INDENRIGS- OG SUNDHEDSMINISTERIET

Indenrigs- og Sundhedsministeriet

Enhed: Informationssikkerhed- og Databeskyttelse
Sagsbeh.: HBN
Sagsnr.: 2026 - 513
Dok. nr.: 9874315
Dato: 02-06-2026

Udvalg for Cyber-, og Informationsikkerhed og Databeskyttelse (CID-Udvalg)

Referat af møde i CID-udvalg 1-2026

Dato for mødet
29. april 2026

Deltagere
Henriette Benzon Bang (HEB), Kontorchef CSI, forperson
Annette Baun Knudsen (ABKN), Enhedsleder ISDB&IT, CSI
Trine Brøbecher (TRBR), Kontorchef HR
Pernille Seaton (PES), Chefkonsulent, CSI
Lene Jensen (LRJ), Chefkonsulent IT, CSI

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

Ressourcepersoner
Frederik Kastoft-Davidsen (FKD), Chefkonsulent, ISDB, CSI
Camilla Heering Elong (CHE), Fuldmægtig, CSI

Sekretariat
Helga Brask Nielsen, DPA, ISDB, CSI

Indhold

1. Velkomst

v/HEB

Referat

HEB bød velkommen.

2. Referat af CID-udvalgsmøde d. 11. december 2025

v/HEB

Indstilling

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

Sagsfremstilling

Referatet er godkendt i skriftlig proces i december og er nu tilgængeligt på intranettet.

Informationssikkerhedsudvalg (CID)

Bilag

Bilag 2. Referat af CID-Udvalg den 11.12.2025

Beslutning

CID-udvalget tog orienteringen til efterretning.

3. Status på arbejdet med beredskabsplan, herunder it-beredskabsplan

v/CHE og HEB

Indstilling

Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

På CID-udvalgsmødet gives en mundtlig status på arbejdet med beredskabsplanen:

I forbindelse med arbejdet omkring styrkelse af departementets sikkerhedsorganisation har direktionen i november 2025 besluttet, at ISM's beredskabsplan skal opdateres.

Den opdaterede beredskabsplan og dertilhørende bilag blev forelagt og godkendt med enkelte bemærkninger på direktionsmødet den 21. april 2026.

Formålet med opdateringen af beredskabsplanen er at opdatere planen efter departementets aktuelle organisation og gøre den lettere at anvende i tilfælde af en trussel, hændelse eller krise. Beredskabsplanen er bl.a. sprogligt forenklet, instruktioner knyttet til beredskabsplanen er lagt i et separat bilag, og skabelonerne i instruktionerne er forenklede. Endvidere har det været et formål at tydeliggøre, hvilken rolle direktionen og andre relevante beredskabsmedarbejdere skal varetage i tilfælde af en trussel, hændelse eller krise.

ABK giver herefter en mundtlig status på it-beredskabsplanen.

Den opdaterede beredskabsplan og de tilhørende bilag er vedlagt t.o.

Videre proces

Efter direktionens bemærkninger til beredskabsplanen på direktionsmødet den 21. april 2026 er blevet inkorporeret, er beredskabsplanen lagt til departementschefen med henblik på underskrift.

CSI arbejder på de næste skridt mhp. at styrke ISM's sikkerhedsorganisation, herunder den fysiske sikkerhed og kommunikationsinfrastruktur samt kommunikation om den opdaterede beredskabsplan. Dette arbejde fortsætter, og der forventes udrullet initiativer og kampagner mhp. at informere om den opdaterede beredskabsplan og styrkelse af ISM's sikkerhedsorganisation frem til og med slutningen af sommeren. CID-udvalget vil løbende blive orienteret om arbejdet med at styrke ISM's sikkerhedsorganisation og vil blive forelagt eventuelle handleplaner.

Bilag

Bilag 3.1. Beredskabsplan for Indenrigs- og Sundhedsministeriets departement (den version som ligger til DC's underskrift).

Bilag 3.2. Bilag til Beredskabsplan for Indenrigs- og Sundhedsministeriets departement (den version som ligger til DC's underskrift).

Referat

HGN spurgte om, hvorvidt der var taget højde for, at en beredskabssituation også kan betyde længerevarende strøm og /eller systemnedbrud. I sådanne situationer er det væsentligt, at have relevant materiale i fysisk form.

CHE oplyste, at der er taget højde for disse forhold i beredskabsarbejdet. Eksempelvis er der printet fysiske beredskabsplaner og dertilhørende bilag.

CID-udvalget tog orienteringen til efterretning.

4. AI-retningslinjer/ChatGPT

v/ABK

Indstilling

Det indstilles, at CID-udvalget godkender endelig version af retningslinjerne.

Sagsfremstilling

I marts 2026 fik CID-udvalget de nye retningslinjer for anvendelse af generativ AI i form af ChatGPT.

Der er siden CID-udvalgets godkendelse i marts 2026 sket en yderligere tilpasning af retningslinjerne.

De konkrete ændringer vil blive gennemgået på mødet.

Bilag

Bilag 4. Endelig version af retningslinjerne

Referat

ABKN bemærkede, at retningslinjerne forelægges til godkendelse med forbehold for, at der vil kunne ske ændringer i retningslinjerne efter forelæggelse af risikovurderingen og efterlevelsestjekket for direktionen. I det tilfælde vil retningslinjerne blive sendt til skriftlig godkendelse på ny hos CID-udvalgets medlemmer.

ABKN bemærkede desuden, at der også er udarbejdet en vejledning, der instruerer i korrekt konfigurering af ChatGPT.

HEB præciserede, at der blandt andet er sket en tydeliggørelse af hvordan og hvornår ChatGPT må bruges i departementets arbejde. FKD bemærkede, at det var tillige en præcisering af hvilken generativ AI, der må anvendes.

HGN bemærkede, at arbejdet med risikovurderingen og legalitetsvurderingen kan ende med, at der må tages forbehold for lovlighed. HGN bistår med rådgivning i arbejdet med risikovurderingen og legalitetsvurderingen.

TRBR spurgte, om hvorvidt det er tilladt at påbegynde ibrugtagelse af ChatGPT Business. Der blev oplyst, at der ikke er givet tilladelse til at ibrugtage ChatGPT Business i departementet endnu.

Beslutning

CID-udvalget godkendte retningslinjerne med de fremlagte forbehold.

5. Status på arbejde med informationssikkerheden og databeskyttelse

v/FKD

Indstilling

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

Sagsfremstilling

I afsnit 5 i CID-politikken fremgår det, at CID-udvalget skal udarbejde étårige handleplaner for at realisere målsætningerne i arbejdet med informationssikkerhed med henblik på at prioritere indsatserne.

På CID-udvalgsmødet i december 2025 præsenterede ISDB-status for arbejdet med informationssikkerhed og databeskyttelse i 2025 samt handleplan for 2026. På mødet bemærkede DPO HGN bl.a., at formatet for status og handleplan og manglende opdatering af SoA-dokument gjorde det svært at danne sig et overblik over det, der mangler af blive udført i løbet af året.

ISDB har i forlængelse heraf arbejdet med et nyt format for handleplan, der kan bruges til at give status over, om planlagte opgaver udføres i overensstemmelse med handleplanen eller udskydes, men som også kan bruges til prioritering af opgaver.

Formatet for handleplanen er fortsat under udarbejdelse. SOA-dokumentet vil ligeledes blive opdateret.

Status for de væsentligste opgaver inden for hvert emne vil blive gennemgået på mødet, herunder de opgaver, som er udskudt som følge af ændrede prioriteringer i forhold til den fremlagte plan på CID-udvalgsmødet i december 2025.

Bilag

Bilag 5. Handleplan.

Bilaget opdateres frem mod mødet og opdateret version medbringes i print på mødet.

Beslutning

CID-udvalget tog orienteringen til efterretning.

HBN eftersender handleplanen, der blev udleveret i print på mødet, til HGN pr. mail.

6. Ændringer i sikkerhedscirkulæret

v/PSE

Indstilling

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

Sagsfremstilling

Ministeriet for Samfundssikkerhed og Beredskab har opdateret sikkerhedscirkulæret, med ikrafttrædelse den. 1. marts 2026, og har i den forbindelse orienteret alle statslige myndigheder den 3. marts 2026 om ændringerne.

Opdateringen betyder, at det nu er muligt, at "overtage" en sikkerhedsgodkendelse fra en anden myndighed.

I orienteringen fra SAMSIK om opdateringen fremgår følgende:

- at en myndighed fremover har mulighed for at træffe afgørelse om at sikkerhedsgodkende en person på baggrund af en allerede gældende sikkerhedsgodkendelse og dermed uden at anmode Politiets Efterretningstjeneste om en ny sikkerhedsundersøgelse.
- at en anmodning om at forny en allerede gældende sikkerhedsgodkendelse fremover suspenderer udløbet af den pågældende sikkerhedsgodkendelse i op til 12 måneder.

Betydningen for Indenrigs- og Sundhedsministeriet

CSI skal udarbejde en beskrivelse af, i hvilket tilfælde det vil give mening at overtage en sikkerhedsgodkendelse. Der er dialog med ISDB med henblik på at kortlægge hvordan personoplysninger behandles ifm. sikkerhedsgodkendelser. CSI/ISDB vil i forlængelse heraf i samarbejde med HR opdatere oplysningsteksten til medarbejdere. Ændringerne i sikkerhedscirkulæret vil indgå i arbejdet.

Departementets HR-afdeling er orienteret om ændringerne i sikkerhedscirkulæret.

Referat

Der blev drøftet, om der er behov for at udarbejde retningslinjer for, hvornår man skal sikkerhedsgodkendes i departementet. På nuværende tidspunkt sker det ud fra en konkret vurdering.

Beslutning

CID-udvalget tog orienteringen til efterretning.

7. Orienteringspunkter

7a. Awareness campuskurser

v/HBN

Indstilling
Det 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 et senere CID-udvalgsmøde i 2025. Det drejer sig om følgende kurser:

- Introduktion til databeskyttelse

- Cyber- og informationssikkerhed for medarbejdere i staten

- Cyber- og informationssikkerhed for ledere og topledere i staten (obligatorisk siden 2024)

ISDB har været i dialog med Koncernprogrammer (KOP) om udarbejdelse af lister over, hvilke medarbejdere der mangler at gennemføre de obligatoriske kurser.

KOP har som et supplement til listerne lagt en nyhed på intranettet med opfordring til, at alle får færdiggjort evt. åbne obligatoriske e-leaningskurser i Campus.

Næste runde af de obligatoriske e-learningskurser bliver rullet ud 1. oktober 2026.

På næste CID-udvalgsmøde i juni måned vil CSI komme med et oplæg til drøftelse af, hvor ofte ledere og medarbejder skal tilmeldes de obligatoriske e-learningskurser om informationssikkerhed og databeskyttelse og hvordan der skal ske opfølgning på, at de enkelte gennemfører disse.

Bilag

Bilag 7.a. Intranetnyhed om campus.

Referat
CID-udvalget tog orienteringen til efterretning.

TRBR tilbød forud for næste møde, at HR og KOP udarbejder en kort beskrivelse af, hvilke lister der kan trækkes. HR og KOP er desuden ved at undersøge, om det er muligt kun at sende påmindelser til de medarbejdere, som mangler at gennemføre kurser, samt hvordan evalueringspåmindelser for tidligere gennemførte kurser kan håndteres.

7b. Tilsyn med departementets informationssikkerhed og databeskyttelse

v/HBN

Indstilling

Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

Departementet gennemgår årligt et tilsyn med informationssikkerhed og databeskyttelse, som gennemføres af Deloitte.

Der føres tilsyn med perioden 2025. Deloitte har fremsendt en spørgeramme, og departementets frist for besvarelsen af spørgerammen er den 6. maj 2026.

Tilsynet med departementet følger samme tilsynskoncept, som bliver ført af departementet i styrelserne. Departementet er underlagt tilsynskoncept 1, som tager udgangspunkt i institutionens efterlevelse af Styrelsens for Samfundssikkerheds[1] modenhedsmåling, der er baseret på ISO 27001-standarden med den tilføjelse, at udvalgte ISO 27701-foranstaltninger er tilføjet.

Tilsynsemnerne for 2025 omhandler følgende områder fra Modenhedsmålingen: 1. Kontekst (ISO27001 kap. 4.) 5. Drift (ISO27001 kap. 8.), 7. Løbende evaluering (ISO27001 kap. 10.)

Tilsynet vedr. databeskyttelse omfatter departementets efterlevelse af følgende to styringsmål:

- ISO 27701 - A.7.5 Deling, overførsel og videregivelse af personoplysninger - Dataansvarlig
- ISO 27701 - B.8.5 Deling, overførsel og videregivelse af personoplysninger – Databehandler

Der vil være en del af tilsynsemnerne, der har sammenhæng med departementets fortegnelser over behandlingsaktiviteter og systemlister. Fortegnelsesprojektet har været i proces siden september 2024 og er endnu ikke færdiggjort, jf. punkt 7.c. Det forventes derfor, at der i forbindelse med tilsynet vil komme bemærkninger hertil.

Resultaterne fra tilsynet vil blive afrapporteret på næste CID-udvalgsmøde.

Referat
CID-udvalget tog efterretningen til orientering.

7c. Fortegnelsesprojekt

v/HBN

Indstilling
Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

Der gives en status på projektet på mødet.

Departementet er som dataansvarlig forpligtet til at føre fortegnelser over departementets behandlingsaktiviteter. Både Indenrigsdelen og SUM-delen har fortegnelser, men navnlig i forhold til SUM-delen er der behov for en opdatering for at sikre, at fortegnelserne er retvisende. Arbejdet med at opdatere fortegnelserne er påbegyndt i januar 2025, hvor ISDB modtog tilbagemeldinger fra alle kontorer i huset med oplysninger om deres behandlingsaktiviteter ISDB er pt. i gang med at samle op på disse tilbagemeldinger, hvor det er nødvendigt. Det vil sige, at visse behandlingsaktiviteter kræver yderligere afklaring.

Referat

FKD præciserede, at punktet vedrører de fortegnelser, som departementet er forpligtet til at føre efter databeskyttelsesforordningens regler, ikke NIS 2-logvningen, som også stiller krav til fortegnelser. CID-udvalget tog efterretningen til orientering.

7d. Implementering af AI i departementet

v/HEB og ABKN

[1] Tidligere Digitaliseringsstyrelsen

Indstilling

Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

Der gives en mundtlig status på mødet.

Direktionen har besluttet, at der skal implementeres tre AI-løsninger i departementet: ChatGPT, Karnovs AI-løsning Kaila og SIT-GPT/STAT-GPT. Dette er blevet meldt ud både på husmødet og på chefmøder. Arbejdet med implementering af AI-løsningerne er påbegyndt. Projektet er forankret i CSI i en projektorganisering bestående af medarbejdere i ISDB & IT samt CSI. Udvalgte fagkontorer vil desuden blive inddraget som pilotkontorer.

Referat

ISDB orienterede om, at status er, at der arbejdes med legalitets- og risikovurderinger af ChatGPT og KAILA. Der arbejdes også på, hvordan departementet kan forberede sig på STAT- GPT bedst muligt.

HGN bemærkede, at AI og andre cloud-løsninger normalt kræver, at der er passende governance på plads, herunder kan det være nødvendigt systematisk at overvåge, om leverandøren udruller ændringer af betydning for databeskyttelse og informationssikkerhed uden forudgående varsel, som det f.eks. er set ift. MS Copilot via SIT.

TRBR bemærkede, at der skal være et fokus på kompetenceudvikling af departementets medarbejdere indenfor AI. HEB oplyste, at det er et opmærksomhedspunkt blandt arbejdsgruppen der beskæftiger sig med AI i departementet. TRBR fremhævede, at HR gerne ville understøtte arbejdet med kompetenceudvikling indenfor AI.

CID-udvalget tog efterretningen til orientering.

7e. Sikkerhedshændelser, databrud og afvigelser

v/HBN

Indstilling

Det indstilles, at orienteringen tages til efterretning.

Sagsfremstilling

I perioden fra medio december 2025-medio april 2026 har der været 7 sikkerhedshændelser, hvor 3 af dem har medført et brud på persondatasikkerheden. Et af dem blev anmeldt til datatilsynet.
Der er derudover noteret to afvigelser i samme periode.

Sikkerhedshændelser vil blive gennemgået på mødet. Hvor også de handlinger, der evt. er blev iværksat, eller planlægges iværksat, på baggrund af sikkerhedshændelserne eller afvigelserne, også bliver gennemgået

Bilag

Bilag 7.e. Uddrag af log over sikkerhedshændelser, databrud og afvigelser

Referat

CID-udvalget tog efterretningen til orientering.

8. Næste møde

v/HEB

Næste møde afholdes torsdag d. 18. juni kl. 12.30-14.00, hvor bl.a. beslutningen om at inddrage sikkerhed i CID-udvalget vil blive drøftet yderligere.