INDENRIGS- OG SUNDHEDSMINISTERIET

Enhed: Informationssikkerhed- og Databeskyttelse
Sagsbeh.: hbn
Koordineret med:
Sagsnr.: 2025 - 7838
Dokumentnr.: 9277222
Dato: 21-10-2025

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

Referat for møde i CID-udvalg 3-2025

Dato for møde
16. sep. 2025

Deltagere
Annette Baun Knudsen (ABKN), ISDB&IT
Trine Brøbecher (TRBR), HR
Pernille Seaton (PES), Intern Administration
Lene Jensen (LRJ), IT

Observatør
Helle Ginnerup-Nielsen (HGN), DPO

Ressourcepersoner
Frederik Kastoft-Davidsen (FKD), ISDB

Sekretariat
Helga Brask Nielsen (HBN), DPA

Afbud
Cecillie Louise Svane Olesen (CLSO), Afdelingschef 5. afdeling, forperson - afbud

Indhold

1. Velkomst
v/CLSO

ABKN bød velkommen på vegne af Cecilie.

2. Referater vedr. CID-udvalgsmøder d. 20. marts og d. 29. august 2025
v/CLSO

Indstilling
Det indstilles, at CID-udvalget
- tager orienteringen til efterretning vedr. referatet af 20. marts 2025
- godkender udkast til referat af møde d. 29. august 2025.

Sagsfremstilling:
Referat fra CID-udvalgets møde den 20-03-2025 er godkendt i skriftlig proces i F2. Referatet blev godkendt uden bemærkninger og er efterfølgende gjort tilgængeligt på ISM's intranet Informationssikkerhedsudvalg (CID) (Stien er som følger på Intranettet: Forside → Organisation → Informationssikkerhed / CID-udvalg).

Udkast til referatet af CID-udvalgsmødet d. 29. august 2025 er vedlagt.

Videre proces
Med udvalgets godkendelse vil referatet fra mødet d. 29. august 2025 blive offentliggjort på intranettet.

Bilag
Bilag 2.1. – Udkast til 'Referat af CID-udvalgsmøde 29-08-2025'

Beslutning
Udvalget godkendte referatet.

3. Gennemgang og drøftelse af kontekst for ledelsessystemet
v/FKD

Indstilling

Det indstilles, at CID-udvalget
- drøfter og kvalificerer udkast til kontekst for ledelsessystemet, herunder om de beskrevne hovedopgaver er dækkende.
- godkender den videre proces.

Sagsfremstilling
ISDB har udarbejdet et udkast til dokumentet kontekst for ledelsessystemet (Bilag 3.1.), der indgår som en del af departementets ledelsessystem.

Det er et krav ifølge NIS 2-loven og best practice, at kontekst for ledelsessystemet godkendes af den øverste ledelse, dvs. direktionen.

Dokumentet fastlægger, i hvilken grad departementets ledelsessystem som minimum skal forholde sig til efterlevelse. Det beskriver kontraktmæssige og lovgivningsmæssige krav samt krav og forventninger fra relevante interessenter og myndigheder.

I udkastet beskrives desuden departementets hovedopgaver, som danner rammen for omfanget af ledelsessystemet, og som vil blive anvendt som udgangspunkt for vurderingen af, i hvilket omfang NIS 2-loven gælder for departementets systemer. ISDB har indtil videre identificeret følgende hovedopgaver:

Administrative opgaver

- HR-administration
- Koncernadministration og -rådgivning
- IT-administration, inkl. CID-arbejdet
- departementets økonomi

Forvaltningsopgaver

- Borgerhenvendelser
- Valghandlingen
- Aktindsigt
- Tilsynsopgaver
- Kommunale og regionale tilskudsordninger
- Afgørelser overfor myndigheder og kommuner

Udvikling og gennemførelse af politik

- Politikudvikling og implementering
- Lovforberedende arbejde

Det foreslås, at udvalget drøfter, hvorvidt disse hovedopgaver samlet set giver et fyldestgørende billede af departementets virke, samt om de er tilstrækkeligt præcist beskrevet i relation til ledelsessystemet.

Det bemærkes, at kontekst for ledelsessystemet understøtter alle departementets styringsdokumenter, herunder retningslinjen for risikostyring, retningslinjen for styring af aktiver og retningslinjen for hændelseshåndtering. Sammenhængen mellem dokumenterne er illustreret i bilag 3.2.

Styringsdokumentet i sig selv forventes ikke at medføre et ressourcetræk for departementet.

Videre proces

På baggrund af CID-udvalgets drøftelse vil ISDB tilrette dokumentet med henblik på efterfølgende godkendelse af direktionen i forbindelse med den planlagte interne undervisning i NIS 2 og cybersikkerhed i efteråret.

Bilag
Bilag 3.1. – Kontekst for ledelsessystemet – Udkast
Bilag 3.2. – Overblik over implementering af styring af aktiver og hændelseshåndtering

Beslutning

CID-udvalget bidrog med flere bemærkninger til definitionen af hovedopgaver i kontekst for ledelsessystemet. Bemærkningerne er indarbejdet af ISDB og fremgår med TC af opdateret bilag 3.1, som er vedlagt referatet.

CID-udvalget godkendte videre proces.

4. Godkendelse af retningslinje for styring af aktiver

v/FKD

Indstilling

Det indstilles, at CID-udvalget

- godkender udkast til retningslinje for styring af aktiver
- godkender den videre proces.

Sagsfremstilling

Retningslinje for styring af aktiver (Bilag 4.1) er en udmøntning CID-politikken og beskriver departementets krav til klassifikation, styring og dokumentation af aktiver på informationssikkerheds- og databeskyttelsesområdet.

Retningslinjen omfatter følgende aktivtyper:

- Hovedopgaver
- Processer
- Systemer

Retningslinjen fastsætter metode, roller og ansvar for styring af aktiver, herunder decentralt aktivejerskab, samt krav til proces-, system- og hovedopgaveejere. Formålet er at sikre, at departementets aktiver er korrekt klassificeret og dokumenteret i overensstemmelse med gældende lovgivning og standarder (ISO/IEC 27001:2023, ISO/IEC 27701:2019, GDPR samt NIS 2).

Retningslinjen beskriver, hvordan aktiver skal håndteres i hele deres livscyklus – fra identifikation og etablering til drift, vedligehold samt nedlukning og afskaffelse. Derudover redegør den for krav om risikostyring, legalitetsvurderinger, leverandørstyring og konsekvensvurderinger i relation til GDPR og NIS 2.

Det bemærkes, at retningslinjen understøtter departementets styringsdokumenter, herunder retningslinjen for risikostyring og retningslinjen for hændelseshåndtering. Sammenhængen mellem dokumenterne er illustreret i bilag 3.2.

Efterlevelse af retningslinjen forventes at medføre et ressourcetræk for ISDB og IT samt for aktivejere i departementet.

Den videre proces

Retningslinjen for styring af aktiver vil efter godkendelse blive offentliggjort på intranettet.

ISDB vil etablere de processer og registre, der afledes af retningslinjen, holde dem ajourført samt påbegynde implementeringen af den kontinuerlige drift, som retningslinjen foreskriver.

Bilag

Bilag 4.1. – Retningslinje for styring af aktiver - Udkast

Referat

TRBR fremhævede nødvendigheden af tydeligt at formidle kravene i nærværende retningslinje til aktivejere i forbindelse med implementeringen, da der er en risiko for, at de ikke er bekendte med deres ansvar i henhold til retningslinjen.

ANBK svarede, at ISDB, ligesom med retningslinjen for risikostyring, der blev godkendt på sidste CID-udvalgsmøde, er bevidste om denne problemstilling, og at et større udviklingsarbejde med informationssikkerhedssiden på intranettet er under opbygning.

FKD supplerede med, at ISDB vil udarbejde en one-pager, der beskriver aktivejernes ansvar i et let forståeligt sprog, som kan udleveres, når aktivejerne identificeres.

Beslutning

Udvalget godkendte 'retningslinje for styring af aktiver', herunder at konsekvenstærsklen vedr. klassifikation, der definerer hvorvidt departementets systemer er omfattet af NIS 2, indføres i retningslinjen efter godkendelse af direktionen.

5. Godkendelse af retningslinje for hændelseshåndtering

v/FKD

Indstilling

Det indstilles, at CID-udvalget

- godkender retningslinje for hændelseshåndtering.
- godkender den videre proces.

Sagsfremstilling

Retningslinjen for hændelseshåndtering (Bilag 5.1.) er en udmøntning af CID-politikken og beskriver departementets krav til håndtering af sikkerhedsbegivenheder, informationssikkerhedshændelser, databrud og afvigelser. Retningslinjen fastlægger metode, roller og ansvar i relation til identifikation, evaluering, håndtering og dokumentation af hændelser på informationssikkerheds- og databeskyttelsesområdet.

Retningslinjen sikrer, at departementet efterlever de regulatoriske krav i GDPR og NIS 2, herunder anmeldelses- og underretningspligter over for Datatilsynet og relevante myndigheder. Den beskriver desuden processer for klassificering af hændelser, risikovurdering i forbindelse med databrud samt væsentlige hændelser under NIS 2.

Retningslinjen omfatter fire typer hændelser: sikkerhedsbegivenheder, der indikerer en potentiel afvigelse fra politikker eller foranstaltninger; informationssikkerhedshændelser, hvor fortrolighed, integritet, tilgængelighed eller autenticitet kompromitteres; databrud, hvor personoplysninger tilintetgøres, ændres eller videregives uautoriseret; samt afvigelser, hvor regulatoriske eller interne krav ikke efterleves tilstrækkeligt.

Retningslinjen omfatter ligeledes en struktureret tilgang til afledte handlinger på baggrund af læring fra hændelseshåndtering. Handlingerne omfatter: 1) iværksættelse af awarenessaktiviteter vedrørende hændelser, 2) risikostyring af aktiver med henblik på implementering af tilstrækkelige foranstaltninger samt 3) iværksættelse af ad hoc-audits med henblik på identifikation af lignende hændelser.

Retningslinjen understøtter departementets styringsdokumenter, herunder retningslinjen for risikostyring og retningslinjen for styring af aktiver. Sammenhængen mellem dokumenterne er illustreret i bilag 3.2.

Efterlevelse af retningslinjen forventes at udgøre et ressourcetræk for ISDB og IT samt for aktiv- og risikoejere i departementet.

Den videre proces

Retningslinjen for styring af aktiver vil, efter godkendelse, blive offentliggjort på intranettet.

ISDB vil etablere de processer, der afledes af retningslinjen, samt påbegynde implementeringen af den kontinuerlige drift, som retningslinjen foreskriver

Bilag

Bilag 5.1. – Retningslinje for hændelseshåndtering – Udkast

Referat

FKD forklarede, at retningslinjen ud over den lovpligtige håndtering af sikkerhedshændelser også etablerer en struktureret tilgang til håndtering af afvigelser. Afvigelser er hændelser, hvor departementet konstaterer manglende efterlevelse af et lovkrav, en retningslinje eller en politik.

TRBR spurgte ind til baggrunden for udvidelse af omfanget af retningslinjen til også at omfatte håndtering af afvigelser, da dette ikke er et lovkrav eller følger en specifik standard.

HGN bemærkede, at erfaringen generelt er, at indberetninger af afvigelser sjældent følges op af processer, der sikrer tilstrækkelig håndtering. Manglende historik og opfølgning er et kendt problem, og den nye tilgang vurderes derfor som en god løsning, når den er implementeret.

FKD præsenterede efterfølgende den nye tilgang til læring efter hændelser, herunder hvilke dele af organisationen der kan iværksætte læringsbaserede handlinger. FKD fremhævede, at ISDB selvstændigt kan iværksætte awareness-aktiviteter, udarbejde eller genbesøge risikovurderinger samt gennemføre efterlevelsestjek. Hvis der skal gennemføres en ad hoc audit, skal beslutningen dog træffes af CID-udvalget, da dette i højere grad berører hele departementet.

HGN spurgte afslutningsvis, om der på tilsvarende måde som ved anmeldelse af brud på persondatasikkerheden til Datatilsynet er krav i NIS 2 om, at der skal angives et kontaktpunkt hos indberetteren ved indberetning af NIS 2-hændelser. FKD svarede, at der ikke var det samme krav i NIS 2.

Beslutning

Udvalget godkendte 'retningslinje for hændelseshåndtering'.

6. Gennemgang og drøftelse af Deloittes tilsyn med departementet

v/FKD og HBN

Indstilling

Det indstilles, at CID-udvalget

- godkender forslag til håndtering af anbefalinger, herunder videre proces.

Sagsfremstilling

Departementet skal løbende føre tilsyn med informationssikkerhed og databeskyttelse i ministerområdets institutioner, jf. lov om ministres ansvarlighed. Da en institution ikke kan føre tilsyn med sig selv, har Deloitte gennemført tilsynet med departementet på baggrund af den treårige tilsynsplan og tilsynskonceptet. Deloitte afgav endelig rapport den 14. august 2025 (bilag 6.1.).

Tilsynet omfattede 43 målepunkter, herunder generelle spørgsmål, ISO-modenhed, ISO 27701:2019 og opfølgning på tidligere anbefalinger. Rapporten indeholder 25 anbefalinger til forbedring af ledelsessystemet, der varierer i kritikalitet og ressourcebehov. Overordnet skal departementet udarbejde en samlet implementeringsplan med formelle tidsfrister.

Hovedparten af anbefalingerne vedrører behovet for ensartede metoder inden for risikostyring (herunder risikotolerance), styring af aktiver, hændelseshåndtering og leverandørstyring. Derudover anbefales bl.a. en backuppolitik, opdaterede databeskyttelsestekster, samt specifikke opgaver som review af DPO'ens organisatoriske forankring i koncernen og risikovurdering af mobile enheder.

Forslag til håndtering af anbefalinger

ISDB havde før gennemførelse af Deloittes tilsyn identificeret flere af de samme mangler i ledelsessystemet og iværksat et udviklingsarbejde med udkast til politikker og retningslinjer for risikostyring, styring af aktiver og hændelseshåndtering samt en opdatering af fortegnelser og oplysningstekster. Nogle af tiltagene er implementeret, bl.a. på CID-udvalgsmødet den 29. august, hvor politik og retningslinje for risikostyring samt konsekvens- og sandsynlighedsskalaer blev godkendt. Endelig fastlæggelse af risikotolerancen er planlagt til midt oktober. Tiltagene forventes

implementeret i 2025 og imødekommer 17 af Deloittes 25 anbefalinger. For de resterende otte anbefalinger har ISDB udarbejdet et forslag til, hvordan efterlevelse kan sikres.

ISDB vil med udgangspunkt i bilag 6.2 gennemgå tilsynets anbefalinger, forslag til håndtering af anbefalinger samt estimeret tidsfrister for efterlevelse af anbefalingerne. ISDB vil i den forbindelse samtidig orientere om sammenhængen med punkt 10d, som vedr. departementets afrapportering til Styrelsen for Samfundssikkerhed (SAMSIK) 4. april 2025 vedr. bl.a. ISO-modenhedsmåling.

Ressourcetræk
Udarbejdelse af politikker, retningslinjer mv. vil indebære et væsentligt ressourcetræk hos ISDB. Efterfølgende efterlevelse af retningslinjerne vil herudover indebære et væsentligt og løbende ressourcetræk for ISDB og IT men også for organisationens aktiv- og risikoejere, da efterlevelse af retningslinjerne indebærer løbende opgavevaretagelse hen over året.

Videre proces

Med CID-udvalgets godkendelse vil Deloittes tilsynsrapport og ISDB's forslag til håndtering af anbefalinger blive forelagt DC til orientering i skriftlig proces.

Bilag

Bilag 6.1. - Tilsynsrapport - tilsyn 2024 - final140825
Bilag 6.2. – Forslag til håndtering af anbefalinger, inkl. estimerede tidsfrister for efterlevelse

Referat

ABKN oplyste, at de dokumenter, der blev vedtaget på CID-mødet d. 29. august, løfter mange af de anbefalinger, Deloitte er kommet med.

Leverandørstyring, der også vil løfte en af anbefalingerne fra Deloitte, foreslås udskudt til 2026.

Fortegnelsesprocessen er ligeledes et arbejde, der løfter anbefalinger, herunder oplysningsforpligtelsen, som tilsynet har udtalt kritik af.

ABKN bemærkede desuden, at tilsynet har udtalt kritik af departementets manglende backuppolitik. ISDB har ud fra en risikobaseret tilgang til forholdet lagt op til at vente lidt med denne opgave, idet SIT og C-Brain (de to største IT-leverandører til ISM) har en backup-politik.

Beslutning

CID-udvalget godkendte forslag til håndtering af anbefalinger, herunder den videre proces.

7. Gennemgang af Finansministeriets tilsyn med Statens IT
v/HBN og LRJ

Indstilling
Det indstilles, at CID-udvalget

- tager orienteringen til efterretning.

Sagsfremstilling
Statens IT (SIT) er databehandler for departementet, idet SIT behandler personoplysninger på vegne af og efter instruks fra departementet. Departementet er som dataansvarlig forpligtet til at sikre sig, at der føres et passende tilsyn med SIT som databehandler.

Hvert år udfører Finansministeriets Center for Tilsyn og Jura (CTJ) tilsynet med SIT på vegne af alle SIT's dataansvarlige. CTJ afrapporterer en gang årligt i maj, både skriftligt (Tilsynsberetning og en Tilsynsrapport, se bilag 7.1. – 7.3.) og mundtligt i regi af DPO-hubmøde (19. maj 2025) og i regi af Arbejdsgruppen for Informationssikkerhed (21. maj 2025).

ISDB og IT har gennemgået det skriftlige tilsynsmateriale med særligt fokus på, hvad der er væsentligt for departementet som dataansvarlig, og har i den forbindelse navnlig fokus på to kritikpunkter:

1) Krav til indeholder af databehandleraftalen, som vedr. GDPR-systemliste (tilsynsrapport nr. 4, kritikken uddybet i pkt. 3.2.3, side 15 ff)
2) Krav til behandlingssikkerhed, hvor der er 3 gule og 2 røde (tilsynsrapport nr. 4, kritikken uddybet i punkt 3.2.4, side 17 ff).

Ad 1)
SIT har i foråret (2025) afholdt to seminarer, hvor SIT har gennemgået, hvordan systemlisten opdateres korrekt. ISDB og IT er i forlængelse heraf ved at gennemgå departementets systemlister hos SIT med henblik på, at ajourføre dem.

Ad 2)
SIT har i forlængelse af tilsynsrapporten igangsat flere aktiviteter med henblik på at rette op på alle kritikpunkter, herunder også dette. ISDB og IT vurderer ikke, at der for nuværende er behov for yderligere men vil løbende og ifm. næste års tilsyn vurdere, om SIT er lykkes med de allerede igangværende tiltag på dette område.

Det bemærkes, at SIT d. 4. september 2025 har udgivet 'Notat om beretningen om tilsynet med Statens It for 2024 (bilag 7.3, hvori SIT adresserer CTJ's kritiske fund og fremlægger en handlingsplan for at rette op.

Bilag
Bilag 7.1. - Tilsyn med Statens (rapport nr. 4)
Bilag 7.2. - Beretning om tilsynet med Statens It for 2024.
Bilag 7.3. - Notat om beretning om tilsynet med Statens It for 2024

Referat
HBN redegjorde for det forholdsvist utilfredsstillende resultat af Finansministeriets tilsyn med SIT. Herunder, at der ud af de 15 undersøgelsespunkter kun var 4, der var blevet fundet tilfredsstillende.

CID-udvalget tog orienteringen til efterretning.

8. Forslag til ændring af 'Retningslinjer for medarbejdere i departementet om informationssikkerhed'

v/ABKN

Indstilling

Det indstilles, at CID-udvalget

- godkender de foreslåede ændringer i 'Retningslinjer for medarbejdere i Indenrigs- og Sundhedsministeriets departement om informationssikkerhed'

Sagsfremstilling

Retningslinjer om informationssikkerhed for medarbejdere i Indenrigs- og Sundhedsministeriets departement blev godkendt af CID-udvalget på møde den 23. maj 2024, punkt 5. Det blev i den forbindelse besluttet, at ISDB skal genbesøge og forelægge retningslinjerne efter behov og senest i 2025, og at CID-udvalget i den forbindelse tager stilling til fremtidig frekvens for gennemgang af retningslinjerne.

Der vurderes at være behov for at konsekvensrette retningslinjerne navnlig som følge af opdaterede retningslinjer om AI og nye retningslinjer om 'Retningslinjer for brug af departementets it-udstyr på farten og på rejser'.

Der foreslås således ændringer i:

- Afsnit 5. Anvendelse af departementets it-systemer og it-løsninger
  Muligheden for at anvende adblockers fjernes, da IT har oplevet problemer hermed
- Afsnit 6. Anvendelse af kunstig intelligens (AI)
  Ændres, så der henvendes til retningslinjer for AI
- Afsnit 7. Passwords
  Ændret fra 12 til 15 tegn som følge af ændrede krav fra SIT
  Afsnit 8. Lokal- og fællesdrev.
  To mindre præciseringer
- Afsnit 9. Bærbare medier
  Præcisering af hvilke usb-stick der må anvendes
- Afsnit 12. E-mail.
  Præcisering af adgangen til at sende ukrypteret mellem SIT-kunder
- Afsnit 13. Anvendelse af it-systemer uden for arbejdspladsen, herunder hjemmearbejdspladser m.v.
- Afsnit 14.3. Tjenesterejser og private rejser med udstyr der synkroniserer med F 2 og mail
  Konsekvensrettelser som følge af retningslinjer for brug af departementets it-udstyr på farten og på rejser

Det foreslås desuden at ændre afsnit 14.2. Private enheders adgang til data, således at det fremgår, at medarbejdere ikke har mulighed for installation af MIA på private telefoner. Denne ændring foreslås som en konsekvens af direktionens beslutning af 21. februar 2025 om udfasning af privat brug af arbejdstelefoner (blandede telefoner). Direktionens beslutning er efterfølgende behandlet på SAM-møde den 18. marts 2025, og de medarbejdere, som vi har haft kendskab til har/havde blandede telefoner har ved e-mail af 11. april 2025 modtaget besked om, at brug af blandede telefoner skal afvikles inden for seks måneder.

De foreslåede ændringer er markeret med TC i bilag 8.1.

Det bemærkes, at ISDB er blevet opmærksom på, at der er flere medarbejdere, der har blandede telefoner udover de som har modtaget direkte besked. Da det ikke er muligt at give disse medarbejdere direkte besked, vil ISDB i stedet lave en intranetnyhed med orientering om direktionens beslutning.

Bilag

Bilag 8.1. - Retningslinjer for medarbejdere i Indenrigs- og Sundhedsministeriets departement om informationssikkerhed

Beslutning

CID-udvalget godkendte de foreslåede ændringer i 'Retningslinjer for medarbejdere i Indenrigs- og Sundhedsministeriets departement om informationssikkerhed.'

CID-udvalget besluttede desuden, at videre proces er, at Samarbejdsudvalget orienteres skriftligt om ændringerne, og at de opdaterede retningslinjer sammen med information om blandede telefoner herefter kommunikeres til medarbejderne via intranettet.

9. Drøftelse af 'myndighedsfælles koncept for sikkerhed på rejser uden for rigsfællesskabet fra Styrelsen for Samfundssikkerhed'

v/ABKN

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning
- godkender den videre proces.

Sagsfremstilling
Styrelsen for Samfundssikkerhed (SAMSIK) har sammen med Statens It (SIT) udviklet et myndighedsfælles rejsekoncept for informationssikkerhed på rejser uden for Rigsfællesskabet (vedlagte bilag 9.1. - 9.4.). Rejsekonceptet gælder også for private udlandsrejser, hvor der er behov for at behandle eller medbringe arbejdsrelateret information eller udstyr.

Rejsekonceptet blev udrullet til sikkerhedsministerierne i 2024 og er justeret en smule i version 1.1, som nu udrulles til alle ministerier med virkning fra 1. september 2025.

Konceptet udgør et såkaldt minimumsniveau af sikkerhed ift. spionagetruslen, som vurderes at være markant og konstant.

Konceptet og styringen heraf flugter overordnet med de retningslinjer, som er implementeret i departementet vedr. brug af med departementets it-udstyr på farten og på rejser (bilag 9.5.). Det afspejler, at departementets retningslinjer er udarbejdet i samarbejde med det tidl. CFCS, nu SAMSIK.

På mødet vil ABKN orientere om enkelte opmærksomhedspunkter ifm. implementering af det myndighedsfælles rejsekoncept. Det gælder navnlig ift. at tydeliggøre, at formålet med en rejse er væsentligt for den risikovurdering, ISDB skal foretage, ligesom koordination og involvering af SAMSIK ifm. myndighedsfælles rejser skal sikres.

Endelig bemærkes det, at SAMSIK i materialet henviser til en fortrolig liste over højrisikolande, som de forventer at dele i nærmeste fremtid. Listen vil være et brugbart værktøj i ISDB's vurdering af, hvorvidt det er nødvendigt at medbringe rejse-udstyr. Det er forventningen, at listen vil nedbringe antallet af rejser, hvor dette er nødvendigt.

Videre proces

ISDB vil sikre, at det myndighedsfælles rejsekoncept implementeres i departementet.

Bilag

Bilag 9.1. - Koncept for sikkerhed på rejser uden for Rigsfællesskabet
Bilag 9.2. - Governance for det myndighedsfælles rejsekoncept
Bilag 9.3. - Håndbog for sikkerhed på rejser uden for Rigsfællesskabet
Bilag 9.4. - Retningslinjer for sikkerhed på rejser uden for Rigsfællesskabet
Bilag 9.5. – Retningslinjer for brug af departementets it-udstyr på farten og på rejser

Beslutning

CID-udvalget tog orienteringen til efterretning og godkendte den videre proces. Det blev i den forbindelse drøftet, at det ifm. implementering i departementet er vigtigt at sætte fokus på kommunikation, herunder besøg i relevante centre.

10. Orienteringspunkter

10a. Sikkerhedshændelser

v/HBN

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning

Sagsfremstilling

Følgende sikkerhedshændelser har været behandlet af ISDB siden CID-udvalgsmødet d. 20. marts:

Beskrivelse af sikkerhedshændelse	Brud på persondatasikkerhed	Anmeldt til Datatilsynet
Videresendt oplysninger som ikke skulle være sendt	Nej	-
*Mapper tilgængelige på Fællesdrev (G:)- og (F)-drev**	*Nej*	-
HR-KOP kunne se de ellers "lukkede" møder oprettet af HR	Ja	Nej
En forkert modtager var sat cc på mail	Ja	Nej
Genåbning af KOP-sagen	Ja	Nej
Stålskab i Holbergsgade	Ja	Nej
Varsling fra CFCS Sensornet vedr. mistænkelig net-trafik i december måned fra kompromitteret browserplugin i Chrome fra PC i departementet. PC indleveret til SIT. (Opdatering, var også med sidst)	-	Afventer afklaring hos SIT

Referat

CID-udvalget tog orienteringen til efterretning.

**For så vidt angår mapper tilgængelige på Fællesdrev (G:)- og (F)-drev bemærkes det, at ISDB-enheden er ved at undersøge om der er tale om brud på persondatasikkerheden. ISDB vil orientere om status på næste mødet*

10b. Obligatoriske e-learningskurser/CAMPUS-kurser

v/ABKN

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning

Sagsfremstilling

På CID-udvalgsmødet den 20. marts 2025, punkt 5, blev udvalget orienteret om status på medarbejdere og chefers gennemførelse af obligatoriske kurser, som viste en relativt lav gennemførelsesprocent (19 ledere havde ikke gennemført "Cyber- og informationssikkerhed for topledere og ledere i staten", 172 medarbejdere havde ikke gennemført "Cyber- og informationssikkerhed for medarbejdere i staten" og 168 medarbejdere havde ikke gennemført "Introduktion til databeskyttelse").

Det blev oplyst, at en forklaring på den lave gennemførselsprocent kunne være, at Campus først rapporterer et kursus som bestået, hvis evalueringen er gennemført. Det har efterfølgende vist sig ikke at være tilfældet.

HR/KOP har trukket en ny liste, som medbringes på mødet til orientering.

Det bemærkes, at kurserne fortsat vurderes at være relevante, og at de fremover vil blive opdateret af Styrelsen for Samfundssikkerhed, der har overtaget kurserne om Cybersikkerhed fra det nu nedlagte Statens Digitaliseringsakademi.

Det bemærkes endvidere, at Campus fremadrettet vil sende påmindelser til medarbejdere, som ikke har taget kurserne 30 dage før forfaldsdato, 7 dage før og på dagen for forfald. Forfaldsdatoen er 90 dage efter, at medarbejderen første gang får tilsendt besked fra Campus om gennemførsel af kurserne, dvs. medarbejderne har 90 dage til at gennemføre kurser. Udsendelsen af kurser bliver sendt til nye medarbejdere og desuden hvert andet år til medarbejdere, der er ansat, næste gang den 1. oktober 2026.

Videre proces

ISDB vil sikre, at personaleledere til de medarbejdere, der ikke har gennemført kurserne vil modtage besked.

Bilag

Liste fra Campus over deltager i obligatoriske kurser vedr. informationssikkerhed og databeskyttelse (tages med på mødet).

Referat

ABKN oplyste, at ISDB i samarbejde med KOP har igangsat et arbejde med påmindelser til de, som mangler at gennemføre. Der arbejdes fortsat på at udtrække korrekte lister.
I det omfang, der kan trækkes korrekte lister, vil personalelederne modtage besked, hvis deres medarbejdere ikke har gennemført kurserne. Alternativt vil der blive orienteret på intranettet om, at alle skal bestå kurset.

10c. NIS 2-loven

v/FKD

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning
- godkender den videre proces.

Sagsfremstilling

NIS 2-loven 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 (MSSB) 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 MSSB's første tilsyn forventes iværksat i 4. kvartal 2025.

Effektiv implementering af NIS 2-loven 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 2026.
Implementeringen omfatter bl.a. undervisning af topledelsen samt indførelse af en række retningslinjer og styringsdokumenter, der tilsammen giver ledelsen tilstrækkelig styring af risici, foranstaltninger, aktiver og hændelser i de netværksforbundne systemer, der klassificeres som relevante NIS 2-systemer.
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-lovens 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-lovens 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-loven 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.

Videre proces
ISDB vil med godkendelse af kontekst for ledelsessystem, retningslinje for styring af aktiver og retningslinje for hændelseshåndtering have gennemført punkt 2, 4 og 5 og vil fortsætte med punkt 1, 3 og 6 efterfølgende.

Referat
FKD præsenterede kort NIS 2 og forklarede, at ISDB havde udarbejdet en implementeringsplan, som fremgår af punktet. Godkendelse af retningslinjer og fastsættelse af risikotolerancen indgår som en del af implementeringsplanen, og der er derfor synergi med den tilgang, ISDB har valgt i udviklingen af ISMS-arkitekturen.

FKD bemærkede desuden, at SAMSIK ville føre tilsyn med implementeringen af NIS 2 i departementet, men at tilsynet i det første år ikke ville være dybdegående. Også her er der en synergi med ISDB's tilgang.

CID-udvalget tog orienteringen til efterretning.

10d. ISO-modenhedsmåling og tekniske minimumskrav
v/ABKN

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning

Sagsfremstilling
Departementet har i april 2025 overfor Styrelsen for Samfundssikkerhed og Beredskab (SAMSIK) afrapporteret for 1. halvår 2025 vedr. ISO-modenhedsmålingen og status på 29 tekniske minimumskrav
SAMSIK stiller krav om, at der skal udarbejdes en handleplan i de tilfælde, hvor et eller flere af de tekniske minimumskrav ikke efterleves, og i de tilfælde, hvor modenhedsmålingen ikke er på niveau 4 (styret og målbart).

Vedr. ISO 27001 modenhedsmåling 2025
Formålet med SAMSIK ISO-27001 modenhedsmåling er i regi af den nationale strategi for cyber- og informationssikkerhed 2022-2024 at gennemføre opfølgning på efterlevelsen af forskellige krav til it-sikkerhed i statslige myndigheder gennem vurdering af 9 områder.

I 2023 vurderede departementet, at vi var på niveau 3 på alle områder undtagen et enkelt område (kontekst). Af handleplanen for 2023 fremgik det, at departementet ville være på modenhedsniveau 4 på enkelte spørgeområder i 2023 og på alle spørgeområder i 2024 under forudsætning af, at de rekrutteringsmæssige udfordringer (vakancer i ISDB-enheden) kunne løses. I 2024 viste modenhedsmåling forbedring på et enkelt område, *Lederskab.*

I afrapporteringen for 2025 har departementet i modenhedsmålingen (bilag10d.1) vurderet, at der er forbedringer på tre områder, *Support*, *Beredskabsplaner*, og *Løbende forbedringer* (se også tabel 1 nedenfor). Området *Support* omfatter bl.a. *bevidsthed* og *dokumenteret information* og begrundelsen for løftet i egenvurderingen er de strukturerede awarenes aktiviteter i departementet og udarbejdelsen af SoA-dokumentet med løbende opfølgning på CID-udvalgsmøderne. Området *Beredskabsplaner*, omfatter bl.a. *Håndtering af beredskabssituationer* og *Afprøvning og evaluering* hvor løftet i egenvurderingen blandt andet skyldes, at den generelle beredskabsplan blev afprøvet ifm. test af valgenhedens del-beredskabsplan ift. Europaparlamentsvalget i 2024. Området *Løbende forbedringer* omfatter bl.a. *afvigelser og korrigerende handlinger*, hvor den systematiske opfølgning på sikkerhedshændelser løfter egenvurderingen.

I handleplanen for departementet til SAMSIK er det angivet, at departementet forventer at være på modenhedsniveau 4 på hovedparten af spørgeområderne i 2025 med mulighed for et enkelt eller to udestående spørgeområder ved næste i afrapportering i 2026 (Bilag 10.d.2 - DEP ISO 27001 – handleplan 2025).

Forventningen ved senest afgivne status i efteråret 2024 var, at departementet ville være på modenhedsniveau 4 på alle spørgeområder i 2025. Begrundelsen for dette års forbehold for enkeltområder er bl.a. usikkerhed ift. tidsplanen for at nå i mål med "planlægning", herunder risikostyringsproces, og leverandørstyring.

Tabel 1

Status – 2025									
Spørgeområder	Kontekst	Lederskab	Planlægning	Support	Drift	Evaluering	Løbende forbedringer	Leverandørstyring	Beredskabsplaner
Departementet 2025	4	4	3	4	3	3	4	3	4
Status – 2024									
Departementet 2024	4	4	3	3	3	3	3	3	3
Status – 2023									
Departementet 2023	4	3	3	3	3	3	3	3	3

Tekniske minimumskrav

SAMSIKs 29 tekniske minimumskrav til sikkerheden for statslige myndigheders it-løsninger har primært til formål at beskytte statslige it-arbejdspladser (herunder arbejdsnetværk og arbejdsstationer) mod ondsindede cyber- og informationssikkerhedshændelser, for eksempel hackerangreb og spredning af malware.

Afrapporteringen for1. halvår 2025 (bilag 10.d.3.) viser ingen udeståender i efterlevelsen af de tekniske minimumskrav, som altid er et øjebliksbillede ift. det altid skiftende tekniske landskab, som at f.eks. at programversioner bliver forældede.

Afrapporteringen for 2.halvår 2024 viste to udeståender, som begge er løst på tidspunktet for denne afrapportering: 1) en manglende proces for regelmæssig gennemgang af installeret specialsoftware på Statens IT-Arbejdsplads (SIA-PC), 2) et udestående vedr. indtast.dk, hvor kryptering ikke levede op til minimumskravet på minimum tls. version 1.2.

Videre proces

Det er ikke afklaret, hvordan SAMSIK fremadrettet vil foretage overvågningen af ISO modenhedsmåling og tekniske minimumskrav, herunder sammenhængen til NIS 2

Som det fremgår af dagsordenens punkt 6, bilag 6.2., har Deloitte haft en lavere vurdering end departementet på nogle af spørgeområderne, herunder beredskabsplaner. Dette vil indgå i departementets vurdering ved en eventuel kommende afrapportering til SAMSIK.

Bilag

Bilag 10d.1. - DEP ISO 27001 – spørgeramme 2025
Bilag 10d.2. - DEP ISO 27001 – handleplan 1. halvår 2025
Bilag 10d.3. - DEP rapporteringsskema tekniske minimumskrav

10e. Status på afdækning af databeskyttelsesretlig konstruktion for HR-opgaver i koncernen

v/HBN

Indstilling

Det indstilles, at CID-udvalget

- tager orienteringen til efterretning.

Sagsfremstilling

Den nuværende HR-organisering, der trådte i kraft den 1. oktober 2022 indebærer, at der i Sundhedsstyrelsen er en koncernfunktion for lønadministration, ledelsesinformation og koncernregnskab, tilsammen KRØL, og at der i departementet er koncernfunktioner for personalejura og overenskomster (PJO) samt HR-koncernprogrammer (KOP). Der har siden 1. oktober 2022 pågået et arbejde i samarbejde med styrelserne med at afdække, hvilken databeskyttelsesretlig konstruktion der er gældende for hver af de tre koncernfælles funktioner.

Status i forhold til KRØL er, at det er fastlagt, at SST (KRØL) er databehandler for de øvrige institutioner i koncernen ift. de personoplysninger, som KRØL behandler i henhold til den aftale, som indgås mellem SST (KRØL) og de enkelte institutioner.

SST udarbejder i øjeblikket databehandleraftaler med henblik på at kunne indgå aftaler med de øvrige institutioner, herunder departementet, inden udløbet af Q3.

Der er aftalt en fælles tilsynsmodel, som er godkendt af Styringsforum d. 18. august 2025, som i hovedtræk indebærer, at departementet på vegne af de enkelte institutioner gennemfører tilsynet med SST som databehandler, således at der er et tidsmæssigt sammenfald med det tilsyn, som departementet i øvrigt gennemfører med informationssikkerhed hos SST.

Spørgerammen for tilsynet med SST som databehandler vil blive udarbejdet i samarbejde med de enkelte institutioner.

Der gives en mundtlig orientering på mødet vedr. status for KOP og PJO.

Referat

HBN oplyste, at status er, at udkast til notat om den databeskyttelsesretlige rollefordeling for KOP's varetagelse af opgaver skal i høring hos institutionerne via CID-Koordinationsforum. Den foreslåede rollefordeling i notatet er, at der er et fælles dataansvar mellem den enkelte institution og departementet.

Ift. koncernfunktioner for personalejura og overenskomster (PJO) oplyste ABKN, at der også vil blive udarbejdet et notat, der beskriver den databeskyttelsesretlige rollefordeling i forhold til PJO's varetagelse af opgaver.

Det kan supplerende oplyses, at KOP-notatet efter CID-udvalgsmødet har været i høring hos CID-K. Næste skridt er, at der skal udarbejdes aftaler om fælles dataansvar.

11. EVT.

HGN bemærkede, at informationssikkerhed og databeskyttelse efter hendes vurdering bør have en mere fremtrædende placering på intranettet, der passer bedre til vigtigheden af emnet, idet væsentlige dokumenter rettet til medarbejdere er for svære at finde, fx 'Retningslinje for indberetning af sikkerhedshændelse'.

HGN bemærkede endvidere, at den proces, der er beskrevet i 'Retningslinje for indberetning af sikkerhedshændelse', som forudsætter, at medarbejderen selv foretager indberetningen til SIT og herefter videresender kvitteringen til ISDB, ikke forekommer hensigtsmæssig. Problemet er, at videreformidling af opfølgende svar og spørgsmål fra SIT til ISDB p.t sker via medarbejderen, som manuelt skal videresende disse til ISDB, hvilket kan indebære risiko for, at relevante oplysninger for håndtering af sagen ikke kommer til ISDB's kundskab.

Hertil kommer, at denne proces er unødigt besværlig for indberetter, hvilket øger risikoen for, at sikkerhedshændelser ikke indberettes i det omfang, de burde.

ISDB vil overveje, om det er den mest hensigtsmæssige måde.