INDENRIGS- OG SUNDHEDSMINISTERIET

Indenrigs- og Sundhedsministeriet

Enhed: Informationssikkerhed- og Databeskyttelse

Sagsbeh.: Helga Brask Nielsen

Sagsnr.: 2025 - 9515

Dok. nr.: 9545546

Dato: 04-12-2025

Udvalg for Cyber-, og informationsikkerhed og databeskyttelse (CID-udvalg)

Referat af møde i CID-udvalg d. 11.12.2025

Dato for møde
11.12.2025

Deltagere
Kontorchef Henriette Benzon Bang (HEB), Center for Service, Sikkerhed og IT (CSI)
Enhedsleder Annette Baun Knudsen (ABKN), CSI
Chefkonsulent Lene Jensen (LRJ), IT
Alberte Treiner (ALTR), HR, suppleant for Trine Brøbecher

Observatør
Helle Ginnerup-Nielsen (HGN), koncernfælles DPO for departementet

Ressourcepersoner
Frederik Kastoft-Davidsen (FKD)

Afbud
Afdelingschef Cecilie Louise Svane Olesen (CLSO), 5. afdeling
Kontorchef Trine Brøbecher (TRBR), HR
Chefkonsulent Pernille Seaton (PSE), sikkerhedsofficer

Sekretariat
Specialkonsulent Helga Brask Nielsen (HBN), DPA

Indhold

1. Velkomst

v/HEB

Referat

HEB bød velkommen på vegne af CLSO

2. Referat af CID-udvalgsmøde d. 16. september 2025, herunder justering af beslutning under referatets pkt. 8 vedr. retningslinjer om informationssikkerhed

v/ABKN

Indstilling

Det indstilles, at

- at CID-udvalget godkender referatet fra CID-udvalgsmøde den 16. september 2025.
- at CID-udvalget godkender justering af retningslinjer om informationssikkerhed

Sagsfremstilling

Referat fra CID-udvalgets møde den 16-09-2025 er godkendt i skriftlig proces i F2 uden bemærkninger.

Det blev under referatets pkt. 8 "Forslag til ændring af 'Retningslinjer for medarbejdere i departementet om informationssikkerhed'' bl.a. besluttet at tilføje i retningslinjerne, at der kan sendes ukrypterede mails med fortrolig information mails til LMST. De opdaterede retningslinjer er den 20. oktober sendt til Samarbejdsudvalget men endnu ikke offentliggjort på intranettet.

Statens IT har efterfølgende på et møde i oktober i SIT's mødeforum for DPO'er gennemgået sikkerheden omkring fremsendelse af e-mails til myndigheder, der ikke er SIT-kunder, og på den baggrund har ISDB foretaget en fornyet risikovurdering, der fører til, at der fortsat som teknisk foranstaltning skal anvendes funktionen "send sikkert" ved fremsendelse af mails med fortrolig information til Lægemiddelstyrelsen. Der gives på mødet en mundtlig orientering om risikovurderingen.

Retningslinjerne og referat foreslås i forlængelse heraf opdateret i overensstemmelse hermed, jf. bilag 2.1 og 2.2.

Bilag

Bilag 2.1. Endeligt referat af CID-Udvalgsmøde 16-09-2025
Bilag 2.2. Retningslinjer som godkendt på mødet den 16. september 2025 med markering af ovenstående ændring vedr. fremsendelse af e-mails til LMST.

Videre proces

Med udvalgets godkendelse orienteres Samarbejdsudvalget på ny om retningslinjerne, hvorefter referat og opdateret retningslinje for informationssikkerhed for medarbejdere gøres tilgængeligt på intranettet.

Referat

HGN bemærkede, at det var en stor byrde at pålægge medarbejderne, at de selv skal være opmærksomme på 'send-sikkert'-funktionen.
HGN spurgte ind til, om rettelsen i materialet var begrundet i, at der ikke foreligger en endelig risikovurdering.

ABKN og FKD redegjorde for, at selvom risikovurderingen ikke foreligger endeligt endnu, er den dog så så tæt på at være færdig, at det ikke er udslagsgivende for tilpasningen. Der foreligger pt. kun almindelig tunnelkryptering, hvilket ikke vurderes at være tilstrækkeligt.

ABKN bemærkede, at arbejdet med at kigge på sikkerheden fortsættes, herunder kommunikation med LMST.

HGN bemærkede, at organisatoriske foranstaltninger i form af instrukser til medarbejdere om, at de i nogle tilfælde skal gøre noget andet, end de plejer, som udgangspunkt er svage og derfor ikke nødvendigvis nedbringer sandsynligheden væsentligt.

HEB var enig i betragtningen og bemærkede, at lægemiddelkontoret ligeledes har meget kommunikation med LMST, og at lægemidler er en del af den kritiske infrastruktur. HEB bemærkede derfor, at der også til lægemiddelkontoret, ligesom over for HR, skal informeres specifikt om retningslinjen.

Der pågik derudover en drøftelse vedr. awareness-aktiviteter i relation til nærværende foranstaltning. Herunder at der er i foråret 2026 planlægges igangsat et informationsarbejde vedr. sikkerhed og retningslinjer, også i relation til beredskab generelt.

Beslutning
CID-udvalget godkendte indstillingen, herunder den foreslåede videre proces.

3. CID-udvalget godkendte indstillingen, herunder den foreslåede videre proces. Udmøntning af direktionens beslutning om etablering af Sikkerhedsudvalg

v/ABKN

Indstilling

Det indstilles, at CID-udvalget i forlængelse af direktionens beslutning om etablering af et Sikkerhedsudvalg drøfter og godkender, at Center for Service, Sikkerhed og It (CSI) udarbejder forslag til 1) Kommissorium for Departementets Sikkerhedsudvalg samt 2) forslag til revideret CID-politik, hvorefter begge dokumenter sendes i skriftlig proces i CID-udvalget. Dernæst forelægges DC materialet til endelig godkendelse.

Sagsfremstilling
På direktionens møde den 19. november 2025 blev det drøftet og besluttet at integrere arbejdet med de forskellige områder omkring sikkerhed i departementet i et Sikkerhedsudvalg. Dette flugter med anbefaling fra PET om at etablere et fast mødeforum for alle kontorer, der arbejder med sikkerhed. For ikke at etablere et nyt organisatorisk set-up, men at drage nytte af den eksisterende governance, godkendte direktionen, at der arbejdes videre med at ændre CID-udvalget til også at omfatte spørgsmål om sikkerhed generelt.

Implementering af direktionens beslutning vil indebære:

a) Etablering af et Sikkerhedsudvalg til at afløse CID-udvalget
b) Etablering af et integreret ledelsessystem (ISMS)

Ad A) Etablering af et Sikkerhedsudvalg
Sikkerhedsudvalget skal beskæftige sig med emner indenfor både cyber-, informationssikkerhed, databeskyttelse og fysisk sikkerhed.

Formålet er at sikre, at indsatsen på de forskellige områderne i videst muligt omfang understøtter hinanden.

Jf. indstillingen foreslås det, at CSI udarbejder et forslag til Kommissorium for Sikkerhedsudvalget og sender i skriftlig proces blandt CID-udvalgets medlemmer, hvorefter det forelægges DC til endelig godkendelse.

Ad b) Etablering af et integreret ISMS
Udgangspunktet for Sikkerhedsudvalgets arbejde vil være at fortsætte implementeringen af ledelsessystemet efter ISO 27001-standarden med fokus på, hvordan styringslogikken i standarden kan bidrage til en strømlinet og effektiv styring af den samlede sikkerhed.

Fordelen ved at integrere ledelsessystemet på tværs af sikkerhedsområder er, at styringen og kontrollen med sikkerheden vil følge samme systematik for løbende planlægning, gennemførsel, kontrol og opfølgning.

En integreret tilgang vil sikre en mere robust og holistisk sikkerhedsstruktur, hvilket i sidste ende også vil understøtte arbejdet med at styrke sikkerhedskulturen blandt medarbejderne i departementet.

Dette vil indebære en tilpasning af bl.a. CID-politikken, så politikken som overordnet styringsdokument favner alle relevante områder.

Jf. indstillingen foreslås det, at Center for Service, Sikkerhed og It udarbejder forslag til revideret CID-politik og sender i skriftlig proces blandt CID-udvalgets medlemmer, hvorefter forslaget forelægges DC til endelig godkendelse.

Integrationen på tværs af sikkerhedsområder vil også skulle implementeres i andre relevante styringsdokumenter, herunder vedr. Styring af aktiver. ISDB vil udarbejde forslag til – samt plan for dette.

Videre proces
Med CID-udvalgets godkendelse, vil CSI udarbejde forslag til hhv. Kommissorium for Departementets Sikkerhedsudvalg og forslag til revideret CID-politik og sende begge dele i skriftlig proces i CID-udvalget mhp. godkendelse, hvorefter det forelægges DC til endelig godkendelse.

ISDB vil desuden udarbejde plan for øvrig integration nye sikkerhedsområder i ISMS'et, herunder konkrete forslag til tilpasning af relevante styringsdokumenter.

Bilag
Bilag 3.1. Kommissorium for CID-udvalget
Bilag 3.2. Departementets CID-politik

Referat

HGN bemærkede, at CID-navnet (cyber- informationssikkerhed og databeskyttelse) er velovervejet og tilpasset koncernorganiseringen og anbefalede derfor, at dette bibeholdes i et fremtidigt navn for "Sikkerhedsudvalget".

HGN anbefalede desuden, at "informationskoordinator" og "DPA" indarbejdes i kommissoriet, når det skal opdateres, idet disse funktioner ikke er nævnt i det gældende kommissorium.

HGN spurgte, om der er ulemper eller andre forhold forbundet med integrationen, der bør tages højde for i det videre arbejde. FKD svarede, at det forudsætter justering af relevante styringsdokumenter i ISM's ISMS og PIMS, som pt er under ombygning, hvis det også skal omfatte andre områder end det nuværende.

Beslutning

CID-udvalget godkendte indstillingen, herunder den foreslåede videre proces.
CID-udvalget vil lade anbefalinger fra HGN indgå i det videre arbejde.

4. Status for arbejdet med cyber-, informationssikkerhed og databeskyttelse i 2025 og handleplan for 2026

v/FKD, HBN

Indstilling

Det indstilles, at CID-udvalget godkender

- Status for arbejdet med cyber- informationssikkerhed og databeskyttelse i 2025 (bilag 4.1 og 4.2)
- Udkast til handleplan for cyber- informationssikkerhed og databeskyttelse i 2026 og frem (bilag 4.3)
- Forslag til videre proces

Sagsfremstilling

Det følger af CID-politikkens afsnit 5, at CID-udvalget og departementschefen mindst én gang om året modtager en status på den samlede implementering af ISO27001 og ISO27701, herunder de fire målsætninger i CID-politikken.

ISDB har udarbejdet en samlet status for implementeringen af ISO27001 og ISO27701 i 2025. Det overordnede arbejde med at etablere og modne ledelsessystemet er styrket gennem udvikling og godkendelse af centrale politikker og retningslinjer, herunder på områderne risikostyring, styring af aktiver og hændelseshåndtering.

Der er fortsat enkelte udeståender i implementeringen af styring af aktiver, herunder opdatering af fortegnelser for systemer og processer.

Det bemærkes, at drift og fuld implementering af risiko- og aktivstyring er en betydelig, kontinuerlig og ressourcekrævende opgave for ISDB, CID-udvalget og de aktivejere der er ansvarlige for departementets systemer og processer. Se bilag 4.1. for et overblik over udviklingen af ledelsessystemet og bilag 4.2 for status med arbejdet.

Det fremgår endvidere af CID-politikkens afsnit 5, at CID-udvalget skal udarbejde étårige handleplaner for at realisere målsætningerne og med henblik på at prioritere indsatserne. Som handleplan vedlægges bilag 4.3., som indeholder en oversigt over arbejde i departementet på sikkerhedsområdet med angivelse af, om arbejdet er gennemført samt hvornår arbejdet planlægges gennemført.

Det bemærkes, at ovenstående arbejde afspejler CID-udvalgets ønske om en mere gennemgribende gentænkning af compliance-arkitekturen. ISDB har derfor ikke realiseret alle dele af handleplanen for 2025. Udarbejdelsen af en retningslinje for leverandørstyring samt en retningslinje for adgangsstyring er udskudt til henholdsvis 2026 og 2027. Færdiggørelsen af HR-datakonstruktionen i koncernen er fortsat under udarbejdelse og vil strække sig ind i 2026. ISDB har desuden ikke gennemført en phishingkampagne eller opdateret alle departementets oplysningstekster.

Videre proces
Med CID-udvalgets godkendelse vil statusnotatet (bilag 4.2.) blive forelagt departementschefen til orientering i januar 2026.
ISDB vil fortsætte implementeringen af ledelsessystemet i overensstemmelse med den foreslåede handleplan i bilag 4.3.

Bilag
Bilag 4.1. Overblik over udvikling i ledelsessystemet
Bilag 4.2. Status for arbejdet med cyber-, informationssikkerhed og databeskyttelse i 2025
Bilag 4.3. Gennemført arbejde og handleplan for 2026 og frem

Referat
ABKN orienterede om, at SoA-dokumentet skal opdateres, men at ISDB ikke haft ressourcer til at løfte denne opgave inden CID-udvalgsmødet.
FKD bemærkede, at hver retningslinje indeholder en henvisning til de relevante ISO-foranstaltninger, men at det udestår at blive opdateret i det samlede SoA-dokument.

HGN bemærkede, at det er svært at lave et overblik over det, der mangler, når der ikke foreligger en opdateret version af SoA-dokumentet. Dette også af hensyn til afrapportering til ledelsen ift. prioritering. HGN foreslog desuden, at det også i handleplaner tydeliggøres, f.eks. med rød/gul/grøn-markering, om en given opgave er nået i overensstemmelse med plan.

HGN bemærkede, at der er kommet en ny version af ISO 27001 og anbefalede, at ISDB påbegynder arbejdet ud fra den foreliggende engelske version, i stedet for at afvente den danske oversættelse.

Beslutning

CID-udvalget godkendte indstillingen, herunder den foreslåede videre proces med den tilføjelse, at det i forbindelse med, at statusnotatet forelægges departementschefen også vil fremgå hvilke foranstaltninger, der mangler at blive implementeret.

5. Generel drøftelse af ressourcesituationen i relation til informationssikkerhed

v/ HGN

Punktet er indmeldt af HGN/DPO.

Indstilling

Det foreslås, at udvalget forholder sig til ressourcesituationen på informationssikkerhedsområdet. Der er inden for sidste år sket en reduktion på to årsværk i ISDB-enheden.

Referat

Der blev henvist til drøftelsen under punkt 4. HEB oplyste desuden, at ledelsen er opmærksom på, at der overordnet skal løftes de samme eller flere opgaver inden for den ramme der er, hvilket løbende vil kræve prioritering af opgaver.

Der henvises i øvrigt til beslutning under punkt 4 om, at det i forbindelse med forelæggelse af status for DC skal beskrives, hvilke opgaver der ikke blev nået i 2025.

6. Orienteringspunkter

6a. Implementering af NIS 2-loven

v/ FKD

Indstilling

Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

NIS 2-loven (NIS 2) har været gældende for virksomheder og myndigheder i Danmark siden 1. juli 2025, men med en indfasningsperiode frem til 1. oktober 2025, hvor enheder, der er omfattet af loven, skal registrere sig hos den kompetente myndighed for den pågældende sektor. Styrelsen for Samfundssikkerhed (SAMSIK) er sektoransvarlig myndighed for den offentlige forvaltning, herunder statslige myndigheder som Indenrigs- og Sundhedsministeriet. De kompetente myndigheder skal bl.a. føre tilsyn med efterlevelsen af NIS 2, og SAMSIK's første tilsyn forventes iværksat i 2. kvartal 2026 og ikke i 4. kvartal 2025, som ISDB tidligere har informeret CID-udvalget om.

Det bemærkes, at SAMSIK endnu ikke har offentliggjort deres planlagte vejledning vedr. offentlige myndigheders efterlevelse af NIS 2, og ISDB vurderer, at SAMSIK's tilsyn med departementet først vil blive annonceret efter offentliggørelsen af denne vejledning.

Effektiv implementering af NIS 2 er et større projekt som følge af departementets relativt umodne ISMS, og det må forventes, at en fuld implementering tidligst kan være gennemført ved udgangen af 2027.

ISDB har udarbejdet en implementeringsstrategi, som prioriterer de væsentligste elementer i efterlevelsen, og ISDB har siden 2. kvartal 2025 arbejdet med implementeringen af lovkravene. Overordnet set kan implementeringsstrategien opdeles således:

1. Undervisning af topledelsen i roller og ansvar
2. Implementer NIS 2's krav til risikostyring (Politik for risikostyring, retningslinje for risikostyring, konsekvens- og sandsynlighedstabeller)

3. Fastlæg departementets risikotolerance ift. risiko for samfundet (Workshop vedr. fastlæggelse af risikotolerance, direktionsgodkendelse af risikotolerance på baggrund af udkast udarbejdet på workshop)
4. Implementer NIS 2's krav til hændelseshåndtering (Retningslinje for hændelseshåndtering)
5. Implementer model for klassifikation af, hvilke af departements IT-systemer der er omfattet af NIS2-loven (omfattelsesgrad) (Retningslinje for styring af aktiver, kontekst for ledelsessystemet)
6. Klassificer IT-systemer der er vurderet til at være omfattet af NIS 2 jf. punkt 5
7. Implementer passende krav til foranstaltninger (Emnespecifikke politiker og retningslinjer jf. SAMSIK's vejledning til implementering af cybersikkerhedsforanstaltninger)
8. Kontinuerlig forbedring af implementerede foranstaltninger og styringsdokumenter. ISDB bemærker, at gennemførslen af overordnede implementeringsplan også medvirker til den dokumenterbare efterlevelse af ISO 27001:2023 og ISO 27701:2019.

Det bemærkes. at punkt 6-8 er ressourcekrævende opgaver for ISDB og de aktivejere, hvis systemer er omfattet af NIS 2.

Videre proces

ISDB har ved udgangen af 2025 gennemført punkt 1-5, og vil i 2026 fortsætte arbejdet med punkt 6-8.

Referat

CID-udvalget tog orienteringen til efterretning, herunder den videre proces.

6b. Campus

v/HBN Indstilling

Der indstilles, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling

På CID-udvalgsmødet i december 2024 blev det besluttet, at ISDB skulle udarbejde en liste over hvilke medarbejdere der har og ikke har gennemført de Campus-kurser, der blev besluttet at gøre/fastholde obligatoriske på CID-udvalgsmødet i maj 2024. Det blev besluttet, at listen skal fremlægges på det sidste CID-udvalgsmøde i 2025.
Det drejer sig om følgende kurser:

- Introduktion til databeskyttelse (fastholdt som obligatorisk)
- Cyber- og informationssikkerhed for medarbejdere i staten (fastholdt som obligatorisk)
- Cyber- og informationssikkerhed for leder og topledere i staten (nyt obligatorisk)

ISDB har været i dialog med Koncernprogrammer med henblik på at udarbejde listen. Desværre viser det sig, at der er en fejl i Campus ift. endelig registrering af kurserne som gennemført.

Koncernprogrammer har fejlmeldt hos- og følger op med Campus.

Der gives en mundtlig orientering om status samt eventuelle løsningsmuligheder.

Referat

HBN orienterede om, at der, via KOP, har været en længere dialog med Campus, da de lister, de indtil nu har fremsendt, ikke er retvisende.

ALTR bemærkede, at HR generelt også er interesseret i, at listen over hvem der har gennemført Campuskurser er korrekt.

HBN orienterede om, at dialogen, via KOP, med Campus fortsætter med henblik på, at finde en god løsning. Der var en generel drøftelse af, hvilken effekt organisatoriske foranstaltninger i form af

kurser om sikkerhed har i forhold til departementets generelle informationssikkerhed. Dette skal tages med i de videre overvejelser om, hvor mange ressourcer der skal bruges på at følge op på medarbejdernes gennemførsel af kurser.

CID-udvalget tog i øvrigt orienteringen til efterretning.

6c. Sikkerhedshændelser og afvigelser

v/HBN

Indstilling

Det indstilles til, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling

Der føres et register over sikkerhedshændelser (både med og uden brud på persondatasikkerheden). Det er nu udvidet med en registrering af afvigelser, jf. retningslinje om hændelseshåndtering.

Der afrapporteres derfor nu i begge kategorier. I bilag 6c.1. er der et uddrag af hhv. sikkerhedshændelser og afvigelser der er registreret siden forrige CID-udvalgsmøde.

Videre proces

På baggrund af, at der har været to afvigelser i relation til afholdelse af konferencer, planlægges der udarbejdelse af en vejledning til overholdelse af persondataretlige regler og retningslinjer med relation hertil.

Bilag

Bilag 6c.1. Uddrag af log over sikkerhedshændelser og afvigelser.

Referat

CID-udvalget tog orienteringen til efterretning.

6d. Mødeplan 2026

v/HBN

Indstilling

Det indstilles til, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling

Følgende datoer er fastsat for CID-udvalgsmøderne i 2026.

Fredag d. 27. marts 2026

Torsdag d. 18. juni 2026

Torsdag d. 17. september 2026

Onsdag d. 16. december 2026

Referat

CID-udvalget tog orienteringen til efterretning.

HEB bemærkede, at hun er mødeleder til mødet i marts måned grundet Cecilies barsel.