Udskriftsdato: 5. april 2026 (Gældende)

Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt

Ministerium: Justitsministeriet

Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt

Forpligtelse til at sikkerhedsbeskytte klassificerede informationer består i forhold til Den Nordatlantiske Traktats Organisation (NATO) og Den Europæiske Union (EU) samt i forhold til andre internationale traktater og national lovgivning.

I henhold til aftaler indgået mellem Danmark og internationale organisationer er Danmark forpligtet til

– at overholde disse organisationers regelsæt for sikkerhedsbeskyttelse af fælles, klassificerede informationer,
– at udpege en national sikkerhedsmyndighed, der er pålagt at udøve den til regelsættene hørende kontrolfunktion i Danmark på disse organisationers vegne.

Den nationale sikkerhedsmyndighed har desuden en generel koordinerende funktion, bl.a. i forbindelse med indgåelse af internationale aftaler og fastsættelse af national lovgivning om sikkerhedsbeskyttelse af følsomme informationer.

Politiets Efterretningstjeneste er national sikkerhedsmyndighed. Forsvarets Efterretningstjeneste varetager funktionen som national sikkerhedsmyndighed inden for Forsvarsministeriets område.

Forsvarets Efterretningstjeneste er national it-sikkerhedsmyndighed. Politiets Efterretningstjeneste varetager funktionen som national it-sikkerhedsmyndighed inden for Justitsministeriets område.

Sikkerhedsbeskyttelsesreglerne er gældende uanset informationens form og det medium, hvori den tilvejebringes, nedfældes, transporteres, kommunikeres, arkiveres eller lagres.

Beskyttelsen af informationer udgøres af en række personelmæssige, fysiske og proceduremæssige foranstaltninger, der tilsigter, at informationerne beskyttes mod uautoriseret indsigt og ændring samt er til rådighed for autoriserede brugere, når de skal anvendes.

Omfanget af anvendte sikkerhedsforanstaltninger fastsættes ud fra cirkulærets klassificeringssystem.

Informationer skal i øvrigt behandles i overensstemmelse med Danmarks internationale forpligtelser på området.

A. Informationer af fælles interesse for landene i NATO eller EU m.v.

I. Klassificering

§ 1. Alle informationer mærket med betegnelsen NATO eller EU samt nationale informationer af fælles interesse for landene i NATO eller EU skal, i det omfang de kræver sikkerhedsbeskyttelse, klassificeres efter nedenstående regler.

1) YDERST HEMMELIGT (»COSMIC TOP SECRET«, »TRÈS SECRET UE« / »EU TOP SECRET«)
   Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU overordentlig alvorlig skade.
2) HEMMELIGT (»NATO SECRET«, »SECRET UE« / »EU SECRET«)
   Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU alvorlig skade.
3) FORTROLIGT (»NATO CONFIDENTIAL«, »CONFIDENTIEL UE« / »EU CONFIDENTIAL«)
   Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU skade.
4) TIL TJENESTEBRUG (»NATO RESTRICTED«, »RESTREINT UE« / »EU RESTRICTED«)

Denne klassifikationsgrad anvendes om informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab.

Stk. 2. Andre landes NATO- eller EU-klassifikationsmærkninger skal uden videre sidestilles med den tilsvarende klassifikationsmærkning i stk. 1. Nationale klassifikationsmærkninger og internationale organisationers klassifikationsmærkninger skal i videst muligt omfang sidestilles med den tilsvarende klassifikationsmærkning i stk. 1.

Stk. 3. Forsvarets Efterretningstjeneste offentliggør på sin hjemmeside en liste over andre landes og internationale organisationers klassifikationsgrader.

§ 2. Klassifikationsgraden bestemmes under hensyntagen både til informationernes indhold og til den kilde, hvorfra de hidrører. Bedømmelsen af, hvilken klassifikationsgrad informationens indhold nødvendiggør, foretages uafhængigt af klassifikationen af de delinformationer, som slutproduktet måtte være udfærdiget på grundlag af. Slutproduktet må ikke klassificeres lavere end de højest klassificerede delinformationer.

§ 3. Dele af informationer i et dokument kan kræve individuel klassifikation (delklassifikation). En individuel klassifikation skal fremgå tydeligt.

§ 4. Ved klassifikation af informationer anvendes den laveste klassifikationsgrad, der er forenelig med de sikkerhedsmæssige krav.

Stk. 2. En information, der indeholder underbilag eller lignende, må ikke klassificeres lavere end de højest klassificerede underbilag. Aktpakker (charteques) skal mindst klassificeres til samme grad som den højest klassificerede information i aktpakken (charteque'et).

§ 5. Et følgebrev klassificeres mindst lige så højt som den højest klassificerede vedlagte information. Et følgebrev bør bære en påtegning om, at det nedklassificeres eller afklassificeres, når den eller de klassificerede vedlagte informationer fjernes.

§ 6. Ansvaret for, at informationer, som kræver sikkerhedsbeskyttelse, klassificeres som beskrevet i § 1, påhviler udstederen.

§ 7. Udstederen kan ved påtegning på informationen eller ved instruks bestemme, at informationen efter et nærmere angivet tidspunkt skal nedklassificeres eller afklassificeres.

Stk. 2. Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede. Nedklassifikation og afklassifikation meddeles til dem, der har modtaget informationerne.

Stk. 3. I forbindelse med ned- og afklassificering af klassificerede informationer, foretages overstregning af den oprindelige klassifikationsafmærkning, og eventuel ny klassifikation påføres.

§ 8. Modtageren af klassificerede informationer må ikke

1) nedklassificere eller afklassificere informationerne uden udstederens forudgående skriftlige samtykke,
2) anvende informationerne til andre formål end dem, der eventuelt er fastsat af udstederen,
3) videregive informationer, der er mærket med betegnelsen EU, samt nationale informationer af fælles interesse for landene i EU til et land uden for EU eller til en anden international organisation uden forudgående skriftligt samtykke fra udstederen og en passende aftale med det pågældende land eller den pågældende organisation om beskyttelse af de klassificerede informationer, eller
4) videregive informationer, der er mærket med betegnelsen NATO, samt nationale informationer af fælles interesse for landene i NATO til et land uden for NATO eller til en anden international organisation uden forudgående skriftligt samtykke fra udstederen og en passende aftale med det pågældende land eller den pågældende organisation om beskyttelse af de klassificerede informationer.

Stk. 2. Er informationerne åbenbart for lavt klassificerede af udstederen, kan modtageren klassificere dem til en højere grad. Udstederen skal da straks underrettes om opklassificeringen.

§ 9. Digitale lagermedier skal klassificeres og beskyttes efter de indeholdte informationers klassifikationsgrad. Sådanne medier skal derfor mærkes med den højest forekommende klassifikation af den information, som er eller har været lagret på mediet. Udskrifter af klassificeret information på sådanne medier skal behandles som klassificerede informationer i dokumentform. Der skal herunder tages hensyn til, at større mængder information med en given klassifikation samlet kan nødvendiggøre en højere klassifikation.

Stk. 2. Digitale lagermedier, der indeholder informationer klassificeret FORTROLIGT eller højere, skal registreres med oplysning om mediets unikke identifikationsnummer. Den nationale it-sikkerhedsmyndighed kan dog i sikkerhedsgodkendelsen fravige kravet om registrering.

§ 10. Software og dokumentation, der specifikt retter sig mod sikkerhedsforhold, skal, efter at være taget i brug, have mindst samme klassifikation og beskyttes i overensstemmelse med den information, der behandles, herunder frembringes, kommunikeres eller lagres i det pågældende system.

§ 11. Klassificerede digitale lagermedier må ikke nedklassificeres og skal destrueres i overensstemmelse med godkendte procedurer, uanset om de klassificerede informationer måtte være slettet.

II. Indsigt i klassificerede informationer

§ 12. Klassificerede informationer må ikke gøres tilgængelige for personer, der ikke er sikkerhedsgodkendt til at behandle informationer af den pågældende klassifikationsgrad.

§ 13. Enhver offentlig myndighed træffer afgørelse om sikkerhedsgodkendelse af ansatte i myndigheden og ansatte i private firmaer, der arbejder for den offentlige myndighed. Sikkerhedsgodkendelsen har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende myndighed.

Stk. 2. En sikkerhedsgodkendelse til at behandle informationer af klassifikationsgraden YDERST HEMMELIGT er gyldig i højst 5 år fra afgørelsestidspunktet. En sikkerhedsgodkendelse til at behandle informationer af klassifikationsgraden HEMMELIGT og FORTROLIGT er gyldig i højst 10 år fra afgørelsestidspunktet.

Stk. 3. Politiets Efterretningstjeneste foretager en sikkerhedsundersøgelse til brug for den offentlige myndigheds afgørelse om sikkerhedsgodkendelse af ansatte.

§ 14. Afgørelsen om sikkerhedsgodkendelse træffes på grundlag af en konkret vurdering af alle de oplysninger, der foreligger om personen. Der lægges herved navnlig vægt på, om den pågældende

1) har udvist ubestridt loyalitet og
2) har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer.

Stk. 2. Oplysninger om en ægtefælles, samlevers, registreret partners eller samboendes adfærd, karakter og forhold i øvrigt kan tilsvarende tillægges vægt ved afgørelsen om sikkerhedsgodkendelse.

§ 15. Sikkerhedsgodkendelse må kun gives til personer, når det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage.

Stk. 2. Der skal foreligge en ajourført liste over de medarbejdere, der er sikkerhedsgodkendt hos den offentlige myndighed (f.eks. hos sikkerhedsofficeren, jf. § 54). Listen skal indeholde oplysninger om klassifikationsgrad, som den pågældende er godkendt til, samt sikkerhedsgodkendelsens udstedelsesdato og gyldighedsperiode.

§ 16. Indsigt i klassificerede informationer må kun gives personer, for hvem sådan indsigt er tjenstligt nødvendig (»Need to Know«).

Stk. 2. Ingen må gøre sig bekendt med klassificerede informationer, når det ikke er tjenstligt nødvendigt (»Need to Know«).

Stk. 3. Enhver, som har klassificerede informationer til gennemsyn eller behandling, har pligt til at udvise den største omhu for at sikre, at uvedkommende ikke bliver bekendt med informationernes indhold.

§ 17. I forbindelse med sikkerhedsgodkendelse skal den pågældende gøres bekendt med dette cirkulære og straffelovens kapitel 12, 13 og 16.

Stk. 2. Alle personer, der sikkerhedsgodkendes, skal endvidere gøres bekendt med indholdet af henholdsvis NATO´s sikkerhedsforskrifter eller EU´s sikkerhedsforskrifter i det omfang, sikkerhedsgodkendelsen omfatter informationer beskyttet heraf.

III. Behandling af klassificerede informationer

§ 18. Behandling af klassificerede informationer må kun betros personer, der er godkendt af vedkommende offentlige myndighed til at behandle informationer af den pågældende klassifikationsgrad.

§ 19. En klassificeret information skal foreligge i et så begrænset antal som muligt.

§ 20. Klassifikationsgraden påføres ved klassificerede informationer i dokumentform som tydelig mærkning på dokumentets første side samt foroven og forneden på hvert af dokumentets øvrige ark, jf. vedlagte bilag.

Stk. 2. Består dokumentet af flere ark, skal arkene være forsvarligt sammenhæftede, og siderne skal nummereres.

Stk. 3. Dokumenter klassificeret YDERST HEMMELIGT eller HEMMELIGT skal på første side være forsynet med angivelse af sideantallet. Hvis dokumentet fremstilles i mere end et eksemplar, skal hvert eksemplar nummereres.

§ 21. Behandling, herunder afskrift, udskrivning, kopiering, oversættelse eller anden gengivelse, formidling eller videregivelse, af klassificerede informationer må kun foretages i det omfang, det er tjenstligt nødvendigt, jf. dog stk. 2.

Stk. 2. Informationer klassificeret YDERST HEMMELIGT må i almindelighed hverken helt eller delvist gengives af modtageren uden forud indhentet bemyndigelse fra udstederen. Hvis modtageren ikke uden væsentlig ulempe kan afvente udstederens bemyndigelse, og det anses for absolut påkrævet at gengive informationerne yderligere, må dette i hvert enkelt tilfælde kun ske efter bemyndigelse af vedkommende chef i den offentlige myndighed. Gengivelsen skal

1) udfærdiges af personer, der er godkendt til at behandle informationer klassificeret YDERST HEMMELIGT,
2) være forsynet med originalinformationens journal- og eksemplarnummer tillige med angivelse af udstederen,
3) være forsynet med et særligt eksemplarnummer, som den, der udfærdiger gengivelsen, påfører dokumentet, og
4) indberettes til udstederen, der skal underrettes om det udfærdigede antal af gengivelser.

Stk. 3. Foreligger gengivelsen af informationerne i dokumentform, skal den endvidere være forsynet med påtegningen YDERST HEMMELIGT, jf. § 20.

§ 22. Kladder, notater og informationsbærende medier, f.eks. digitale lagermedier, der danner grundlaget for udfærdigelsen af klassificerede informationer, skal efter brugen behandles på samme måde som de klassificerede informationer.

§ 23. Mundtlig eller anden auditiv gengivelse af klassificerede informationer må ikke finde sted under sådanne forhold, at gengivelsen kan aflyttes.

§ 24. Inden for den enkelte offentlige myndigheds lokaliteter skal klassificerede informationer overdrages fra hånd til hånd mellem personer, der er sikkerhedsgodkendt til at behandle informationer af den pågældende klassifikationsgrad, befordres i lukket emballage af et dertil særligt udpeget bud eller overdrages på anden betryggende måde. Såfremt informationerne ikke befordres i lukket emballage, skal de bæres således, at deres indhold er utilgængeligt for uvedkommende.

§ 25. Klassificerede informationer skal i almindelighed journaliseres straks ved modtagelsen.

Stk. 2. Journaler, der indeholder klassificerede informationer, skal behandles på samme måde som de i journalen indførte højest klassificerede informationer.

IV. Sikkerhedsgodkendelse af elektroniske informationssystemer

§ 26. Elektronisk behandling af informationer klassificeret YDERST HEMMELIGT kræver i hvert enkelt tilfælde en særskilt tilladelse fra den nationale it-sikkerhedsmyndighed.

§ 27. Alle former for elektroniske informationssystemer beregnet til behandling af informationer klassificeret HEMMELIGT eller FORTROLIGT skal sikkerhedsgodkendes af den nationale it-sikkerhedsmyndighed.

Stk. 2. Den enkelte offentlige myndighed skal føre en oversigt over de elektroniske informationssystemer, som er beregnet til behandling af informationer klassificeret TIL TJENESTEBRUG.

§ 28. Nye versioner af software til anvendelse i sikkerhedsgodkendte elektroniske informationssystemer skal sikkerhedsgodkendes af den nationale it-sikkerhedsmyndighed før ibrugtagning.

§ 29. Kryptografiske metoder til beskyttelse af informationer klassificeret til TIL TJENESTEBRUG eller højere, der transmitteres via offentlige telenet eller øvrige net, som den offentlige myndighed ikke ejer, skal godkendes af den nationale it-sikkerhedsmyndighed.

§ 30. Sikkerhedsgodkendelse efter §§ 27-29 skal sikre, at det elektroniske informationssystem opfylder gældende sikkerhedskrav inden ibrugtagning. Den nationale it-sikkerhedsmyndighed bør derfor inddrages på det tidligst mulige tidspunkt i forbindelse med planlægning af anskaffelse af elektroniske informationssystemer, eller ved ændringer af tidligere godkendte elektroniske informationssystemer.

§ 31. Som led i sikkerhedsgodkendelsen påhviler det den enkelte offentlige myndighed at udarbejde systemspecifikke sikkerhedskrav og forskrifter for sikkerhedsforanstaltninger, jf. § 53, stk. 4, der skal godkendes af den nationale it-sikkerhedsmyndighed.

Stk. 2. Udarbejdelsen af systemspecifikke sikkerhedskrav skal påbegyndes på et så tidligt tidspunkt i projektet som muligt for derefter at blive revideret og uddybet i takt med projektets udvikling.

Stk. 3. Systemspecifikke sikkerhedskrav er en fuldstændig og nøjagtig beskrivelse af, hvilke sikkerhedsprincipper og sikkerhedskrav der skal opfyldes. Disse krav udgør en integreret del af systemdokumentationen.

V. Fysisk og elektronisk forsendelse m.v. af klassificerede informationer

§ 32. Ved fysisk forsendelse af informationer klassificeret FORTROLIGT eller højere skal informationerne anbringes i to emballager af materiale, der ikke kan gennemlyses.

Stk. 2. Den indre emballage forsynes med samme klassifikationspåtegning som informationerne i emballagen, og denne emballage forsegles.

Stk. 3. Klassifikationspåtegning må ikke påføres den yderste emballage. Den yderste emballage skal kun forsynes med et forsendelsesnummer med henblik på kvittering for modtagelsen.

§ 33. Fysisk forsendelse af informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT må kun ske ved kurer, der er sikkerhedsgodkendt til forsendelsens klassifikationsgrad.

Stk. 2. Forsendelse af informationer klassificeret FORTROLIGT bør kun ske ved kurer, der er godkendt til mindst forsendelsesklassifikationsgraden. Forsendelse ved andet bud kan dog ske, såfremt det efter en konkret vurdering i det enkelte tilfælde skønnes forsvarligt.

Stk. 3. I Danmark må informationer klassificeret FORTROLIGT tillige sendes med rekommanderet post. Sådan forsendelse til Grønland og Færøerne bør dog kun ske, hvis det efter en konkret vurdering i det enkelte tilfælde skønnes forsvarligt.

§ 34. Transmission af informationer klassificeret TIL TJENESTEBRUG eller højere må kun finde sted under anvendelse af en kryptografisk metode godkendt af den nationale it-sikkerhedsmyndighed, jf. § 29.

Stk. 2. Ved transmission af informationer klassificeret HEMMELIGT eller lavere kan kryptering under helt særlige omstændigheder og efter fornøden autorisation undlades, hvis meddelelsen er yderst hastende, hvor kryptering ikke er mulig, og informationen ellers ikke kan nå rettidigt frem. Helt særlige omstændigheder vil kunne foreligge ved overhængende eller helt aktuelle kriser, konflikter eller krigssituationer.

Stk. 3. Vejledning og bistand i forbindelse med anskaffelse og anvendelse af kryptografi kan indhentes hos Forsvarets Efterretningstjeneste.

§ 35. Forsendelser, der indeholder klassificerede informationer, må kun adresseres til og åbnes af personer, der er sikkerhedsgodkendt til den klassifikationsgrad, som den pågældende forsendelse indeholder.

§ 36. Ved fysisk forsendelse af informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT skal der altid på særskilt blanket kvitteres for informationens modtagelse. Ved andre klassifikationsgrader er kvittering kun nødvendig, hvis udstederen har stillet krav derom. Blanketten, der nedlægges i den indre emballage, underskrives straks af modtageren og tilbagesendes afsenderen. Kvitteringen, som ikke kræver nogen klassifikation, må kun indeholde oplysning om informationernes journal- og eksemplarnummer, men ikke om f.eks. titel. Modtager informationernes afsender ikke kvitteringen, eller modtages denne med forsinkelse, skal en undersøgelse af årsagen hertil straks iværksættes.

§ 37. Bude og kurerer skal i en særlig bog sikre sig kvittering for aflevering af forsendelser, der indeholder klassificerede informationer. I den forbindelse benyttes forsendelsesnummeret, der er anført på den ydre emballage.

§ 38. Forsendelse af digitale medier indeholdende klassificerede informationer, eller udstyr indeholdende sådanne medier, skal sidestilles med forsendelse af andre klassificerede informationer.

VI. Opbevaring, fysisk sikkerhed, installationssikkerhed og destruktion m.v.

§ 39. Kontorer og lokaler, hvor der opbevares klassificerede informationer og elektronisk informationsudstyr, herunder kabler og krydsfelter, skal være således sikret, at uvedkommende ikke kan skaffe sig adgang hertil.

Stk. 2. Kontorer og lokaler, hvor der er mulighed for indblik i klassificerede informationer, skal til stadighed være under opsyn af en medarbejder, der er sikkerhedsgodkendt til de pågældende informationer.

§ 40. Tilkobling af eksterne elektroniske informationssystemer til interne elektroniske informationssystemer, der indeholder klassificerede informationer, må kun finde sted efter godkendelse af den nationale it-sikkerhedsmyndighed.

§ 41. Udstyr, herunder kabler, krydsfelter, printere m.v., der behandler informationer klassificeret FORTROLIGT eller højere, skal være installeret på en sådan måde, at informationerne ikke kompromitteres

via direkte elektromagnetisk udstråling eller bortledning. Forsvarets Efterretningstjeneste kan vejlede de enkelte offentlige myndigheder vedrørende specifikke forholdsregler.

§ 42. Informationer klassificeret FORTROLIGT eller højere skal opbevares i opbevaringsmidler forsynet med låseanordninger og skal være placeret i lokaler med alarmovervågning. Alle sikkerhedsanordninger skal være godkendt af den nationale sikkerhedsmyndighed.

Stk. 2. Opbevaringsmidler, hvori der opbevares informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT, skal uden for særligt sikrede områder være forsynet med alarmsystemer af anerkendt fabrikat med sabotagesikret signaloverførsel til døgnbemandet alarmcentral.

Stk. 3. De foreskrevne låseanordninger og boksalarmanlæg skal regelmæssigt efterses.

§ 43. Nøgler til penge- eller stålskabe, hvori der opbevares klassificerede informationer, skal, når bygningen forlades, anbringes i et nøgleskab forsynet med sikker kombinationslås godkendt af den nationale sikkerhedsmyndighed. Nøgler må aldrig medbringes uden for bygningen.

Stk. 2. Tab af nøgle eller kompromittering af kode til penge- eller stålskabe, hvori der opbevares klassificerede informationer, skal straks meldes til den relevante chef eller sikkerhedsofficeren, jf. § 54, der træffer foranstaltning til, at låsen omkodes eller udskiftes.

§ 44. Klassificerede informationer, der medtages fra tjenestestedet, må ikke fremtages på offentlige steder og må ikke efterlades på ubeskyttede steder, herunder f.eks. i flyvemaskiner, togkupeer, motorkøretøjer, hotelværelser eller garderober.

Stk. 2. Når informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT medtages fra tjenestestedet, skal de under transporten opbevares i et opbevaringsmiddel, som er godkendt af den nationale sikkerhedsmyndighed.

Stk. 3. Forinden informationer klassificeret FORTROLIGT eller højere medtages fra tjenestestedet, skal der udfærdiges en fortegnelse i to eksemplarer over de medbragte informationer. Det ene eksemplar opbevares på tjenestestedet, og det andet eksemplar medtages til brug ved eventuel mønstring. For elektroniske dokumenters vedkommende kan en sikkerhedskopi, der opbevares og registreres på tjenestestedet, træde i stedet for fortegnelsen.

§ 45. Hvis klassificerede informationer bortkommer, eller der næres mistanke om, at uvedkommende kan have fået kendskab til indholdet, skal dette meldes til den relevante chef eller sikkerhedsofficeren, jf. § 54, der underretter den relevante chef og foranlediger, at der iværksættes en undersøgelse, at informationens udsteder underrettes, og at der træffes nødvendige forholdsregler for at begrænse følgerne af, at uvedkommende er blevet eller kan befrygtes at være blevet bekendt med informationernes indhold.

§ 46. Opstår der ved krigshandlinger eller under en kritisk situation af anden art fare for, at klassificerede informationer kan komme uvedkommende i hænde, skal den, der er ansvarlig for informationerne, straks iværksætte foranstaltninger for at få dem bragt i sikkerhed eller - hvis dette ikke er muligt - tilintetgjort.

Stk. 2. Den enkelte offentlige myndighed udarbejder en kriseplan med henblik på sikring eller tilintetgørelse som nævnt i stk. 1.

§ 47. Med henblik på at undgå unødig ophobning bør klassificerede informationer destrueres, så snart de er sat ud af kraft eller i øvrigt må anses for overflødige, medmindre andet følger af lov eller bestemmelser fastsat i medfør af lov.

Stk. 2. Sikkerhedsofficeren, jf. § 54, foranstalter destruktionen.

Stk. 3. Destruktionen foretages under kontrol ved brænding, formaling, makulering eller på anden måde, der sikrer mod rekonstruktion og er godkendt af den nationale sikkerhedsmyndighed eller den nationale it-sikkerhedsmyndighed.

Stk. 4. Ved destruktion af informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT udfærdiges en attest, der underskrives af to personer, som har overværet destruktionen. I attesten skal der angives journalnummer, informationens betegnelse, eksemplarnumre og destruktionsmetoden.

§ 48. Ligeledes med henblik på at undgå unødig ophobning kan klassificerede informationer mikrofotograferes, hvorefter originaludgaven af informationen tilintetgøres i overensstemmelse med bestemmelsen i § 47. Mikrofotografering må kun foretages af personer, der er sikkerhedsgodkendt til den pågældende klassifikationsgrad, og mikrofilmene skal gives samme sikkerhedsmæssige beskyttelse som originalinformationen.

VII. Områdesikkerhedsgodkendelse

§ 49. Den nationale sikkerhedsmyndighed kan i samråd med den nationale it-sikkerhedsmyndighed træffe afgørelse om at tildele en områdesikkerhedsgodkendelse (Facility Security Clearance) i overensstemmelse med regler herom i NATO og EU.

VIII. Mobilt elektronisk informationsudstyr

§ 50. Mobilt elektronisk informationsudstyr, hvori der behandles klassificeret information, skal opfylde tilsvarende krav, som gælder for mærkning, registrering, opbevaring og transport af klassificerede dokumenter.

IX. Privatejet, leaset, lånt eller lejet elektronisk informationsudstyr

§ 51. Privatejet, leaset, lånt eller lejet elektronisk informationsudstyr må ikke benyttes til behandling, herunder frembringelse, kommunikation eller lagring, af klassificeret information, jf. dog § 49.

X. Virus

§ 52. Alle udefra kommende lagermedier skal kontrolleres for virus inden indlæsning af data m.v.

Stk. 2. Viruskontrollen skal udføres med et antivirusprogram, der til stadighed holdes opdateret.

Stk. 3. Hvis der under brugen af arbejdspladsen opstår unormale forhold, skal den sikkerhedsansvarlige straks underrettes.

XI. Udførelse og tilsyn

§ 53. De enkelte offentlige myndigheder skal på ledelsesniveau udstede forskrifter, som beskriver de nødvendige sikkerhedsforanstaltninger, der skal træffes med henblik på, at bestemmelserne i dette cirkulære overholdes.

Stk. 2. Hvor det i de enkelte offentlige myndigheder ud fra en risikovurdering må anses for nødvendigt, at der gennemføres yderligere sikkerhedsforanstaltninger, udarbejder vedkommende offentlige myndighed forskrifter herfor i samråd med den nationale sikkerhedsmyndighed.

Stk. 3. Hvor de i stk. 2 nævnte sikkerhedsforanstaltninger vedrører elektroniske informationssystemer, udarbejder vedkommende offentlige myndighed forskrifter herfor i samråd med den nationale it-sikkerhedsmyndighed.

Stk. 4. Forskrifter for sikkerhedsforanstaltninger vedrørende elektroniske informationssystemer skal som minimum beskrive

1) sikkerhedsorganisationen, herunder roller og ansvarsområder for arbejdet med informationssikkerhed,
2) myndighedens elektroniske informationssystemer, herunder driftsforhold og teknologier,
3) de it-sikkerhedsprocesser, der skal følges for at opretholde et acceptabelt risikoniveau, og
4) procedurer for håndtering af it-sikkerhedshændelser.

Stk. 5. Relevante dele af forskrifter for sikkerhedsforanstaltninger skal være tilgængelige for medarbejderne i de enkelte offentlige myndigheder.

§ 54. De enkelte offentlige myndigheder skal udpege én eller flere medarbejdere som sikkerhedsofficer og it-sikkerhedsofficer til at bistå ved gennemførelsen af bestemmelserne og den fortsatte kontrol med, at bestemmelserne overholdes. De enkelte offentlige myndigheders medarbejdere kan rette henvendelse om sikkerhedsanliggender direkte til den relevante sikkerhedsofficer.

§ 55. Den nationale sikkerhedsmyndighed yder rådgivning ved gennemførelsen af bestemmelserne i dette cirkulære og af forskrifter, der er udarbejdet af de enkelte offentlige myndigheder efter § 53, stk. 2.

Stk. 2. Den nationale it-sikkerhedsmyndighed yder rådgivning ved gennemførelsen af bestemmelserne i dette cirkulære og af forskrifter, der er udarbejdet af de enkelte offentlige myndigheder efter § 53, stk. 3.

§ 56. Den nationale sikkerhedsmyndighed og den nationale it-sikkerhedsmyndighed fører tilsyn med overholdelsen af de sikkerhedsmæssige foranstaltninger, som Danmark er forpligtet til at gennemføre, og foretager periodiske inspektioner, eventuelt bistået af eksperter fra NATO eller EU.

B. Andre informationer af sikkerhedsmæssig betydning

§ 57. Enhver offentlig myndighed kan bestemme, at reglerne i kapitel A inden for rammerne af gældende lovgivning skal finde anvendelse på andre informationer af sikkerhedsmæssig betydning, som behandles af den pågældende myndighed.

Stk. 2. Vejledning og bistand om sikkerhedsbeskyttelse af sådanne informationer kan indhentes hos den nationale sikkerhedsmyndighed. It-sikkerhedsmæssig vejledning og bistand om sikkerhedsbeskyttelse af sådanne informationer kan indhentes hos den nationale it-sikkerhedsmyndighed.

Stk. 3. Efter aftale med vedkommende myndighed kan den nationale sikkerhedsmyndighed eller den nationale it-sikkerhedsmyndighed ligeledes yde vejledning og bistand til private eller andre, der modtager sådanne informationer fra myndigheden.

§ 58. I tilfælde, hvor det efter § 57, stk. 1, er bestemt, at kapitel A finder anvendelse, kan den nationale it-sikkerhedsmyndighed ved sikkerhedsgodkendelse efter §§ 27-29 af mobilt elektronisk informationsudstyr efter en konkret vurdering, og uanset § 50, fravige de krav, der stilles til elektroniske informationssystemer, for så vidt angår behandlingen i det pågældende udstyr af klassificerede informationer, der sidestilles med informationer klassificeret FORTROLIGT, jf. § 1, stk. 1, nr. 3, eller lavere.

Stk. 2. Den nationale it-sikkerhedsmyndighed kan i forbindelse med en sikkerhedsgodkendelse efter stk. 1 fastsætte nærmere angivne vilkår for godkendelsen, herunder vilkår om de informationer, der behandles på det pågældende mobile elektroniske informationsudstyr, f.eks. om informationernes karakter, formål, anvendelse, mærkning, registrering, opbevaring, transport m.v.

Stk. 3. Tilkobling af eksterne elektroniske informationssystemer til mobilt elektronisk informationsudstyr, som er sikkerhedsgodkendt efter stk. 1, og som indeholder klassificerede informationer, må kun finde sted efter godkendelse af den nationale it-sikkerhedsmyndighed, jf. § 40.

Stk. 4. Informationer mærket med betegnelsen NATO eller EU samt nationale informationer af fælles interesse for landene i NATO eller EU må ikke behandles i det efter stk. 1 godkendte mobile elektroniske informationsudstyr.

C. Ikrafttræden m.v.

§ 59. Cirkulæret træder i kraft den 1. januar 2015.

Stk. 2. En sikkerhedsgodkendelse til at behandle informationer klassificeret YDERST HEMMELIGT, der er udstedt senest den 1. januar 2011, bevarer uanset § 13, stk. 2, 1. pkt., sin gyldighed, indtil der på baggrund af en fornyet vurdering er truffet ny afgørelse om sikkerhedsgodkendelse, dog senest til den 1. januar 2020.

Stk. 3. En sikkerhedsgodkendelse til at behandle informationer klassificeret HEMMELIGT eller FORTROLIGT, der er udstedt senest den 1. januar 2006, bevarer uanset § 13, stk. 2, 2. pkt., sin gyldighed, indtil der på baggrund af en fornyet vurdering er truffet ny afgørelse om sikkerhedsgodkendelse, dog senest til den 1. januar 2025.

Stk. 4. En sikkerhedsgodkendelse, der kun i medfør af stk. 2 eller 3 bevarer sin gyldighed, skal optages til fornyet vurdering hurtigst muligt.

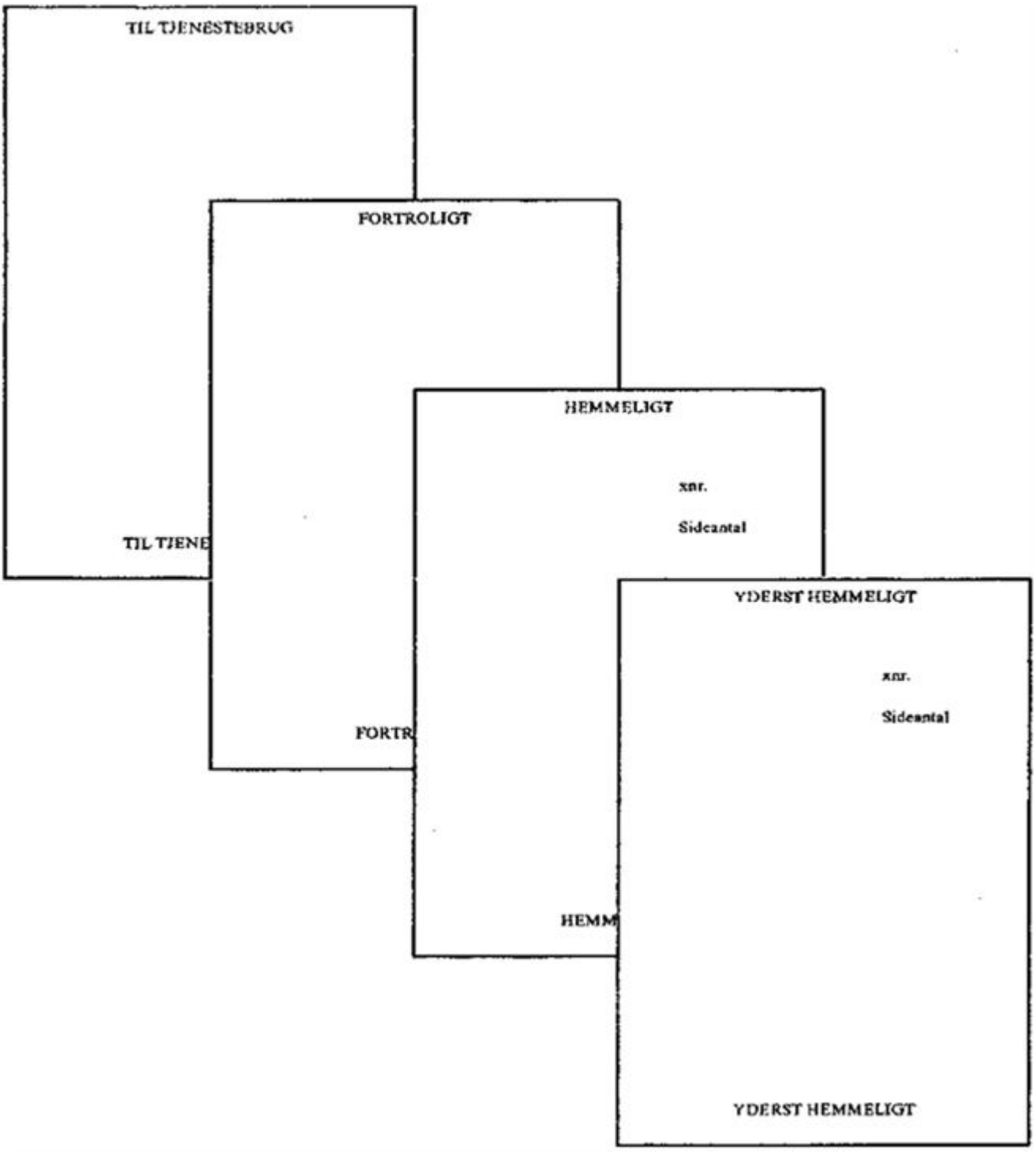
Stk. 5. Cirkulære af 21. december 2013 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO og EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt ophæves.

Statsministeriet, den 17. december 2014

HELLE THORNING-SCHMIDT

/ Jens Teilberg Søndergaard

Bilag 1


TIL TJENESTEBRUG
FORTROLIGT
HEMMELIGT
xxx.
Sideantal
YDERST HEMMELIGT
xxx.
Sideantal
YDERST HEMMELIGT