Bilag til Beredskabsplan for Indenrigs- og Sundhedsministeriets departement

Sidst opdateret 27. maj 2026

Bilagsliste

1

BILAG 1: INSTRUKS FOR HÅNDTERING AF VARSLER OG ALARMER SAMT AKTIVERING AF BEREDSKABSPLANEN 2
BILAG 2: INSTRUKS FOR AKTIVERING AF TRIN 1 (INFORMATIONSBEREDSKAB) 4
BILAG 3: INSTRUKS FOR AKTIVERING AF TRIN 2 (STABSBEREDSKAB) 5
BILAG 4: INSTRUKS FOR AKTIVERING AF TRIN 3 (OPERATIONSBEREDSKAB) 6
BILAG 5: SUNDHEDSSEKTORENS OPERATIVE STAB (SOST) 8
BILAG 6: KRISESTABSCHEFENS OG VICEKRISESTABSCHEFENS FUNKTIONER 11
BILAG 7: SKABELON FOR BEMANDINGSOVERSIGT OG KRISESTYREORGANISATIONEN 12
BILAG 8: SKABELON FOR DAGSORDNER OG REFERAT FOR KRISESTABENS MØDER 14
BILAG 9: INSTRUKS FOR KLARGØRING AF KRISESTABENS LOKALER MV. 16
BILAG 10: DEPARTEMENTETS SITUATIONSBILLEDE 17
BILAG 10A: SKABELON FOR DEPARTEMENTETS SITUATIONSBILLEDE 18
BILAG 11: INSTRUKS FOR LOGFØRING 20
BILAG 12: INSTRUKS FOR JOURNALISERING 21
BILAG 13: SKABELON FOR KRISESTABENS "TAVLEOVERSIGT" 22
BILAG 14: HUSKELISTE TIL DEPARTEMENTETS FORBINDELSESOFFICERER 23
BILAG 15: SKABELON FOR STATUSNOTAT TIL ANDRE MYNDIGHEDER 24
BILAG 16: STÅENDE OPERATIONSPROCEDURE FOR PRESSE OG KOMMUNIKATION 25
BILAG 17: SKABELON FOR PRESSE- OG KOMMUNIKATIONSSTRATEGI 26
BILAG 18: KONTAKTOPLYSNINGER PÅ BEREDSKABSANSVARLIGE PÅ MINISTEROMRÅDET 28
BILAG 19: KONTAKTOPLYSNINGER PÅ CHEFER I DEPARTEMENTET OG PÅ MINISTEROMRÅDET 28
BILAG 20: SUNDHEDSSTYRELSENS BEREDSKABSPLAN 28
BILAG 21: NATIONAL KRISESTYRING VED UDBRUD AF PANDEMISK INFLUENZA 28
BILAG 22: INSTRUKS FOR HÅNDTERING AF KLASSIFICERET INFORMATION 29
BILAG 23: INSTRUKS FOR HÅNDTERING AF DEPARTEMENTETS SINE RADIOER 32
BILAG 24: TTJ-MATERIALE OG SMART TTJ-KOMMUNIKATION VIA MOBILNETTET 34
BILAG 24A: SIKKERHEDSINSTRUKS FOR BRUGERE AF SMART 36
BILAG 25: DRIFT OG OVERVÅGNING AF REGNEM 38
BILAG 26: IT-SIKKERHED 39
BILAG 27: INDENRIGS- OG SUNDHEDSMINISTERIETS BEREDSKABSINSTRUKS 40

Bilag 1: Instruks for håndtering af varsler og alarmer samt aktivering af beredskabsplanen

Formål: At sikre hurtig og effektiv visitation og håndtering af varsler og alarmer samt lignende information med henblik på orientering af relevante personer og på eventuel aktivering af beredskabsplanen.

Opgave
Instruksen aktiveres, når der modtages varsler, alarmer, eller når en chef eller medarbejder i øvrigt finder anledning til at orientere om en situation, der kan kræve aktivering af beredskabsplanen.

Ledelse/ansvar for udførelse af opgave
Chefen for den enhed, der modtager varsel/alarm, er ansvarlig for, at instruksen aktiveres.

Organisation
Selve opgaven med håndtering af varsler og alarmer kan varetages under normal organisation (ikke behov for forstærkning).

Procedurer:

Modtagelse af varsler og alarmer og lignende information
Varsling og lignende kan ske pr. telefon, e-mail, almindelig post via departementets sædvanlige kontaktveje, overvågningssystemer eller REGNEM.

De typiske varsler og alarmer mv. består af:

- Varsler om farligt vejr.
- Trusselvurderinger vedrørende sikkerhedsmæssige trusler fra sikkerhedstjenester.
- Aktivering af tværgående stabe (f.eks. den Lokale Beredskabsstab (LBS), Den Nationale Operative Stab (NOST), Den Internationale Operative Stab (IOS), Det Centrale Operative Kommunikationsberedskab (DCOK), Embedsmandsudvalget for Sikkerhedsspørgsmål eller regeringens Sikkerhed valg).
- Varsler og alarmer fra internationale organisationer.
- Medieomtale af større hændelser, der kan have særlig interesse for departementet.
- Uheld eller andre hændelser, der i øvrigt kan vedrøre departementets sektoransvar.

Varsler og alarmer mv. modtages af Ministersekretariatet og Ledelsessekretariatet eller af medarbejdere/chefer i departementets forskellige enheder. Varsler og alarmer kan forekomme både inden for og uden for departementets åbningstid.

Når det drejer sig om trusler eller hændelser vedr. it-sikkerhed/cyberangreb, vil varsler/alarmer ofte blive modtaget af Statens IT og Styrelsen for Samfundssikkerhed (SAMSIK) der melder videre til departementets interne it (ISDB & IT) og til de øvrige institutioner på ministerområdet.

Modtagende chef vurderer, hvem der skal orienteres internt og eksternt. Forsigtighedsprincip anvendes – det er bedre at orientere en gang for meget end en gang for lidt. Ved tvivl skal der konfereres med kontorchefen i Center for Service, Sikkerhed og IT.

Ved aktivering af Den Nationale Operative Stab (NOST) eller forvarsel om eventuel aktivering af Den Nationale Operative Stab (NOST) skal kontorchefen i Center for Service, Sikkerhed og IT samt sikkerhedsofficeren straks orienteres.

I tilfælde af en trussel, hændelse eller krise, der vedrører bygningen, skal Center for Service, Sikkerhed og IT kontakte Bygningsstyrelsen på hovednummeret 41701010. Det kan fx være ved oversvømmelse, strømnedbrud eller lignende.

Vurdering af behov for aktivering af krisestaben

Medarbejderen kontakter sin chef (alternativt dennes stedfortræder eller én af afdelingscheferne) med henblik på vurdering af aktivering af krisestaben. Hvis en chef vurderer, at det er nødvendigt at aktivere beredskabsplanen og evt. krisestaben, kontaktes en afdelingschef, der kan indstille aktivering af beredskabsplanen og evt. krisestaben til departementschefen. Det er kun departementschefen, der kan aktivere beredskabsplanen og krisestaben. Hvis departementschefen ikke er tilgængelig, er ansvaret for aktivering af beredskabsplanen og krisestaben delegeret til krisestabschefen, som er afdelingschefen med ansvar for sikkerhed. I tilfælde hvor hverken departementschefen eller krisestabschefen er tilgængelige, er det afdelingschefen med ansvar for stab, der er ansvarlig for aktivering af beredskabsplanen og krisestaben.

Ved aktivering af krisestaben sender krisestabschefen en SMS til alle faste medlemmer af krisestaben. Beskeden sendes både via almindelig SMS og via SMART til gruppen "ISM-krise - Krisestab", der består af samme medlemmer i begge grupper.

Hvis krisestaben beslutter at udsende forbindelsesofficer, til eksempelvis en styrelse i Indenrigs- og Sundhedsministeriets koncern, uden (eller inden) aktivering af krisestaben, udpeges forbindelsesofficeren af den kontorchef, der normalt er ansvarlig for det pågældende område.

Hvis det besluttes at aktivere krisestaben eller at orientere potentiel kommende krisestab og støttefunktioner, sker det efter procedurerne i bilag 2, 3 og 4: Aktivering af trin 1 (Informationsberedskab), aktivering af trin 2 (Stabsberedskab), aktivering af trin 3 (Operationsberedskab).

Hvis beredskabet hæves, skal afdelingschefen med ansvar for sikkerhed, kontorchefen i Center for Service, Sikkerhed og IT, sikkerhedsofficeren samt enhedsleder i ISDB & IT og departementets interne it straks varsles af hensyn til sikkerheden i bygningen (Slotsholmsgade 10-12).

Bilag 2: Instruks for aktivering af trin 1 (Informationsberedskab)

Formål: At sikre at relevante i departementet er velinformeret om situationen og dens udvikling.

Opgave
Instruksen aktiveres, når departementschefen vurderer, at relevante chefer og nøglepersoner bør orienteres om en indtruffen hændelse, men at der ikke umiddelbart er behov for at etablere krisestab og støttefunktioner.

Ledelse/ansvar for udførelse af opgave
Ledelsessekretariatet.

Organisation
Normal organisation. Der afholdes evt. enkelte møder efter behov.

Procedurer/foranstaltninger
De enkelte tiltag tilpasses den konkrete situation for at sikre en fleksibel håndtering af situationen. Som udgangspunkt iværksættes følgende tiltag som minimum under trin 1 (Informationsberedskab):

- Planer gennemgås og ajourføres efter behov af relevante enheder
- Overvågning af situationen. Sagsbehandlere fra relevant enhed udpeges af egen chef.
- Presseovervågning iværksættes.
- Løbende orientering af relevante chefer og nøglepersoner internt samt evt. eksternt. Nøglepersoner internt tæller som udgangspunkt afdelingschef med ansvar for sikkerhed, kontorchefen i Center for Service, Sikkerhed og IT, kontorchef for Beredskab, chef for Ledelsessekretariatet, sikkerhedsofficeren og chef for Presse og Kommunikation.
- Opstart og føring af log.
- Løbende stillingtagen til fortsat aktivering af trin 1 (Informationsberedskab). Dette skal dokumenteres i loggen.

Bilag 3: Instruks for aktivering af trin 2 (Stabsberedskab)

Formål: At sikre at de relevante i departementet er velinformerede om situationen og dens udvikling, samt at der kan etableres krisestab og støttefunktioner med kort varsel.

Opgave
Instruksen aktiveres, når departementschefen vurderer, at der ikke umiddelbart er behov for at etablere krisestab og støttefunktioner, men at relevante chefer og nøglepersoner skal holde sig orienteret om situationen. Derudover kan krisestaben mødes, hvis behovet opstår.

Ledelse/ansvar for udførelse af opgave
Afdelingschefen for Sikkerhed eller kontorchefen i Center for Service, Sikkerhed og IT.

Organisation
Normal organisation, dog orienteres krisestabschef. Der afholdes løbende møder (evt. virtuelt).

Bemanding
Inden for og uden for normal arbejdstid varetages opgaver af medarbejdere i den eller de relevante enheder samt krisestabschef.

Procedurer/foranstaltninger
De enkelte tiltag tilpasses den konkrete situation for at sikre en fleksibel håndtering af situationen. Som udgangspunkt iværksættes følgende tiltag som minimum under stabsberedskab (trin 2):

- Hvis ikke krisestabschef er tilstede udpeges ny krisestabschef.
- Potentielle medlemmer af krisestab og støttefunktioner varsles om aktiveringen af stabsberedskab (trin 2), herunder evt. snarlig overgang til operationsberedskab (trin 3).
- Planer gennemgås og ajourføres efter behov.
- Situationen overvåges nøje af relevante enheder. Sagsbehandler(e) fra den eller de relevante faglige enheder udpeges af egen chef.
- Presseovervågning iværksættes.
- Løbende orientering af relevante chefer og nøglepersoner internt samt evt. eksterne samarbejdspartnere om situationen og beredskabet i departementet.
    - Nøglepersoner internt tæller som udgangspunkt minimum krisestabschef og chef for Presse og Kommunikation, kontorchef i Center for Service, Sikkerhed og IT samt sikkerhedsofficeren.
    - Eksterne samarbejdspartnere kan være Sundhedsstyrelsen, Lægemiddelstyrelsen, Styrelsen for Patientsikkerhed, Sundhedsdatastyrelsen, Statens Serum Institut, regioner/kommuner, andre myndigheder, Den Nationale Operativ Stab (NOST) samt internationale kontakter.
- Chefer og nøglepersoner mødes løbende (evt. virtuelt) for at blive opdateret på status og opgaver og drøfte beredskabsniveauet i departementet.
- Behov for særlige procedurer vurderes:
    - Rapporteringsordning for samarbejdspartnere.
    - Etablering af særlige lokaler.
    - Udvidelse af Presse og Kommunikations og øvrige enheders kapacitet.
    - Behov for andre særlige foranstaltninger
- Der føres log.
- Løbende stillingtagen til fortsat aktivering af stabsberedskab (trin 2) eller eskalering til operationsberedskab (trin 3) eller nedskalering.

Bilag 4: Instruks for aktivering af trin 3 (Operationsberedskab)

Formål: At sikre, at departementet kan varetage samtlige krisestyringsrelevante opgaver med det samme og i længere tid.

Opgave
Instruksen aktiveres straks, når departementschefen vurderer, at der er behov for at etablere krisestaben og støttefunktioner. Det er kun departementschefen, der kan aktivere krisestaben. Alle afdelingschefer kan indstille til departementschefen, at krisestaben aktiveres. Hvis departementschefen ikke er tilgængelig, er ansvaret for aktivering af beredskabsplanen og krisestaben delegeret til krisestabschefen, som er afdelingschefen med ansvar for sikkerhed. I tilfælde hvor hverken departementschefen eller krisestabschefen er tilgængelige, er det afdelingschefen med ansvar for stab der er ansvarlig for aktivering af beredskabsplanen og krisestaben.

Ledelse/ansvar for udførelse af opgave
Krisestabschefen, kontorchefen og/eller sikkerhedsofficeren i Center for Service, Sikkerhed og IT (eller deres stedfortrædere).

Organisation
Krisestyringsorganisation med krisestab og støttefunktioner, herunder krisestabschef og talsmand. Evt. etableres vagtordning centralt i departementet. Krisestabens mødelokale er lokale 6110 på 5. sal.

Bemanding
Krisestaben sammensættes efter behov, jf. beredskabsplan. Krisestabschef og talsmand udpeges på første møde i krisestaben, hvis det ikke allerede er sket. Bemandingen vurderes løbende.

Procedurer/foranstaltninger
De enkelte tiltag tilpasses den konkrete situation for at sikre en fleksibel håndtering af situationen. Som udgangspunkt iværksættes følgende tiltag under operationsberedskab (trin 3):

- Krisestab og støttefunktioner indkaldes af krisestabschefen.
- Evt. afløsere udpeges afhængigt af situationen og varsles.
- Klargøring af faciliteter i følgende lokaler: Krisestabens mødelokale (lokale 6110), krisestabens arbejdsrum (lokale 6118) og REGNEM-rummet.
- Orientering af alle i departementet, direktørerne i styrelserne på ministerområdet og øvrige relevante samarbejdspartnere om operationsberedskabet i departementet.
- Krisestabschef og talsmand udpeges på første møde i krisestaben, hvis det ikke allerede er sket.
- Krisestaben afholder møder efter skabelon for dagsorden for første møde og dagsorden for efterfølgende møder.
- Ved behov afholdes supplerende møder i krisestaben med henblik på koordinering af opgaverne.
- Arbejdsdeling i krisestaben aftales jf. bilag 7 skabelon for bemandingsoversigt og krisestaben og bilag 13 skabelon for stabens tavleoversigt.
- Faglig rådgivning og vejledning udarbejdes og udsendes til andre myndigheder efter behov.
- Evt. andre situationsbestemte opgaver løses.
- Fælles situationsbillede i departementet udarbejdes og ajourføres løbende (både situations- og mediebillede følges tæt).
- Statusnotat udarbejdes og ajourføres løbende og sendes til samarbejdspartnere.
- Kommunikation til borgere og presse.
- Særlige procedurer iværksættes efter behov:
    - Rapporteringsordning for samarbejdspartnere.
    - Udvidelse af Presse og Kommunikations og andre relevante enheders kapacitet.
    - Sikkerhedsforanstaltninger overvejes – skærpet adgangskontrol m.v.

    - Behov for andre særlige foranstaltninger overvejes.

- Der føres log.
- Løbende stillingtagen til fortsat aktivering af operationsberedskab (trin 3) og evt. nedskalering.

Bilag 5: Sundhedssektorens Operative Stab (SOST)

Indenrigs- og Sundhedsministeriets koncern har etableret Sundhedsstyrelsens Operative Stab (SOST) som en stående struktur til koordination mellem centrale og decentrale myndigheder i sundhedsvæsenet, der kan aktiveres ved større beredskabshændelser med betydning for sundhedssektoren. SOST er i departementet forankret i Center for Lægemidler, Beredskab og Internationalt Samarbejde.

SOST blev etableret i februar 2025 og har til formål at styrke samarbejde, koordination, beredskabsplanlægning og krisehåndtering mellem de nationale sundhedsmyndigheder, Kommunernes Landsforening, Danske Regioner, alle regioner samt udvalgte kommuner.

SOST vil træde sammen og koordinere den nødvendige håndtering af større hændelser i sundhedsvæsenet i helt særlige situationer. Det kan fx være ved hændelser, som omfatter mange tilskadekomne, ved strøm-, tele- eller it-nedbrud eller i situationer hvor lægemiddelforsyningen er påvirket af en hændelse.

SOST kan desuden understøtte beredskabsrelateret tværsektorielt arbejde i andre fora som fx Den Nationale Operativ Stab (NOST) og AC-beredskabsgruppen (ACBG) samt i sundhedsvæsenet generelt.

SOST anvendes derudover også som et løbende forum for informationsudveksling og generel koordination.

SOST's opgaver er, at:

- Etablere et fælles skriftligt situationsbillede
- Koordinere og træffe beslutninger inden for en samlet retning og prioritering
- Koordinere overordnet krisekommunikation på tværs af myndigheder
- Etablere undergrupper, som kan fokusere på særskilte dele af håndteringen
- Etablere et fælles overblik over kapaciteter og ressourcer i sektoren
- Samarbejde om en effektiv, strategisk funderet koordination af handlinger og ressourceanvendelse på tværs af myndigheder samt eventuelle civilsamfundsorganisationer

Sammensætning

SOST er som udgangspunkt sammensat af repræsentanter fra følgende myndigheder og organisationer:

- Indenrigs- og Sundhedsministeriet
- Sundhedsstyrelsen
- Regionerne og Danske Regioner
- Kommuner (én fra hver region) og Kommunernes Landsforening
- Lægemiddelstyrelsen
- Statens Serum Institut og Center for Biosikring og Bioberedskab
- Styrelsen for Patientsikkerhed
- Sundhedsdatastyrelsen

SOST kan aktiveres til mere eller mindre afgrænsede opgaver og derfor med udvalgte repræsentanter afhængigt af den konkrete sammenhæng. Det kan i en konkret sammenhæng fx omfatte alle eller nogle myndigheders og organisationers direktioner eller faglige enheder. Mødekredsen vil fastsættes ud fra den enkelte hændelse eller planlægningsproces.

Organisering af arbejdet

Sundhedsstyrelsen varetager formandskabet og sekretariatsbetjeningen af SOST.

Det påhviler Sundhedsstyrelsen, at:

- Træffe beslutning om og aktivere SOST. Ethvert medlem kan anmode om aktivering af SOST, hvorefter Sundhedsstyrelsen sikrer relevant aktivering
- Træffe indledende beslutning om SOST's sammensætning, herunder eventuelt indkalde supplerende deltagere fra fx ekspertberedskaber og -funktioner
- Lede møderne
- Sammen med øvrige medlemmer at etablere overblik over hændelsen (situationsbillede), understøtte iværksættelse af beredskabstiltag, udarbejde strategi for myndighedernes beredskabskommunikation samt iværksætte eventuelle tiltag
- Koordinere information til- og fra tværsektorielle koordinationsfora som Den Nationale Operativ Stab (NOST), international operativ stav (IOS) og sundhedssektoren generelt og understøtte departementet med at koordinere information til – og fra AC-beredskabsgruppen (ACBG).
- Nedsætte eventuelle ad hoc-arbejdsgrupper eller inddrage ad hoc-deltagere (fx i faglige spor, kommunikationsspor, spor målrettet håndteringen mv.)
- Sammen med øvrige medlemmer forestå evaluering og erfaringsopsamling af SOST's og myndighedernes virke

Departementet og de andre medlemmer skal kunne stille med repræsentanter, som har den fornødne indsigt og kompetence. Det betyder, at departementets repræsentanter skal:

- Kunne repræsentere departementet på det relevante ansvarsområde.
- Forud for møderne, når muligt, at have etableret et samlet overblik fra departementet, herunder overblik over og vurdering af den beredskabsmæssige situation inden for eget ansvarsområde
- Kan vurdere forhold, der kan have politiske implikationer
- Har kendskab til SOST-plan med forståelse for, hvad det vil sige at virke i en stab – indgå i aktiv, bilateral og central koordinering

Alle repræsentanter og mødedeltagere skal være sikkerhedsgodkendt til minimum "Hemmelig" (HEM).
Center for Lægemidler, Beredskab og Internationalt Samarbejde er fast medlem af SOST på vegne af departementet. På baggrund af den konkrete situation, vil Center for Lægemidler, Beredskab og Internationalt Samarbejde vurdere hvem fra departementet der skal deltage.

SOST-plan

Sundhedsstyrelsen har udarbejdet en plan for SOST's virke. Formålet med planen er at operationalisere kommissoriet i form af procedurer mv. Planen beskriver blandt andet aktivering, drift, deaktivering, skabeloner mv.

Planen for Sundhedssektorens Operative Stabs virke kan tilgås her: Plan for Sundhedssektorens Operative Stabs virke (SOST).

Bilag 6: Krisestabschefens og vicekrisestabschefens funktioner

Opgave
Varetage funktioner som krisestabschef og vicekrisestabschef i Indenrigs- og Sundhedsministeriets krisestab.

Krisestabschefen og vicekrisestabschefen koordinerer løbende krisestabsarbejdet.

Procedurer for krisestabschefen
Ansvarlig for den løbende drift af krisestaben, herunder at alle krisestabsfunktioner er passende bemandet, og alle medarbejdere i krisestaben kender og kan løfte deres opgaver.

Derudover gælder:

- Alle nye væsentlige informationer og opgaver skal til orientering og eventuel drøftelse hos krisestabschefen før videre distribution og behandling.
- Krisestabschefen godkender Indenrigs- og Sundhedsministeriets situationsbillede, inden det går ud af huset eller fordeles internt.
- Krisestabschefen sikrer, at der sker tilstrækkelig overlevering ved afløsning. Dette gøres i forbindelse med afholdelse af et krisestabsmøde, hvor både afgående og tilkommende krisestabsmedlemmer deltager.

Desuden varetager krisestabschefen nedenstående opgaver, såfremt der ikke er udpeget en vicekrisestabschef.

Procedurer for vicekrisestabschefen
Vicekrisestabschefen skal fungere som krisestabschefens højre hånd. Ved krisestabschefens fravær kan vicekrisestabschefen fungere som krisestabschef. Vicekrisestabschefen overtager følgende opgaver, men får ellers tildelt ad hoc-opgaver:

- Kontakt til Indenrigs- og Sundhedsministeriets stabsmedlem i Den Nationale Operative Stab (NOST), (herunder sikring af at vedkommende løbende koordinerer med Indenrigs- og Sundhedsministeriets forbindelsesofficer i Det Centrale Operative Kommunikationsberedskab (DCOK)).
- Løbende tjek af mails sendt til departementets TTJ-mailadresse og REGNEM-rummet. Kan evt. uddelegeres.
- Sikring af, at der tilflyder den nødvendige information til og fra Presse og Kommunikation i Indenrigs- og Sundhedsministeriet.
- Sikring af, at samarbejdspartnere, herunder de i den givne situation relevante/alle Indenrigs- og Sundhedsministeriets relevante styrelser løbende orienteres.
- Kontakt til evt. understøttende funktioner til krisestaben, der overvejer situationens udvikling.

Bilag 7: Skabelon for bemandingsoversigt og krisestyreorganisationen

Formål: At skabe overblik over den aktuelle krisestyringsorganisation og bemanding af væsentlige funktioner.

Skabelon for bemandingsoversigter, Indenrigs- og Sundhedsministeriets krisestyringsorganisation (krisestab, støttefunktioner):

Opgave
Oversigterne anvendes, når trin 3 (Operationsberedskab) iværksættes i departementet. Den kan anvendes uden, at departementet er i trin 3, hvis det vurderes hensigtsmæssigt.

Ledelse/ansvar for udførelse af opgave
Krisestabschefen har ansvaret for, at instruksen aktiveres.

Organisation
Krisestaben

Bemanding
Krisestabsmedlem i krisestaben tildeles opgaven med at ajourføre bemandingsoversigterne/evt. vagtplan.

Procedurer
Oversigterne tilpasses i den konkrete situation efter princippet om fleksibel organisering af krisestaben.

Oversigterne kan vises/opsættes i krisestabens lokaler og ajourføres, når der sker tilgang eller frafald i krisestaben, samt når der sker afløsning.

Skabelonen for bemandingsoversigt og krisestaben findes på den næste side.

Skabelonen for bemandingsoversigt og krisestaben:

Krisestaben [Indsæt dato og tidspunkt]

Funktion	**Til stede i krisestaben/navn/kontaktoplysninger**	**Forventet afløsning (tidspunkt og navn på afløser)**
Krisestabschef		
Faste krisestabsmedlemmer		
Alle medlemmer af direktionen		
Afdelingschef for sikkerhed (Krisestabschefen)		
Kontorchef for sikkerhed (Vicekrisestabschef)		
Kontorchef for beredskab		
Kontorchef for Presse og Kommunikation		
Chef for Ministersekretariatet		
Chef for Ledelsessekretariatet		
Ad hoc krisestab		
Alle chefer + deres udvalgte beredskabsmedarbejder(e) i departementets kontorer og centre. *Alle chefer skal udpege en beredskabsmedarbejder, som på ad hoc-basis kan indgå i krisestaben på vegne af chefen.*		
Faste understøttende funktioner til krisestaben		
Stabssekretariat (Ledelsessekretariatet i samarbejde med Center for Service, Sikkerhed og IT, beredskabsenheden og øvrige medarbejdere, der udpeges til opgaverne). Omkring 4-6 personer afhængig af hændelsens omfang. Opgaver: • Overvågning og fordeling af post • Telefonpasning • Logføring • Journalisering • Referent • Andet		
Situationsbillede		
Operation		
Logistik		
Administration		
IT		

Bilag 8: Skabelon for dagsordner og referat for krisestabens møder

Formål: At sikre effektiv mødeledelse og at krisestaben drøfter alle relevante punkter.

Opgave
Skabelonen anvendes, når trin 3 (Operationsberedskab) aktiveres i Indenrigs- og Sundhedsministeriet. Den kan også anvendes uden, at Indenrigs- og Sundhedsministeriet er i trin 3, hvis det vurderes hensigtsmæssigt.

Ledelse/ansvar for udførelse af opgave
Krisetabschefen sørger for, at der foreligger en dagsorden, som tager udgangspunkt i skabelonen på de følgende sider. Hvis der ikke er udpeget en krisestabschef, er mødelederen ansvarlig for, at dagsorden foreligger.

Organisation
Krisestaben.

Procedurer
Dagsordenen tilpasses den konkrete situation. Dagsordenen anvendes som skabelon for beslutningsreferatet, som referent skriver under mødet.

Referent anfører dato og tidspunkt for mødet på referatet som godkendes af krisestabschefen, journaliseres og udsendes til deltagerkreds og øvrige involverede umiddelbart efter mødet. Hvis information er klassificeret, håndteres det i henhold til gældende procedurer.

Skabelon for dagsordner følger på næste side.

Skabelon: Dagsorden for møder i krisestaben

Dagsorden for [indsæt nr.] møde i krisestaben [indsæt dato og tidspunkt] vedr. [indsæt emne].

1. **Velkomst ved departementschef/afdelingschefchef**
    a. Referent udpeges (fra krisestab)
    b. Overvejelser om ad hoc-medlemmer
    c. Udpegning af krisestabschef, talsmand og presseansvarlig [på første møde og ved behov for afløsning]
2. **Situationen kort [på første møde v. relevant chef og v. efterfølgende møder v. krisestabschef]**
    a. Nationalt, regionalt og kommunalt niveau
    b. Forventet udvikling
3. **Bemanding**
    a. Sikkerhedsgodkendte medarbejdere ved klassificeret information
    b. Identifikation af relevante samarbejdspartnere
4. **Mediebilledet ved chef for presse og kommunikation**
    a. Relevante presseaktivitet og henvendelser
5. **Strategisk hensigt**
    a. Overvejelser om passende strategisk hensigt
    b. Vurdere relevante politiske og økonomiske forhold
6. **Krisestabens opgaver ved krisestabschef**
    a. Orientering om relevante opgaver
    b. Overvejelser vedr. ressourcer mv.
7. **Kommunikation**
    a. Godkendelse af presse- og kommunikationsstrategi
    b. Plan for opdatering af hjemmeside mv.
    c. Intern kommunikation
8. **Koordination**
    a. Behov for koordination intern/eksternt
    b. Behov for særlige procedurer
9. **Aktiveringsniveau**
    a. Informationsberedskab, stabsberedskab eller operationsberedskab
10. **Eventuelt**
11. **Opsamling ved mødelederen**
12. **Tidspunkt for næste møde**

Bilag 9: Instruks for klargøring af krisestabens lokaler mv.

Opgaver under kriseberedskab

Opgave Klargøring af krisestabens lokaler: Krisestabens mødelokale (lokale 6110), krisestabens arbejdslokale (lokale 6118) og REGNEM-rummet.
Ansvar for at udføre opgaver under klargøring Center for Service, Sikkerhed og IT aktiverer klargøringen.
Procedurer Repræsentant fra Center for Service, Sikkerhed og IT møder op i krisestabens mødelokale (lokale 6110) og aftaler/gør følgende: • Opsætning af dockingstationer til fire PC'ere i krisestabens arbejdsrum – *kontakt departementets interne it (ISDB & IT)*. • Krisestaben medbringer egne bærbare pc'er til brug for referatskrivning mv. under krisestabens møder, hvis mødet er uklassificeret. • Levering af mad, drikkevarer mv.: Bestilles af Center for Service, Sikkerhed og IT i kantinen eller andet sted, hvis kantinen er lukket. • Levering af kontorartikler: Center for Service, Sikkerhed og IT. • Postaflevering: Center for Service, Sikkerhed og IT. • Papir/toner til printer efter behov: Center for Service, Sikkerhed og IT. • Omstilling til pressemøder i egnet lokale efter aftale med krisestabschef. • Opsætning af oppustelige madrasser efter aftale med krisestabschef. • Etablering af særlig/skærpet adgangskontrol til departementet eller til udvalgte områder i huset: Aftales med portvagten (Securitas) og med Justitsministeriet – *kontakt en af departementets sikkerhedsofficerer i Center for Service, Sikkerhed og IT*. • Ad hoc-opgaver.

Bilag 10: Departementets situationsbillede

Formål: At etablere og fastholde et fælles situationsbillede i departementet. Bilaget består af en instruks for opgaven og en skabelon for situationsbilledet.

Opgave
Udarbejdelse af departementets samlede situationsbillede.

Instruksen aktiveres, når departementschefen har aktiveret krisesituationsbilledet på trin 2 (Stabsberedskab).

Ledelse/ansvar for udførelse af opgave
Krisestabschefen har ansvaret for at etablere og ajourføre situationsbilledet, og at skabelonen anvendes.

Organisation
Krisestaben.

Bemanding
Krisestabschefen uddelegerer opgaven til beredskabsenheden for så vidt angår eksterne hændelser, der vedrører sundhedsområdet/sundhedsberedskabet (evt. med inddragelse af andre enheder), og Center for Service, Sikkerhed og IT for så vidt angår interne hændelser, der vedrører departementet eller ministerområdets øvrige institutioner. I tilfælde af hændelser, der påvirker både eksternt og internt, træffer krisestaben beslutning om, hvilken af de to enheder der skal have ansvaret for udarbejdelsen af departementets situationsbillede.

De enkelte enheder er ansvarlige for at komme med inputs til situationsbilledet forud for hvert møde i krisestaben (eller efter nærmere aftale).

Procedurer

- Skabelon benyttes, da denne er bygget op som det situationsbillede, der benyttes af Sundhedsstyrelsen (væsentligste samarbejdspart vedr. sundhedsberedskabet).
- Det samlede situationsbillede må maks. fylde 2-3 sider.
- Hvis situationen ikke tilsiger, at det er relevant at udfylde enkelte bokse, skrives "Ikke relevant".
- Interne forkortelser skal så vidt muligt undgås.
- Ændringer i forhold til seneste situationsbillede skal tydeligt fremgå.
- Situationsbilledet fremsendes løbende til alle relevante internt i departementet og evt. til samarbejdspartnere.
- Enhederne fortsætter med deres afrapportering, så længe krisestaben er etableret.

Bilag 10a: Skabelon for departementets situationsbillede

Departementets situationsbillede. Situationsbilledet må max fylde 2-3 sider.

[Inspiration til udarbejdelsen af situationsbillede kan hentes i bilag 14 om statusnotat]

Udfærdigelsestidspunkt og version:	*[dato og tidspunkt], [nr. vedr. den givne hændelse]*		
Godkendt af:	*[navn på krisestabschef]*		
Aktiveringstrin (sæt kryds)	[ ] Informationsberedskab	[ ] Stabsberedskab	[ ] Operationsberedskab

Situationen (kort beskrivelse)

[Hvornår, hvor og hvad er sket og med hvilke konsekvenser?
Er Den Nationale Operative Stab (NOST) aktiveret?
Se referater fra krisestabsmøder og Den Nationale Operative Stabsmøder (NOST) National Strategisk Overblik (NSO), information fra region og input fra vicekrisestabschef (eller krisestabschef).

Husk at fjerne forældede oplysninger!

Krisestaben kan bl.a. forholde sig til disse punkter:

- *Kontakt til og aftaler med andre ministerier*
- *Kontakt til og aftaler med regioner og kommuner*
- *Antal berørte og evt. tilskadekomne og dræbte (bekræftet)*
- *Kapacitetsproblemer i departementet og sundhedsvæsenet (regioner og kommuner)*
- *Forbindelsesofficerer i hvilke stabe (nationalt og i krisestaben)*
- *Anmodning sendt til udlandet om assistance*
- *Iværksat psykosocial indsats*
- *Trussel mod ministeriet, f.eks. som følge af strømnedbrug eller cyberhændelse?]*

Seneste udvikling

[Ved hver opdatering skrives situationens seneste udvikling og gammel tekst slettes]

Krisestabens aktuelle prioriteringer

[Krisestaben kan forholde sig til disse punkter:

- *Prioritering af indsatsen i krisestaben*
- *Fastlæggelse af overordnet pressestrategi*
- *Eventuelle beslutninger om økonomiske, politiske eller internationale forhold]*

Krisekommunikation og mediebilledet

[Hvad er meldt ud til borgerne og pressen, og hvordan bliver hændelsen dækket af pressen, på sociale medier mv.? Se referater fra krisestabsmøder og Den Nationale Operative Stabs møder (NOST-stabsmøder), Nationalt Strategisk Overblik (NSO) og tal med koordinator af presse- og kommunikationsindsatsen i krisestaben]

Kapacitet i sundhedsvæsenet

[Er der tilstrækkelig kapacitet til at håndtere hændelsen?
Hvordan søges evt. kapacitetsproblemer løst?]

Situationens mulige udvikling

[Best og worst case scenarier for situationens udvikling. Indsæt max 3-4 punkter. Se referater fra stabsmøder og NOST-stabsmøder, IOS, AC, og tal evt. med personansvarlig for analyse af mulige konsekvenser af hændelsen]

Input til NSO

[Input til Nationalt Strategisk Overblik til repræsentanten såfremt Den Nationale Operative Stab (NOST) er aktiveret. Max 4-5 linjer. Opsummering af vigtigste pointer fra situationsbilledet vedr. situationen, krisestabens aktuelle prioriteringer og strategisk hensigt og evt. mulig udvikling. Skal være godkendt af krisestabschef eller vicekrisestabschef]

Næste situationsbillede

[Hvornår forventer departementet at lave næste situationsbillede]

Bilag 11: Instruks for logføring

Opgave
Instruksen aktiveres, når stabs- eller operationsberedskab aktiveres.

Ledelse/ansvar for udførelse af opgave
Krisestabschefen.

Organisation
Stabsberedskab: Opgaven varetages af Ledelsessekretariatet i samarbejde med Center for Service, Sikkerhed og IT eller anden relevant enhed.

Operationsberedskab: Opgaven varetages i regi af krisestaben.

Bemanding
Opgaven varetages af et krisestabsmedlem, som udpeges af krisestabschefen.

Procedurer/foranstaltninger
Krisestabsmedlem udpeget af krisestabschefen fører log over forløbet efter skabelonen nedenfor. Logføring foretages i krisestabens arbejdsrum (lokale 6118), hvis dette er etableret, og vises på AV-skærmen i lokalet.

Alle væsentlige hændelser, henvendelser, opgaver m.v. logføres. Ved flere samtidige, uafhængige hændelser, oprettes en log for hver hændelse.

Alle i krisestaben har ansvaret for at relevante ting føres i log. Evt. afleveres skriftlige input til logføreren.

Krisestabschefen gennemlæser og godkender teksten minimum ved arbejdsdagens afslutning samt ved vagtskifte.

Skabelon
Departementets logbog [måned og år]

Titel:
Plan:
Problemstillinger:

Dato og tidspunkt (ugedag, dato, årstal, klokkeslæt)	Hændelse	Reaktion	Bemærkninger/huskeliste

Bilag 12: Instruks for journalisering

Opgave
Instruksen aktiveres, når stabs- eller operationsberedskab aktiveres.

Ledelse/ansvar for udførelse af opgave
Krisestabschefen.

Organisation
Stabsberedskab: Opgaven varetages under almindelig organisation af Ledelsessekretariatet og/eller anden relevant enhed.

Operationsberedskab: Opgaven varetages i regi af krisestaben.

Bemanding
Opgaven varetages af et krisestabsmedlem, som udpeges af krisestabschefen.

Procedurer/foranstaltninger:
Der oprettes en ny sag i F2 af et af krisestabens understøttende funktioner. Der journaliseres udelukkende i F2.

I tilfælde af længerevarende strømnedbrud benyttes fysisk pen og papir i arbejdet i krisestaben. Derudover etableres et fysisk journaliseringssystem, som lever op til retningslinjerne for god journaliseringspraksis. Når strømmen vender tilbage, har krisestaben en pligt til at journalisere det fysiske materiale i F2.

Journalisering
Krisestabsmedlemmet, som udpeges af krisestabschefen, journaliserer mails, breve og andre dokumenter. Journalisering kan evt. foretages i krisestabens arbejdsrum (lokale 6118).

Indkommende mails
Alle relevante indkommende mails gemmes i Outlook, indtil journalisering er foretaget.

Udgående mails
Alle udgående mails gemmes i Outlook, indtil journalisering er foretaget.

Klassificeret post
Håndteres efter særlige procedurer. Se instruks for håndtering af klassificeret information (bilag 14).

Andre dokumenter
Øvrige dokumenter indscannes og journaliseres løbende.

Bilag 13: Skabelon for krisestabens "tavleoversigt"

Formål: At give krisestaben et overblik over igangværende opgaver/prioriteter.

Opgave
Skabelonen anvendes, når trin 3 (Operationsberedskab) aktiveres i departementet. Den kan også anvendes uden departementet er i trin 3, hvis det vurderes hensigtsmæssigt.

Ledelse/ansvar for udførelse af opgave
Krisestabschefen har ansvaret for, at instruksen aktiveres.

Organisation
Krisestaben.

Bemanding
Krisestabschef og krisestabsmedlemmer.

Procedurer
- Oversigten tilpasses i den konkrete situation efter princippet om fleksibel organisering af krisestaben.
- Krisestabschef opretter og ajourfører oversigten, der vises på AV-skærmen i krisestabens lokale (lokale 6110).
- Et krisestabsmedlem udpeget af krisestabschefen sørger for, at oversigten føres elektronisk (og evt. printes) og løbende journaliseres (dokumentation).
- Samme oversigt anvendes også til møder.
- I tilfælde af strømnedbrud laves krisestabens tavleoversigt på papir/whiteboard.

Skabelon for krisestabens "tavleoversigt"

Situation	**Opgave**	**Ansvarlig**	**Deadline**	**Status:** - gennemført - under udførelse - afventer

Bilag 14: Huskeliste til departementets forbindelsesofficerer

Formål: At forberede forbindelsesofficerer på deres opgaver.

Opgave
At fungere som bindeled mellem departementet og en anden myndighed med henblik på koordinering af opgaverne mellem departementet og den pågældende myndighed i en krisesituation.

Ledelse/ansvar for udførelse af opgave
Når departementets egen krisestab er nedsat, vil forbindelsesofficerer referere direkte til krisestabschefen, og forbindelsesofficeren skal derfor på forhånd sikre sig kontakt direkte til krisestabschefen.

Procedurer:

Før afgang
Følgende medbringes/afklares før afgang:

- Bærbar pc, strømforsyning, internetkabel, USB-sticks.
- Mobiltelefon, oplader.
- Relevante planer (National Beredskabsplan, departementets beredskabsplan).
- Kontaktnumre til relevante personer.
- Kommunikation med bagland afklares: Hvem, hvordan og hvor ofte?
- Situationsbillede, faglige spørgsmål og mandat afklares inden afgang.

Under ophold i en anden myndighed
- Deltag løbende i krisestabsmøder.
- Kommuniker løbende med bagland i departementet.
- Repræsentere departementet og sende relevant info fra den anden myndighed til departementet og fra departementet til den anden myndighed – vær opmærksom på eventuelle klassificerede informationer.
- Bidrage med information til myndighedernes fælles situationsbillede ved at have overblik over situationen i departementet/på sundhedsområdet.
- Før løbende log.
- Overdrag, hvis der sker afløsninger (lav skriftlige notater og gennemgå dette med afløser).

Bilag 15: Skabelon for statusnotat til andre myndigheder

Status vedr. [XXX]

1. Aktuel situationsbeskrivelse fx
- Trusselsvurdering
- Antal smittede, syge/tilskadekomne [herunder grad/karakter], døde
- Antal indlagte [fordelt på region]
- Sygdommens/epidemiens/hændelsens udvikling
- Beredskabsniveau i departementet [Informationsberedskab/mødeberedskab/Operationsberedskab]

2. Forventning til udvikling
- Forventning til kortsigtet udvikling – én til tre dage
- Forventning til langsigtet udvikling – hvornår forventer vi, at situationen/hændelsen bliver bedre/værre/overstået?

3. Operative beredskabsforanstaltninger og tiltag
- Hvilke initiativer har departementet taget?
- Hvilke udfordringer forventer departementet i den kommende tid?

4. Kapacitet i sundhedsvæsenet
- Er der tilstrækkelig kapacitet til at håndtere hændelsen på sygehusene/præhospitalt/hos lægerne/særligt indrettede afdelinger, apoteker/sygehusapoteker, lægemidler, lægemiddelgrossister, medicinalfirmaer el.lign.?
- Hvordan søges evt. kapacitetsproblemer løst?

5. Mediebilledet
- Hvordan bliver situationen behandlet/beskrevet i medierne?
- Hvordan bliver departementets rolle beskrevet?
- Hvilke informationer bliver efterspurgt?

6. Kommunikationsinitiativer
- Hvilke handlingsanvisninger er givet til hvilke grupper?
- Hvad gør departementet for at informere befolkningen?
- Hvad gør departementet for at informere medierne?
- Hvad gør departementet for at informere myndigheder i sundhedsvæsenet?

7. Resumé af hændelsen
- Kort resumé af hændelsen, som den har udviklet sig fra begyndelsen. [Kan genbruges løbende i statusnotatet].

8. Frekvens af notat
- Hvornår laver departementet det næste statusnotat?

9. Modtagere
- Hvem modtager dette notat?

Bilag 16: Stående operationsprocedure for Presse og Kommunikation

Denne stående operationsprocedure træder som udgangspunkt i kraft, når krisestyringsorganisationen er på trin 2 (Stabsberedskab). Planen beskriver, hvordan de afgørende funktioner skal varetages i en krisesituation.

De overordnede retningslinjer for Presse og Kommunikations og opgaver i krisesituationer fremgår af departementets beredskabsplan.

1. Bemanding og ressourcer
Presse og Kommunikation bemandes som udgangspunkt med samme niveau som normalt. I ekstraordinære situationer, kan det være nødvendigt at tilkalde mandskab fra andre enheder.

2. Funktioner
Planen beskriver en række funktioner, der skal udføres af én eller flere personer. Chefen for Presse og Kommunikation (eller dennes stedfortræder) udpeger personer til de enkelte funktioner.

Funktionerne i planen er:
- Daglig leder af Presse og Kommunikation/leder af presseindsatsen.
- Medieovervåger.
- Kommunikationsmedarbejder.

3. Beskrivelse af funktionerne

Daglig leder af Presse og Kommunikation:
- Leder, fordeler og prioriterer arbejdet.
- Beslutter, hvem der deltager i krisestabsmøder og briefer om kommunikationsstrategi og mediebilledet.
- Ansvarlig for at få udarbejdet en kommunikations- og pressestrategi.
- Ansvarlig for pressekontakt.
- Ansvarlig for, at alle henvendelser fra – eller udspil til – medier bliver håndteret i overensstemmelse med vedtaget kommunikations- og pressestrategi.
- Udarbejder udkast til svarberedskaber og talsmandspapirer i samråd med krisestabschefen og berørte chefer.
- Bidrager til statusnotaters afsnit om mediebilledet.
- Vurderer og håndterer behov for evt. tilførsel af ekstra ressourcer fra andre enheder.

Medieovervåger:
- Overvåger aviser, radio, TV og internetmedier – dels for at skabe indsigt i, hvordan situationen bliver beskrevet og dels for at give mulighed for at gribe ind, hvis der opstår fejl, myter eller misforståelser i medierne beskrivelse af situationen.
- Orienterer løbende den daglige leder af presseindsatsen om relevante udviklinger i medierne.
- Bidrager til briefing af krisestaben og til statusnotatets afsnit om mediebilledet.
- Både danske og internationale medier skal overvåges.

Kommunikationsmedarbejder:
- Sikrer at information, trusselsvurdering, handlingsanvisninger mm. er overskuelige og tilgængelige på www.sum.dk eller andre valgte platforme.
- Udarbejder ved større eller længerevarende hændelser forslag til struktur for emnet på www.sum.dk
- Ansvarlig for løbende kommunikation til medarbejderne via intranet eller mails.
- Skriver i samarbejde med fagmedarbejdere handlingsanvisninger, trusselsvurderinger mv. til hjemmesiden og giver input til informationsmateriale mv.

Bilag 17: Skabelon for presse- og kommunikationsstrategi

Når departementets krisestab bliver nedsat, er det Presse og Kommunikations ansvar at udarbejde en kommunikations- og pressestrategi. Første version af strategien skal om muligt være færdig til første møde i krisestaben. Strategien skal derefter justeres i forhold til situationen.

Kommunikations- og pressestrategi		
Emne *XX (f.eks. ebola)*	**Dato** *[indsæt dato]*	**Version** *[indsæt version – f.eks. 1]*
Udarbejdet af *Xx, Telefon xx xx xx xx, mail: xx@sum.dk*		
Hændelse		
[indsæt kort beskrivelse af hændelsen]		
Formål med kommunikationen		
Hvad er det eller de vigtigste formål med kommunikationen? *F.eks.:* • *Eksternt: At give borgerne præcise handlingsanvisninger, at oplyse om faktiske forhold og myndighedernes råd og anbefalinger samt understøtte de øvrige sundhedsmyndigheders indsats.* • *Internt: At sørge for, at medarbejderne er velorienterede og klædt på til at besvare spørgsmål, og at medarbejderne ved, hvad der forventes af dem.*		
Hovedbudskaber samt begrundelse/fakta		
Hvad er departementets hovedbudskab? Eventuelt flere budskaber til forskellige målgrupper *F.eks.:* • *At risikogrupper eller befolkningen som helhed skal følge særlige handlingsanvisninger.* • *At der ikke er grund til bekymring.*		
Målgrupper, medier og budskaber		
Hvordan vil man i den kommende tid få opdateret information om forskellige aspekter af situationen? F.eks.: • *Egne eller eksterne eksperter.* • *Andre institutioner på ministerområdet (*Sundhedsstyrelsen (*SST), Lægemiddelstyrelsen (LMST), Styrelsen for Patientsikkerhed (STPS), Styrelsen for Patientklager (STPK), Sundhedsdatastyrelsen (SDS), Statens Serum Institut (SSI)).* • *Andre ministerier.* • *Internationale organisationer som (f.eks. World Health Organisation (WHO)).* *Hvem er den eller de vigtigste eksterne målgrupper for departementets kommunikation om hændelsen? Evt. i prioriteret rækkefølge.* *OBS: Hvilke særlige kommunikationsbehov har de udvalgte målgrupper og på hvilke sprog? I nogle tilfælde kan særskilte gruppers kommunikationsbehov undersøges systematisk.*		

Dertil kommer medarbejdere og chefer i departementet. *Se eksempel herunder:*		
Befolkningen	*Trykte og digitale medier, herunder egne sociale platforme*	*Information om situationen, og hvorfor sikkerheden er på plads*
Indenrigs- og Sundhedsministeriet medarbejdere	*Intra*	*Information om situationen, og hvad der bliver gjort.*
Xx	*xx*	*xx*
Valg af medier		
Hvilke medier og kanaler skal departementet bruge til at kommunikere? F.eks.: • *Medierne (nyheder/pressemeddelelser på www.sum.dk, interviews, pressemøder)* • *Hjemmesiden (www.sum.dk)* • *Sociale medier*		
Kontaktpersoner og talspersoner		
Talsperson ved mediehenvendelser: xx, tlf. xx, mail		
Kontaktperson ved pressehenvendelser: Pressetelefon, tlf. xx xx xx xx, mail		
Kontaktperson xxx		
Koordination med andre organisationer		
Hvem er det afgørende for departementet at koordinere sine budskaber med? F.eks.: • *Andre myndigheder* • *Eksterne eksperter* • *Interesseorganisationer*		
Beredskabsstyrelsen	Chef for Presse og Kommunikation: xx, telefon:	
XX	Chef for Presse og Kommunikation: xx, telefon:	

Bilag 18: Kontaktoplysninger på beredskabsansvarlige på ministerområdet

Kontaktoplysninger på ansvarlige for beredskabsplaner på ministerområde kan finde i dette dokument: Kontaktoplysninger på ansvarlige for beredskabsplaner på ministerområdet

Bilag 19: Kontaktoplysninger på chefer i departementet og på ministerområdet

Kontaktoplysninger på chefer i departementet og på ministerområdet kan findes i dette dokument: Kontaktoplysninger (skærmet adgang)

Bilag 20: Sundhedsstyrelsens beredskabsplan

Sundhedsstyrelsens beredskabsplan kan findes her: Sundhedsstyrelsens beredskabsplan (skærmet adgang)

Bilaget til Sundhedsstyrelsens beredskabsplan kan finde her: Bilag til Sundhedsstyrelsens beredskabsplan (skærmet)

Bilag 21: National krisestyring ved udbrud af pandemisk influenza

Skal udarbejdes.

Bilag 22: Instruks for håndtering af klassificeret information

Håndtering af **klassificeret information** er beskrevet i Cirkulære nr. 10338 af 17/12 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt).

Det er klassifikationsgraden på en konkret information/dokument, der bestemmer, hvordan informationen eller dokumentet skal håndteres/behandles. Sikkerhedscirkulæret har fire klassifikationsgrader:

1) **YDERST HEMMELIGT** anvendes om informationer, hvis videregivelse ville kunne forvolde Danmark eller landene i NATO eller EU **overordentlig alvorlig skade**
2) **HEMMELIGT** anvendes om informationer, hvis videregivelse ville kunne forvolde Danmark eller landene i NATO eller EU **alvorlig skade**
3) **FORTROLIGT** anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO eller EU-skade
4) **TIL TJENESTEBRUG** anvendes om informationer, der **ikke må offentliggøres eller komme til uvedkommendes kendskab.**

Alle chefer og medarbejdere, der er sikkerhedsgodkendt i departementet, er som udgangspunkt godkendt til **HEMMELIGT** (HEM). Når man er sikkerhedsgodkendt til HEMMELIGT (HEM) kan man behandle alle klassificerede informationer til og med HEMMELIGT (dvs. både TIL TJENESTEBRUG, FORTROLIGT og HEMMELIGT).

Departementets sikkerhedsofficerer forestår sikkerhedsgodkendelser af chefer og medarbejdere i samarbejde med Politiets Efterretningstjenestes (PET) Personsikkerhedsafdeling. Departementets sikkerhedsofficerer har en liste over alle sikkerhedsgodkendte medarbejdere, herunder sikkerhedsgodkendelse til hvilken klassifikationsgrad.

Oversigten over sikkerhedsgodkendte medarbejdere kan tilgås her: Sikkerhedsgodkendte medarbejdere i Indenrigs- og Sundhedsministeriet (skærmet adgang).

Hvordan foregår sikkerhedsgodkendelse?
En sikkerhedsgodkendelse er en status, der tildeles for at en person kan få adgang til klassificeret materiale eller -områder efter en personundersøgelse.

Enhver offentlig myndighed træffer afgørelsen om sikkerhedsgodkendelse af ansatte i myndigheden. Sikkerhedsgodkendelsen har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende myndighed. Politiets Efterretningstjeneste (PET) foretager en sikkerhedsundersøgelse til brug for den offentlige myndigheds afgørelse om sikkerhedsgodkendelse af ansatte.

Afgørelsen om sikkerhedsgodkendelser træffes på grundlag af en konkret vurdering af alle de oplysninger, der foreligger om personen. Der lægges særlig vægt på, om den pågældende har udvist ubestridt loyalitet, og om den pågældende har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed ifm. håndtering af klassificerede informationer.

Afgørelsen om sikkerhedsgodkendelse træffes på baggrund af oplysninger, som personen selv giver ved at udfylde et oplysningsskema og de oplysninger, som Politiets Efterretningstjeneste indhenter.

Ansvar og forpligtelser ved sikkerhedsgodkendelse
Når man er sikkerhedsgodkendt i Indenrigs- og Sundhedsministeriet, og dermed kan være modtager af klassificeret information, medfølger ansvar og forpligtelser. Som modtager af klassificerede informationer må man ikke:

- Nedklassificere eller afklassificere informationerne uden udstederens forudgående skriftlige samtykke
- Anvende informationer til andre formål end dem, der evt. er fastsat af udstederen
- 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
- 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.

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

Behandling af klassificerede informationer
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. Kladder, notater og informationsbærende medier, der danner grundlaget for udfærdigelsen af klassificerede informationer, skal efter brugen behandles på samme måde som de klassificerede informationer.

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

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, transporteres i lukket emballage af et dertil særligt udpeget bud eller overdrages på anden betryggende måde. Såfremt informationerne ikke transporteres i lukket emballage, skal de bæres således, at deres indhold er utilgængeligt for uvedkommende.

Klassificerede informationer skal i almindelighed journaliseres straks ved modtagelsen.

Sikkerhedsbrud
Hvis man som medarbejder konstaterer et sikkerhedsbrud, skal man foretage de nødvendige tiltag for at minimere eventuel skade og kontakte sikkerhedsofficererne i Indenrigs- og Sundhedsministeriet.

Såfremt der er tale om risiko for kompromittering af TTJ-informationer, skal man underrette udstederen og i samråd vurdere, om sikkerhedsmyndigheden skal orienteres.

Aktindsigt
Klassificeret materiale er ikke undtaget fra retten til aktindsigt.

Ved anmodninger om aktindsigt vurderes, om klassificeret materiale bør udleveres ud fra de almindelige regler om aktindsigt.

Man skal herunder:
- overveje, om der er oplysninger, der bør undtages fra aktindsigt.
- overveje, om den myndighed, der har udstedt eller videregivet oplysningerne, eller som oplysningerne vedrører, skal høres med henblik på at vurdere, om der er oplysninger, der bør undtages fra aktindsigt. Hvis myndigheden vurderer, at der bør meddeles aktindsigt i klassificerede oplysninger (eller materialer), skal disse oplysninger afklassificeres forinden. Såfremt myndigheden ikke er udsteder af de klassificerede oplysninger, må myndigheden ikke afklassificere oplysningerne uden udstederens forudgående skriftlige samtykke.

Værd at vide om REGNEM og TTJ-licens

Ministeriets **REGNEM-PC** kan bruges til at modtage eller sende e-mails/dokumenter fra/til andre ministeriers REGNEM-PC 'er (kan bruges til mails/dokumenter til og med klassifikationsgraden **HEMMELIGT**).

Når en chef/medarbejder er sikkerhedsgodkendt til HEMMELIGT (HEM) (eller TIL TJENESTEBRUG (TTJ)), skal Center for Service, Sikkerhed og IT bestille en **TTJ-licens** til vedkommende. Herefter sørger Statens IT for sikkerhedshærdning af chefens/medarbejderens PC og giver vedkommende adgang til TTJ-miljøet. Herefter vil den sikkerhedsgodkendte medarbejder kunne sende mails/dokumenter (der er klassificeret **TIL TJENESTEBRUG (TTJ)**) via TTJ-systemet til andre sikkerhedsgodkendte, der er oprettet i TTJ-miljøet. Før der bestilles sikkerhedshærdning af PC og TTJ til en chef/medarbejder, tjekker vi altid, at vedkommende er sikkerhedsgodkendt på tilstrækkeligt niveau.

Klassificerede dokumenter skal altid behandles og opbevares forsvarligt i et aflåst skab eller pengeskab.

Man kan printe TTJ-klassificerede dokumenter på de én af de to TTJ-printere i huset. Den ene TTJ-printer er placeret i Slotsholmsgade 10 i stueetagen i lokale 672, mens den anden er placeret i Slotsholmsgade 12, 3. sal havnefløj i teknikrummet overfor lokale 4038. Printerne skal være aflåst, kontakt en af departementets sikkerhedsofficerer, hvis du har brug for at få adgang til en TTJ-printer.

TIL TJENESTEBRUG (TTJ) klassificerede dokumenter skal makuleres, når de ikke skal bruges længere på én af departementets to godkendte makulatorer til brug for makulering af dokumenter klassificeret som TIL TJENESTEBRUG (TTJ). Den ene makulator er placeret i lokale 672 på Slotsholmsgade 10 i stueetagen, mens den anden makulator er placeret i Slotsholmsgade 12 på 5. sal i Østfløjen i kopirummet midt på gangen. Makulatoren sørger for findeling af kasserede TIL TJENESTEBRUG (TTJ) dokumenter i en sådan grad, at dokumentet ikke vil kunne sættes sammen igen.

Bilag 23: Instruks for håndtering af departementets SINE radioer

Hvornår bruges SINE?
I Indenrigs- og Sundhedsministeriets departement anvendes SINE-radioerne til kommunikation med styrelserne i tilfælde af, at telefonnettet er brudt ned. SINE (**SI**kkerheds**NE**ttet) er Danmarks radionet, der er uafhængigt af det almindelige telenet og internet.

Man behøver **IKKE** være sikkerhedsgodkendt for at bruge radioerne.

Det er ikke tilladt at drøfte klassificeret materiale/oplysninger gennem SINE-radioen af sikkerhedshensyn.

Hvor står SINE-radioerne?
Indenrigs- og Sundhedsministeriet har to radioer. På nuværende tidspunkt er begge SINE-radioer placeret i lokale 6163 på 5. sal på Slotsholmsgade 12.

De to SINE-radioer har følgende telefonnumre (ISSI-nummer):

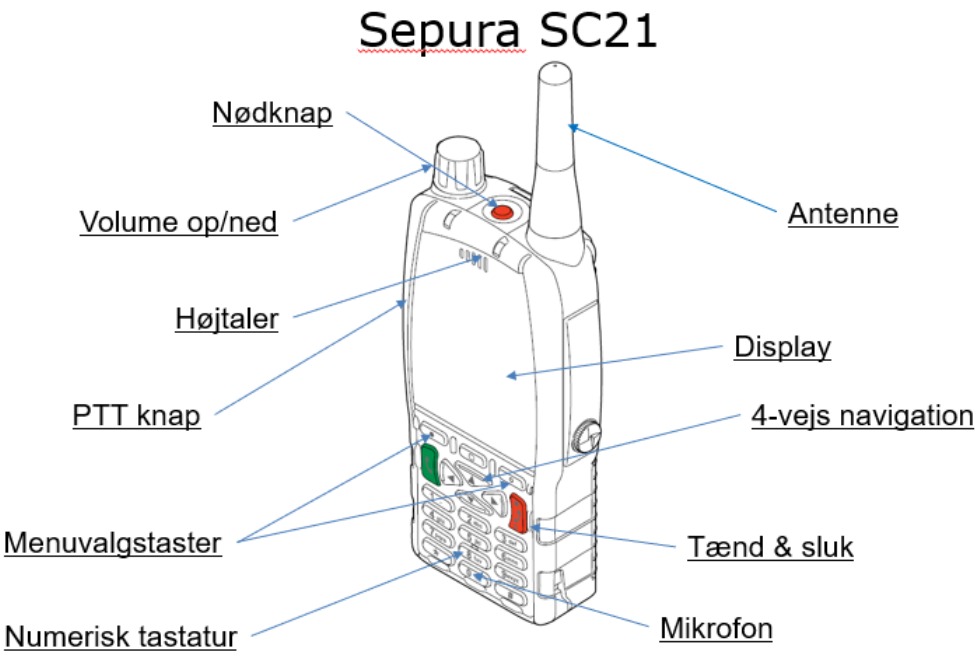
- 7301010
- 7301009

Hvordan bruges SINE-radioerne?
Radioerne bruges til direkte opkald til andre radioer ligesom en almindelig telefon. Et opkald foretages på følgende måde:

1. Radioen er som udgangspunkt tændt og skal forblive tændt efter færdig brug.
2. Hvis radioen er slukket, tændes den ved at holde den røde knap på forsiden af radioen inde. Brug ikke den røde knap på toppen af radioen. Dette er nødopkaldsknappen.
3. Tast modtagerens ISSI-nummer ind.
4. Tryk på den grønne knap på forsiden af radioen for at ringe op.
5. Opkaldet foregår som et opkald på en almindelige telefon. Dvs. at begge parter har mulighed for at tale samtidigt.
6. Hvis du ikke kan høre den anden part, så justeres lydstyrken med drejeknappen på toppen af radioen.
7. Hold opkaldet kort af hensyn til netværkets kapacitet
8. Tryk på den røde knap på forsiden af radioen for at lægge på.

ISSI-numre til Sundhedsstyrelsen og Statens Serum Institut
I tilfælde af et nedbrud på telefonnettet vil det være muligt at kommunikere med Sundhedsstyrelsen og Statens Serum Institut gennem SINE-radio. Sundhedsstyrelsen og Statens Serum Institut kan kontaktes på følgende ISSI-numre.

Sundhedsstyrelsen	**Statens Serum Institut**
5079100	5900912
5079200 (kan kun kontaktes i tilfælde af, at Den Nationalt Operative Stab (NOST) er aktiveret)	5900913
5079300	5900914
	5900915
	5900916
	5900918



Sådan foretager du gruppeopkald

1. På startskærmen skal du trykke på navigationstasterne for at fremhæve den ønskede talegruppe.
2. Tryk på Vælg.
3. Hold PTT knap nede.
4. Vent på taletilladelsestonen (hvis den er konfigureret), og begynd at tale.
5. Slip PTT-knappen for at lytte.

Sådan foretager du private simpleksopkald

1. Indtast et nummer på startskærmen.
2. Tryk på PTT-knappen for at foretage et opkald. Vent på, at den person, du har ringet til, svarer.
3. Når opkaldet er gået igennem, skal du trykke på PTT-knappen og holde den nede for at tale. Vent på taletilladelsestonen (hvis den er konfigureret), Slip PTT-knappen for at lytte.
4. Afslut opkaldet ved at trykke på tasten Afslut.

Bilag 24: TTJ-materiale og SMART TTJ-kommunikation via mobilnettet

Om TTJ-materiale
TTJ er en forkortelse for "TIL TJENESTEBRUG", som er den laveste af de fire klassifikationsgrader, der er beskrevet i Sikkerhedscirkulæret.

TIL TJENESTEBRUG (TTJ) anvendes om informationer, der "*ikke må offentliggøres eller komme til uvedkommendes kendskab*".

Sikkerhedscirkulæret indeholder bl.a. en beskrivelse af de fire klassifikationsgrader, som hedder:
TIL TJENESTEBRUG, FORTROLIGT, HEMMELIGT og YDERST HEMMELIGT

Du skal være sikkerhedsgodkendt, før du må læse og behandle TTJ-klassificerede dokumenter eller informationer.

Du kan se Sikkerhedscirkulæret her: Sikkerhedscirkulæret.

Hvad kan TTJ-platformen bruges til?
I TTJ-miljøet kan du få en mailkonto og dermed en mailadresse, som du skal bruge, når du modtager og sender TTJ-mails.

Der er også adgang til F2-TTJ, som du skal bruge, når du journaliserer dine TTJ-dokumenter. F2-TTJ er opdelt i "søjler". Det betyder, at du kun kan se de dokumenter, der er journaliseret i din egen afdeling.

Hvis du har brug for at modtage, sende eller behandle TTJ-dokumenter i TTJ, skal du først have adgang til TTJ-miljøet. Tal med din chef om behovet og kontakt herefter en af departementets sikkerhedsofficerer og bed om at blive oprettet som bruger i TTJ.

Før bestillingen sendes til Statens It vil vi altid tjekke, at du er sikkerhedsgodkendt.

Departementets interne IT (ISDB & IT) eller departementets sikkerhedsofficerer sender herefter en bestilling til Statens IT vedrørende oprettelse af dig som bruger i TTJ-miljøet samt sikkerhedshærdning af din pc (behandlingstiden for disse bestillinger hos Statens IT er typisk 1–3 dage).

Du modtager herefter e-mails fra Statens IT med oplysning om dels navnet på din nye H-bruger og dels et engangspassword, som du skal bruge, når du logger på TTJ første gang (herefter skal du lave et nyt password, som du selv bestemmer og kender).

Print
Når du skal printe TTJ-dokumenter, skal du bruge én af de to TTJ-printere i huset:
I Slotsholmsgade 10 er TTJ-printeren placeret på stuetagen i lokale 672. Printeren står i det aflukkede rum ved siden af printerrummet. Du får adgang til TTJ-printeren ved at bruge kortlæseren ved siden af døren (brug adgangskort og tast kode).

I Slotsholmsgade 12 er TTJ-printeren placeret på 3. sal i Havnefløjen i teknikrummet overfor lokale 4038. Printeren står i det aflåste teknik-rum for enden af gangen mod Slotsholmsgade. Du skal bruge en nøgle for at komme ind til printeren (kontakt en af departementets sikkerhedsofficerer).

Makulatorer
Når du skal makulere TTJ-dokumenter skal du bruge én af de to TTJ-makulatorer i huset.
I Slotsholmsgade 10 er en makulator placeret i stueetagen i lokale 672.
I Slotsholmsgade 12 er en makulator placeret i printerrummet på 5. sal i Østfløjen.

Makulatorerne sørger for findeling af papiret sådan, at det ikke kan samles igen.

Hvad er SMART?

SMART er en app der kan installeres på iPhone og iPad.

SMART er godkendt til brug for telefonsamtaler, beskeder og videosamtaler klassificeret til TIL TJENESTEBRUG (TTJ).

Udstyr med SMART installeret er ikke klassificeret men skal beskyttes som en personligt værdifuld genstand (pengepung, pas o.l.).

Hvordan bruges appen?
Først skal du tale med din chef om dit behov for at kunne bruge SMART. Herefter kan en af sikkerhedsofficerne kontaktes og du kan bede om, at der bestilles SMART til dig.

Før bestillingen sendes til Statens It, vil vi altid tjekke, at du er sikkerhedsgodkendt, da det er en forudsætning for at få SMART.

Derudover skal brugere af SMART underskrive "Sikkerhedsinstruks for brugere af SMART" forud for ibrugtagning af SMART (bilag 24a).

Bilag 24a: Sikkerhedsinstruks for brugere af SMART

Formålet med denne instruks er at definere de retningslinjer, brugeren skal følge for sikker anvendelse af SMART.

Ved accept og underskrift af indeværende "Sikkerhedsinstruks for brugere af SMART" er brugeren forpligtet til at vedkende sig det fulde ansvar for SMART-enheden, inden ibrugtagning.

Brud på sikkerheden eller mistanke om det, skal uopsætteligt rapporteres til en af departementets sikkerhedsofficerer.

Vær opmærksom på ikke at tale om klassificerede eller følsomme emner, når andre kan overhøre samtalen. Som alternativ kan der kommunikeres via beskeder i SMART.

Ved klassificerede videosamtaler og beskedudvekslinger skal det sikres, at skærmen ikke kan observeres af uvedkommende.

Højtalerfunktionen i SMART-enheden må kun aktiveres hvis det sikres, at samtalen ikke kan overhøres af uvedkommende, og at personel i lokalet er sikkerhedsgodkendt.

Håndfri tale skal foregå med ledningsbaserede headset. Trådløse headset (f.eks. via Bluetooth eller Wifi) må ikke anvendes til klassificerede samtaler.

Endvidere gælder følgende:

- Privacy filter skal være monteret på SMART-enheder og må ikke fjernes
    - Dog med den undtagelse, at iPads som alene anvendes i sikret områder anvendes til møder, ikke behøver privacy filter.
- Telefonbogen er personlig og dedikeret til eget brug ift. arbejdsmæssig funktion. Derfor må enheden eller indhold af telefonbogen ikke deles og ved ændring af arbejdsmæssig funktion, skal dette meddeles til en sikkerhedsofficer i departement.
- Der må ikke tages skærmbilleder af SMART-App eller beskeder, det ligeledes er ikke tilladt at tage skærmbilleder via et eksternt kamera/sekundær enhed.
- SMART-enhed må ikke overdrages til tredje person uden særlig aftale med sikkerhedsofficer
    - Sker dette er det en sikkerhedshændelse, som skal indberettes.
- SMART-enhed skal altid være låst, når den er uden opsyn.
- SMART-enhed må ikke efterlades uden opsyn i det offentlige rum. Skal SMART-enheden være uden opsyn i længere tid, anbefales det at den slukkes.
- Problemer med tilgængelighed af SMART-enhed (f.eks. slettet app, mistet konto, manglende forbindelse) rapporteres til departementets interne IT (ISDB & IT).
- En SMART-enhed skal holdes opdateret for at sikre, at sikkerhedsopdateringer er installeret. I den forbindelse skal SMART-enheden, altid anvende nyeste tilgængelige version af operativsystemet iOS. Dette er brugerens ansvar at dette overholdes.
- Såfremt en bruger konstaterer at have mistet sin SMART-enhed skal dette rapporteres til en af departementets sikkerhedsofficerer. Rapportering skal ske indenfor 24 timer.
- Enhver hændelse eller andre omstændigheder der kan antyde en kompromittering eller mulig kompromittering af samtaler, beskeder eller SMART-App uopsætteligt rapporteres til departementets sikkerhedsofficerer.
- Ved sikkerhedsbrud eller formodet sikkerhedsbrud på SMART-enhed skal denne indleveres til sikkerhedsofficer, som varetager den videre koordination med Styrelsen for Samfundssikkerhed (SAMSIK).
- I tilfælde af at enheden skal til reparation, skal SMART App afinstalleres eller brugerkonto deaktiveres; håndteres ved kontakt departementets interne IT (ISDB & IT).
- Hvis enheden skal bortskaffes, skal SMART App afinstalleres eller brugerkonto deaktiveres; håndteres ved kontakt til departementets interne IT (ISDB & IT).

SMART-enheden skal tilbageleveres såfremt funktion og ansættelsesforhold ikke længere påkræver brug af løsningen. Departementets interne IT (ISDB og IT) sikre korrekt videre håndtering af SMART-enhed iht. udstyrsklassifikation.

Center for Service, Sikkerhed og IT er ansvarlig for, at orienterer brugere af SMART ved væsentlig opdatering af denne instruks ift. nye forhold, instrukser mv. på intranet eller tilsvarende, da der løbende sker opdateringer af SMART-enheden.

Brugere af SMART skal inden ibrugtagning underskrive, at de har læst og er indforstået med indholdet af "Sikkerhedsinstruks for brugere af SMART". Det er departementets sikkerhedsofficerers ansvar at sikre, at brugere underskriver forud for ibrugtagning.

Bilag 25: Drift og overvågning af REGNEM

Under udarbejdelse

Departementet har bestilt egen REGNEM-pc hos Ministeriet for Samfundssikkerhed og Beredskab. Indtil departementets egen REGNEM-pc bliver leveret, så har departementet indgået en aftale med Udlændinge- og Integrationsministeriet om, at vi låner deres REGNEM-pc. Denne REGNEM-pc er placeret i et sikkert REGNEM-rum på adressen Slotholmsgade 10, 2. sal.

Der arbejdes på, at departementet kan få godkendt et eget REGNEM-rum. Dette rum skal godkendes af Styrelsen for Samfundssikkerhed (SAMSIK).

Bilag 26: IT-sikkerhed

Under udarbejdelse.

Ved svigt/nedbrud i IT-systemer

- Kontrollér, om sidemanden samt andre kontorer og afdelinger oplever samme problem.
- Hvis der konstateres et generelt problem kontaktes Statens IT, telefonnr.: 72 31 00 01 og departementets interne IT.

Relevante kontorer i departementet har særlige procedurer for, hvornår IT-beredskabet igangsættes ift. at aktivere IT-leverandørers beredskab og sørge for, at ISM-medarbejdere informeres om hændelse og nødvendige foranstaltninger (eks. igangsættelse af fysisk sagsbehandling, håndtering af fysiske forelæggelser etc.).

Ved længerevarende udfald/nedbrud i IT-systemer

Forelæggelser påføres et omslag, hvorpå der fremgår godkendelsesrækkefølge. Godkenderen påfører underskrift og kommentarer, og er ansvarlig for, at sagen afleveres til den næste i rækkefølgen. Hold en oversigt, over hvilke forelæggelser afdelingen har undervejs, og følg hyppigt op.

Bilag 27: Indenrigs- og Sundhedsministeriets Beredskabsinstruks

Indenrigs- og Sundhedsministeriets beredskabsinstruks kan finde her: Beredskabsinstruks.