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: Statsministeriet

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 udtrykkes i et klassificeringssystem.

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

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

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

§ 3. 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.

§ 4. Enkelte dele af informationerne kan kræve individuel klassifikation (delklassifikation). For så vidt angår mødereferater bør det særligt overvejes, om det er muligt at klassificere de enkelte punkter individuelt med henblik på en lettere adgang til at rundsende ekstraktafskrifter af mødereferater til en videre kreds. Eventuel individuel klassifikation skal fremgå tydeligt.

§ 5. 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).

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

§ 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.

§ 8. Modtageren af klassificerede informationer må ikke uden udstederens samtykke nedklassificere eller afklassificere disse.

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. Magnetiske og optiske 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 det forhold, at større mængder information med en given klassifikation samlet kan nødvendiggøre en højere klassifikation.

Stk. 2. Magnetiske og optiske lagermedier, der indeholder informationer klassificeret FORTROLIGT eller højere, skal registreres efter samme regler som tilsvarende dokumenter.

§ 10. Systemprogrammel, applikations-programmer 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 frembringes, behandles, kommunikeres eller lagres i det pågældende system.

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

II. Indsigt i klassificerede informationer

§ 12. Klassificerede informationer må ikke udlånes eller udleveres til personer, der ikke er sikkerhedsgodkendt til at behandle informationer af den pågældende klassifikationsgrad.

Stk. 2. Alle personer med adgang til elektroniske informationssystemer, der behandler informationer klassificeret FORTROLIGT eller højere, skal være sikkerhedsgodkendt til at behandle de højest klassificerede informationer, som de har adgang til i det elektroniske system.

§ 13. Styrelseschefen træffer afgørelse om sikkerhedsgodkendelse af ansatte i styrelsen og ansatte i private firmaer, der arbejder for styrelsen. Styrelseschefens meddelelse af sikkerhedsgodkendelse har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende styrelse.

Stk. 2. Politiets Efterretningstjeneste foretager en sikkerhedsundersøgelse til brug for styrelseschefens 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 eller samlevers adfærd og karakter kan tilsvarende tillægges vægt ved afgørelsen om sikkerhedsgodkendelse.

§ 15. Antallet af personer, der sikkerhedsgodkendes til klassifikationsgraderne YDERST HEMMELIGT eller HEMMELIGT, skal begrænses mest muligt.

Stk. 2. Hos styrelseschefen eller sikkerhedsofficeren, jf. § 54, skal der bero en ajourført liste over de medarbejdere, der er sikkerhedsgodkendt til klassifikationsgraderne YDERST HEMMELIGT eller HEMMELIGT.

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

Stk. 2. Ingen må gøre sig bekendt med klassificerede informationer, der ikke er forelagt den pågældende til gennemsyn eller behandling i forbindelse med tjenesten.

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 til klassifikationsgraden YDERST HEMMELIGT, skal endvidere gøres bekendt med indholdet af henholdsvis NATO´s sikkerhedsforskrifter eller EU´s sikkerhedsforskrifter i det omfang, sikkerhedsgodkendelsen omfatter informationer beskyttet heraf.

III. Udfærdigelse af klassificerede informationer

§ 18. Udarbejdelse m.v. af klassificerede informationer må kun betros personer, der er godkendt af vedkommende styrelseschef 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. Ved klassifikationsgraderne YDERST HEMMELIGT og HEMMELIGT kan benyttes rød skrift, og ved klassifikationsgraderne FORTROLIGT og TIL TJENESTEBRUG kan benyttes blå skrift.

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. Afskrift, udskrivning, kopiering, oversættelse eller anden gengivelse 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 styrelseschef. 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, koncepter, stenogrammer, notater og maskinlæsbare informationsbærende medier, fx magnetbånd, disketter m.v., der danner grundlaget for udfærdigelsen af klassificerede informationer, samt carbonpapir skal efter brugen enten straks effektivt tilintetgøres eller opbevares og behandles på samme måde som de klassificerede informationer. Det samme gælder farvebånd og trækpapir, såfremt der heraf kan udledes oplysninger om informationernes indhold.

§ 23. Diktat af informationer, der kræver sikkerhedsbeskyttelse, og samtale om deres indhold må ikke finde sted under sådanne forhold, at diktatet eller samtalen kan aflyttes.

§ 24. Klassificerede informationer skal i almindelighed journaliseres straks ved modtagelsen. Journalisering og aktering må kun foretages af personer, der er særligt godkendt dertil.

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

IV. Sikkerhedsgodkendelse af elektroniske informationssystemer

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

§ 26. Alle former for elektroniske informationssystemer og netværk beregnet til frembringelse, bearbejdning, kommunikation eller lagring af informationer klassificeret HEMMELIGT eller FORTROLIGT skal sikkerhedsgodkendes af den nationale it-sikkerhedsmyndighed.

§ 27. Nye versioner af programmel til anvendelse i sikkerhedsgodkendte informationssystemer skal sikkerhedsgodkendes af den nationale it-sikkerhedsmyndighed før ibrugtagning.

§ 28. Kommunikationssystemer (f.eks. telefax, videokonference, og telefon/modem) beregnet til informationer klassificeret TIL TJENESTEBRUG eller højere skal sikkerhedsgodkendes af den nationale it-sikkerhedsmyndighed.

§ 29. Sikkerhedsgodkendelse efter §§ 26-28 skal sikre, at informationssystemet, netværket m.v. 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 netværk, eller ved ændringer af tidligere godkendte elektroniske informationssystemer eller netværk.

§ 30. Som led i sikkerhedsgodkendelsen påhviler det de enkelte styrelser at udarbejde systemspecifikke sikkerhedskrav og en sikkerhedsinstruks, der 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. Forsendelse m.v.

§ 31. Inden for samme bygning kan klassificerede informationer kun overdrages fra hånd til hånd mellem personer, der er sikkerhedsgodkendt til at behandle informationer af den pågældende klassifikationsgrad, eller befordres i lukket kuvert af et dertil særligt udpeget bud. Såfremt informationerne ikke befordres i lukket kuvert, skal de bæres således, at deres indhold er utilgængeligt for uvedkommende.

§ 32. Ved forsendelse af informationer klassificeret FORTROLIGT eller højere skal informationerne anbringes i to kuverter af svært papir.

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

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

§ 33. 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 denne klassifikationsgrad. 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. Forsendelse, drøftelse m.v. via kommunikationssystemer af informationer klassificeret TIL TJENESTEBRUG eller højere må kun finde sted under anvendelse af kryptoudstyr godkendt til den pågældende kommunikation.

Stk. 2. Ved kommunikation af informationer klassificeret HEMMELIGT eller lavere kan kryptering under helt særlige omstændigheder og efter fornøden autorisation undlades, hvis meddelelsen er yderst hastende, kryptoudstyr ikke er tilgængeligt 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 kryptosystemer 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 forsendelse af informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT skal der altid på særskilt blanket kvitteres for informationens modtagelse. Ved andre klassifikationsgrader er sådan kvittering kun nødvendig, hvis udstederen har stillet krav derom. Den særlige blanket, der nedlægges i den indre kuvert, 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 kuvert.

§ 38. Forsendelse af magnetiske og optiske 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 netværk, herunder Internet, til interne netværk (med modem, telefax eller lignende) må ikke finde sted, medmindre der foreligger en installation, der er godkendt 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 styrelser vedrørende specifikke forholdsregler.

§ 42. Informationer klassificeret FORTROLIGT eller højere skal opbevares i penge- eller stålskabe med særligt sikre låsesystemer, der er godkendt af den nationale sikkerhedsmyndighed.

Stk. 2. Penge- og stålskabe, hvori der opbevares informationer klassificeret YDERST HEMMELIGT eller HEMMELIGT, skal uden for særligt sikrede områder være forsynet med boksalarmanlæg 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 styrelseschefen 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 transporteres i en metaltransportkassette forsynet med sikkert låsesystem 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.

§ 45. Hvis klassificerede informationer bortkommer, eller der næres mistanke om, at uvedkommende kan have fået kendskab til indholdet, skal dette meldes til styrelseschefen eller sikkerhedsofficeren, jf. § 54, der underretter styrelseschefen 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 styrelse 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.

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

Stk. 3. Destruktionen foretages under kontrol ved brænding, formaling, strimmelskæring 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 tilintetgørelsesmetoden.

§ 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. Bærbart edb-udstyr

§ 49. Bærbart edb-udstyr (laptops, elektroniske notesbøger m.v.) med fast lagermedie (eksempelvis harddisk), hvorpå der opbevares klassificeret information, skal opfylde tilsvarende krav, som gælder for mærkning, registrering, opbevaring og transport af klassificerede dokumenter.

VIII. Privatejet, leaset, lånt eller lejet elektronisk informationsudstyr

§ 50. Privatejet, leaset, lånt eller lejet elektronisk informationsudstyr må ikke benyttes til frembringelse, behandling, kommunikation eller lagring af klassificeret information.

IX. Edb-virus

§ 51. 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.

X. Udførelse og tilsyn

§ 52. De enkelte styrelser skal udarbejde supplerende forskrifter som vejledning til cirkulæret.

Stk. 2. Hvis det i de enkelte styrelser må anses for nødvendigt, at der gennemføres yderligere sikkerhedsforanstaltninger (f.eks. sikring af kontorer, oprettelse af alarmanlæg eller lignende), udarbejder vedkommende styrelse detailplaner herom i samråd med den nationale sikkerhedsmyndighed.

Stk. 3. Hvis de i stk. 2 nævnte sikkerhedsforanstaltninger består i it-sikkerhedsmæssige tiltag vedrørende elektroniske informationssystemer, udarbejder vedkommende styrelse detailplaner herom i samråd med den nationale it-sikkerhedsmyndighed.

Stk. 4. Sikkerhedsinstruksen for elektroniske informationssystemer, jf. § 30, stk. 1, skal bl.a. beskrive

1) den fysiske sikkerhed omkring klassificerede elektroniske informationssystemer,
2) beskrivelse af den lokale sikkerhedsorganisation,
3) brug af kendeord,
4) nødprocedurer,
5) forholdene omkring installationsændringer og
6) personelsikkerhed.

Stk. 5. Derudover kan sikkerhedsinstruksen eventuelt beskrive

1) antivirus strategi og
2) backup procedure.

Stk. 6. Relevante dele af sikkerhedsinstruksen bør ligge ved den enkelte arbejdsplads.

§ 53. Styrelsen skal etablere kontrol med integriteten af sikkerhedskopier af hele systempakken og sikre, at de opbevares og beskyttes efter samme retningslinjer som de klassificerede informationer, systemet behandler.

§ 54. Vedkommende styrelseschef skal træffe de nødvendige foranstaltninger til sikring af, at bestemmelserne i dette cirkulære overholdes. Styrelseschefen skal udpege en medarbejder (sikkerhedsofficer) til at bistå ved gennemførelsen af bestemmelserne og den fortsatte kontrol med, at de overholdes. Styrelsens personale kan rette henvendelse om sikkerhedsanliggender direkte til sikkerhedsofficeren.

Stk. 2. I relation til elektroniske informationssystemer, der behandler informationer klassificeret HEMMELIGT eller FORTROLIGT, bør der om fornødent udpeges en edb-kyndig assistent. Denne assistent skal støtte sikkerhedsofficeren i forbindelse med overvågning, udvikling, implementering og vedligeholdelse af sikkerhedsforanstaltningerne i elektroniske informationssystemer, herunder udfærdigelse af sikkerhedsinstruksen, jf. § 52, stk. 4.

§ 55. Den nationale sikkerhedsmyndighed yder bistand ved gennemførelsen af bestemmelserne i cirkulæret og de supplerende sikkerhedsforskrifter, der er udarbejdet af de enkelte styrelser efter § 52, stk. 2.

Stk. 2. Den nationale it-sikkerhedsmyndighed yder bistand ved gennemførelsen af it-sikkerhedsmæssige opgaver i cirkulæret og de supplerende sikkerhedsforskrifter, der er udarbejdet af de enkelte styrelser efter § 52, 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 den pågældende myndighed ligger inde med.

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.

C. Ikrafttræden m.v.

§ 58. Cirkulæret træder i kraft den 1. januar 2014.

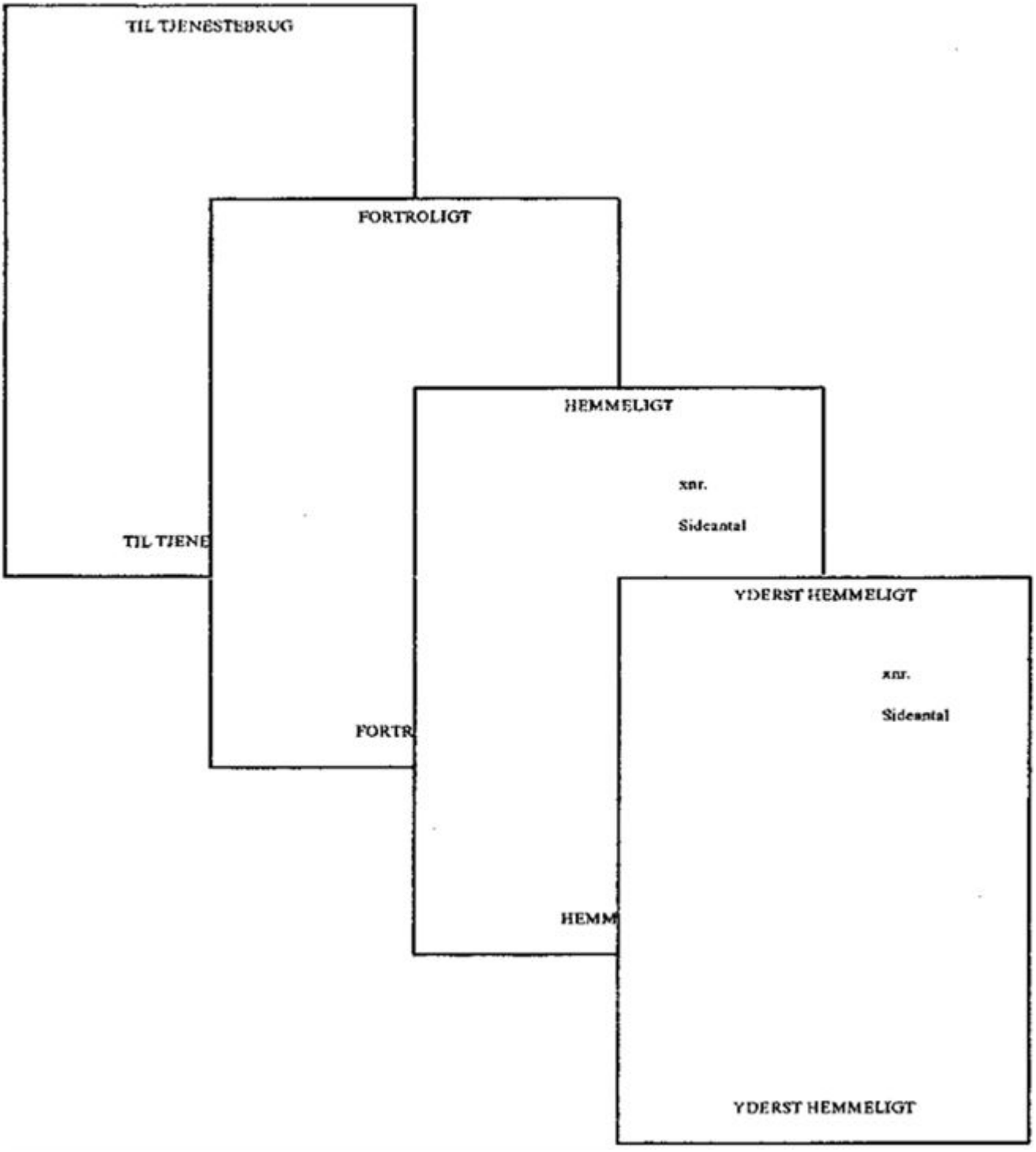
Stk. 2. Cirkulære af 7. december 2001 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt ophæves.

Statsministeriet, den 21. december 2013

HELLE THORNING-SCHMIDT

/ Jens Teilberg Søndergaard

Bilag


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