der er truffet følgende forholdsregler.

EU-Udenrigstjenestens Sikkerhedsdirektorat skal efter at have sikret, at betingelserne som omhandlet i stk. 11 ovenfor er opfyldt:

a) så vidt det er muligt, sammen med sikkerhedsmyndighederne i tredjelandet eller den internationale organisation kontrollere, at landets/organisationens sikkerhedsforskrifter, -strukturer og -procedurer er tilstrækkelige til at sikre, at de EUCI, der videregives, vil blive beskyttet efter standarder, der mindst svarer til dem, der er fastlagt i denne afgørelse

b) opfordre EU-Udenrigstjenestens Sikkerhedsudvalg til på grundlag af de disponible oplysninger at formulere en udtalelse vedrørende den tillid, der kan fæstes til sikkerhedsforskrifterne, -strukturerne og -procedurerne i det tredjeland eller den internationale organisation, som EUCI skal videregives til

c) henvise til EU-Udenrigstjenestens sikkerhedsmyndighed, der kan beslutte at videregive informationerne, forudsat at der er indhentet en enstemmig positiv udtalelse fra medlemsstaterne som repræsenteret i EU-Udenrigstjenestens Sikkerhedsudvalg.

13. Hvis der ikke er etableret en ramme i overensstemmelse med bilag A, artikel 10, stk. 1, skal den pågældende tredjepart skriftligt forpligte sig til at beskytte EUCI hensigtsmæssigt.

TILLÆG A

DEFINITIONER

I denne afgørelse finder følgende definitioner anvendelse:

"afklassificering": fjernelse af enhver klassifikationsgrad

"akkreditering": den proces, der fører til en formel erklæring fra sikkerhedsakkrediteringsmyndigheden (SAA) om, at et system er godkendt til håndtering af informationer med en nærmere bestemt klassifikationsgrad i en bestemt sikkerhedsindstilling i det operative miljø og på et acceptabelt risikoniveau baseret på, at der er gennemført en række godkendte tekniske, fysiske, organisatoriske og proceduremæssige sikkerhedsforanstaltninger

"aktiv": alt hvad der er af værdi for en organisation, dens forretningsmæssige drift og dennes kontinuitet, herunder informationsressourcer, der understøtter organisationens mission

"autorisation til adgang til EUCI": en autorisation udstedt af EU-Udenrigstjenestens sikkerhedsmyndighed i overensstemmelse med denne afgørelse, efter at de kompetente myndigheder i en medlemsstat har udstedt en PSC, og som bekræfter, at en person, forudsat at vedkommendes "need-to-know" er fastslået, kan tildeles adgang til EUCI op til en nærmere bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en nærmere bestemt dato, jf. i bilag A I, artikel 2

"brud": en persons handling eller manglende handling, der er i strid med sikkerhedsbestemmelserne i denne afgørelse og/eller sikkerhedspolitikkerne eller retningslinjerne vedrørende foranstaltninger, der er nødvendige for gennemførelse deraf

"certifikat for personelsikkerhedsgodkendelse" (PSCC): et certifikat udstedt af en kompetent myndighed, som fastslår, at en person er blevet sikkerhedsgodkendt og har en gyldig PSC med den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), den relevante PSC's gyldighedsdato og certifikatets udløbsdato

"CIS-livscyklus": hele det tidsrum, et CIS eksisterer, hvilket indbefatter projektinitiering, idébeskrivelse, planlægning, kravanalyse, udformning, udvikling, afprøvning, implementering, drift og vedligeholdelse samt nedlæggelse

"den udpegede sikkerhedsmyndighed" (DSA): en myndighed, der med reference til en medlemsstats nationale sikkerhedsmyndighed (NSA) er ansvarlig for formidling til industrivirksomheder eller andre enheder af den nationale politik med hensyn til alle spørgsmål vedrørende industrisikkerhed og for opstilling af retningslinjer og ydelse af bistand i forbindelse med denne politiks gennemførelse. DSA'ens funktion kan varetages af NSA'en eller af en hvilken som helst anden kompetent myndighed

"den, der er i besiddelse af": en behørigt autoriseret person med en fastslået "need-to-know", der er i besiddelse af EUCI og derfor er ansvarlig for at beskytte dem

"dokument": registrerede informationer uanset deres fysiske form eller karakteristika

"dybdeforsvar": anvendelse af en række sikkerhedsforanstaltninger, der er organiseret som en kæde af forsvarsmekanismer

"EU's klassificerede informationer" (EUCI): informationer eller materiale mærket med en EU-sikkerhedsklassifikation, jf. artikel 2, litra f), og hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes interesser skade i forskellig grad

"facilitetssikkerhedsgodkendelse" (FSC): en administrativ afgørelse truffet af en NSA eller DSA om, at en facilitet ud fra et sikkerhedsmæssigt synspunkt kan yde tilstrækkelig beskyttelse af EUCI til og med en nærmere bestemt klassifikationsgrad, og om, at dens medarbejdere, der skal have adgang til EUCI, er blevet behørigt sikkerhedsgodkendt og er gjort bekendt med de relevante sikkerhedskrav, der skal opfyldes med henblik på adgang til og beskyttelse af EUCI

"forvaltning af klassificerede informationer": anvendelse af administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus for at supplere foranstaltningerne i artikel 5, 6 og 8 og derved bidrage til at afskrække fra, afsløre og udbedre skade forårsaget af forsætlig eller uagtsom kompromittering eller bortkomst af sådanne informationer. Sådanne foranstaltninger omfatter bl.a. udarbejdelse, registrering, kopiering, oversættelse, transport, håndtering, opbevaring og destruktion af EUCI, jf. bilag A, artikel 7, stk. 1

"FSFP-operation": en militær eller civil krisestyringsoperation i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union

"fysisk sikkerhed" anvendelse af fysiske og tekniske beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til EUCI, jf. bilag A, artikel 6

"håndtering af EUCI": alle de foranstaltninger, som EUCI kan underkastes i hele deres livscyklus. Dette omfatter udarbejdelse, behandling, transport, nedklassificering, afklassificering og destruktion. I forbindelse med CIS omfatter det også indsamling, visning, transmission og opbevaring

"industrisikkerhed": anvendelse af foranstaltninger for at sikre, at kontrahenter eller underkontrahenter beskytter EUCI under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter, jf. i bilag A, artikel 9, stk. 1

"industrivirksomhed eller en anden enhed": en enhed, der er involveret i levering af varer, udførelse af arbejder eller levering af tjenesteydelser. Det kan være en enhed inden for industri, handel, tjenesteydelser, videnskab, forskning, uddannelse eller udvikling eller en selvstændig erhvervsdrivende

"informationssikring" (IA): i forbindelse med kommunikations- og informationssystemer tilliden til, at disse systemer beskytter de informationer, der håndteres, og at de fungerer, som de skal, når de skal, under de legitime brugeres kontrol. Effektiv IA sikrer et passende niveau af fortrolighed, integritet, tilgængelighed, uafviselighed og autenticitet. IA baseres på en risikostyringsproces, jf. bilag A, artikel 8, stk. 1

"klassificeret kontrakt": en kontrakt, som EU-Udenrigstjenesten indgår med en kontrahent om levering af varer, udførelse af arbejder eller levering af tjenesteydelser, såfremt kontraktens opfyldelse kræver eller indebærer adgang til eller udarbejdelse af EUCI

"klassificeret underkontrakt": en kontrakt, som en af EU-Udenrigstjenestens kontrahenter indgår med en anden kontrahent (dvs. underkontrahenten) om levering af varer, udførelse af arbejder eller levering af tjenesteydelser, såfremt kontraktens opfyldelse kræver eller indebærer adgang til eller udarbejdelse af EUCI

"klassifikationsvejledning" (SCG): et dokument, der beskriver de elementer af et program eller en kontrakt, som er klassificeret, med angivelse af de gældende klassifikationsgrader. SCG'en kan udvides i hele programmets eller kontraktens løbetid, og informationselementerne kan om- eller nedklassificeres. Når der findes en SCG, skal den indgå i SAL, jf. bilag A V, afsnit II

"kommunikations- og informationssystem" (CIS): et system, der muliggør håndtering af informationer i elektronisk form. Et kommunikations- og informationssystem omfatter alle de aktiver, der er nødvendige for dets drift, herunder infrastrukturer, organisation, personale og informationsressourcer, jf. i bilag A, artikel 8, stk. 2

"kompromittering af EUCI": hel eller delvis videregivelse af EUCI til uautoriserede personer eller enheder, jf. artikel 8, stk. 2

"kontrahent": en enkeltperson eller en retlig enhed, der har rets- og handleevne til at indgå kontrakter

"kryptografisk (krypto)materiale": kryptografiske algoritmer, kryptografiske hardware- og softwaremoduler samt produkter, der omfatter implementeringsdetaljer og tilhørende dokumentation og nøglingsmateriale

"materiale": ethvert dokument eller enhver maskine eller ethvert udstyr, der enten er fremstillet eller er ved at blive fremstillet

"nedklassificering": nedsættelse til en lavere klassifikationsgrad

"operationelle sikkerhedsprocedurer" (SecOP'er): en beskrivelse af den gennemførelse af sikkerhedspolitikken, der skal vedtages, af de operationelle procedurer, der skal følges, og af personalets ansvarsområder

"personelsikkerhed": anvendelse af foranstaltninger for at sikre, at adgang til EUCI kun gives til personer, som:

— har "need-to-know"

— i forbindelse med adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, er blevet sikkerhedsgodkendt til den relevante klassifikationsgrad eller på anden vis behørigt er godkendt i kraft af deres funktioner i overensstemmelse med nationale love og bestemmelser

— er blevet gjort bekendt med deres ansvar,

jf. bilag A, artikel 5, stk. 1

"personelsikkerhedsgodkendelse" (PSC) med henblik på adgang til EUCI: en erklæring fra en medlemsstats kompetente myndighed på baggrund af en sikkerhedsundersøgelse udført af en medlemsstats kompetente myndigheder, hvorved det attesteres, at vedkommende kan få adgang til EUCI op til en nærmere bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en nærmere bestemt dato, såfremt vedkommendes "need-to-know" er fastslået, og den pågældende betegnes som "sikkerhedsgodkendt"

"program-/projektsikkerhedsinstruktion" (PSI): en liste over sikkerhedsprocedurer, der anvendes i forbindelse med et bestemt program/projekt for at standardisere sikkerhedsprocedurerne, som kan revideres i hele programmets/projektets løbetid

"registrering": anvendelse af procedurer, som registrerer informationernes livscyklus, inklusive dets udbredelse og destruktion, jf. bilag A III, stk. 21

"residualrisiko": den risiko, der fortsat eksisterer, efter at der er gennemført sikkerhedsforanstaltninger, idet ikke alle trusler imødegås, og ikke alle sårbarheder kan fjernes

"risiko": muligheden for, at en given trussel vil udnytte indre og ydre sårbarheder i en organisation eller i nogen af de systemer, den benytter, og derved skade organisationen og dens materielle eller immaterielle aktiver. Den måles som en kombination af sandsynligheden for, at trusler indtræffer, og virkningen deraf

"risikoaccept": beslutningen om at acceptere, at der fortsat findes en residualrisiko efter risikobehandlingen

"risikobehandling": at afbøde, fjerne, reducere (gennem en passende kombination af tekniske, fysiske, organisatoriske eller proceduremæssige foranstaltninger), flytte eller overvåge risikoen

"risikokommunikation": udvikling af bevidstheden om risici blandt CIS-brugere, underretning af godkendelsesmyndigheder om sådanne risici og indberetning af dem til driftsmyndigheder

"risikostyringsproces": hele processen med at identificere, kontrollere og minimere usikre begivenheder, der kan påvirke sikkerheden i en organisation eller i de systemer, den anvender. Den omfatter samtlige risikorelaterede aktiviteter, herunder vurdering, behandling, accept og kommunikation

"risikovurdering": identifikation af trusler og sårbarheder og udførelse af den dertil knyttede risikoanalyse, dvs. analyse af sandsynlighed og virkning

"sammenkobling": i denne afgørelse den direkte kobling af to eller flere it-systemer med henblik på udveksling af data og andre informationsressourcer (f.eks. kommunikation) i en eller flere retninger, jf. bilag A IV, stk. 31

"sikkerhedsundersøgelse": de undersøgelser, som den kompetente myndighed i en medlemsstat foretager i overensstemmelse med denne stats nationale love og bestemmelser med henblik på at kunne konkludere, at der ikke er konstateret negative forhold, som kunne forhindre en person i at få en national PSC eller en EU-PSC med henblik på adgang til EUCI op til en nærmere bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere)

"systemspecifikke sikkerhedskrav" (SSRS): et bindende sæt sikkerhedsprincipper, der skal overholdes, og bestemte sikkerhedskrav, der skal gennemføres, og som danner grundlag for certificering og akkreditering af CIS'er

"særlige sikkerhedsbetingelser" (SAL): et sæt særlige kontraktlige betingelser udstedt af den kontraherende myndighed, som er en integrerende del af en klassificeret kontrakt, der indebærer adgang til eller udarbejdelse af EUCI, og som fastlægger sikkerhedskravene eller de elementer i kontrakten, der kræver sikkerhedsbeskyttelse, jf. bilag A V, afsnit II

"sårbarhed": svaghed af enhver art, som kan udnyttes af en eller flere trusler. Sårbarhed kan være en forsømmelse eller vedrøre en svaghed i kontrolforanstaltninger med hensyn til effektivitet, omfang eller sammenhæng og være af teknisk, proceduremæssig, fysisk, organisatorisk eller operativ karakter.

"Tempest": efterforskning, undersøgelse og kontrol af kompromitterende elektromagnetiske emissioner og foranstaltninger til at fjerne dem

"trussel": en potentiel årsag til en uønsket hændelse, der kan føre til skade på en organisation eller de systemer, den anvender. Sådanne trusler kan være uagtsomme eller forsætlige (ondsindede) og karakteriseres ved trusselselementer, potentielle mål og angrebsmetoder

"udsteder": en EU-institution eller et EU-agentur eller -organ, en medlemsstat, et tredjeland eller en international organisation, under hvis myndighed klassificerede informationer er blevet udarbejdet og/eller bragt ind i EU's strukturer.