INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Dato: 27-02-2024
Enhed: ISDB-enheden
Sagsbeh.: DEPFBG
Sagsnr.: 2023-939
Akt-id.: 115299

Version: 1.0
Godkendt af: MRAN

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

Referat

Tekst fra dagsordenen er medtaget under hvert punkt og er markeret med gråt.

Dato for møde
29. februar 2024

Deltagere

Medlemmer

Cecilie Louise Svane Olesen (CLSO), afd. Strukturel Sundhed, forperson
Trine Brøbecher (TRBR), HR
Carsten Grage (CG), IT
Mette Rye Andersen (MRAN), ISDB-enheden
Dorte Bech Vizard (DBV) (deltog under punkt 11)

Observatører

Helle Ginnerup-Nielsen (HGN), DPO DEP
Philip Joen Bujnoch (PBU), DPO Benchmarkingenheden

Sekretariat

Finn Boilesen Guldbæk (FBG), ISDB-enheden
Sanae Karroum (SAK), ISDB-enheden (referent)

Afbud

Pernille Seaton (PSE), Intern Administration

Bilag: For at skabe en bedre sammenhæng mellem dagsorden og bilag, følger bilagene det nummererede punkt på dagsordenen, således at punkt 3's bilag hedder henholdsvis bilag 3.1 og bilag 3.2.

Dagsorden

1. Velkomst

CLSO bød velkommen til udvalgets andet møde.
CLSO spurgte, om udvalget havde bemærkninger til dagsordenen. Udvalget havde ingen bemærkninger.

PBU spurgte, om organisationsændringen i Indenrigs- og Sundhedsministeriets departement vil have betydning for udvalgets sammensætning. CLSO bemærkede, at det bør afklares frem mod næste møde (**ISDB** følger op).

2. Referat fra CID-udvalgsmøde den 13-12-2023

CLSO præsenterede til udvalgets godkendelse referatet fra første CID-udvalgsmøde med de af HGN foretagne præciseringer til referatets punkt 5.

Konklusion
Udvalget godkendte referatet uden yderligere bemærkninger.

Indstilling
. / . Det indstilles, at CID-udvalget godkender referat fra CID-udvalgsmøde den 13-12-2023 med præciseringer til referats punkt 5 (bilag 2.1).

Sagsfremstilling:
Referat fra CID-udvalgets møde den 13-12-2023 er udsendt til udvalgets medlemmer den 15-01-2024. Der er modtaget præciseringer til referatets punkt 5. Ændringer er anført med TC i vedlagte referat.

Den videre proces
Med udvalgets godkendelse vil referatet blive offentliggjort på ISM INTRA.

Bilag
2.1. Referat fra CID-udvalgsmøde 13.12.2023.

Punktet bliver godkendt. Ingen bemærkninger.

3. Retningslinje for indberetning af sikkerhedshændelser

CLSO indledte og præsenterede udkastet til retningslinje, som var blevet revideret efter beslutning på udvalgets møde den 13. december 2023.

Udvalget drøftede det reviderede udkast til retningslinje og havde følgende bemærkninger:

- Udvalget besluttede, at der på side 2 under punkt 3 tilføjes en formulering om, at medarbejder skal informere sin nærmeste leder om sikkerhedsbruddet.
- HGN spurgte om alle indberetninger af sikkerhedshændelser, bliver sendt videre til ISDB-enheden. CLSO svarede, at alle henvendelser skal sendes til ISDB-enheden for at få et samlet overblik.
- Udvalget drøftede vigtigheden af at fremme en kultur, hvor sikkerhedshændelser indberettes hurtigst muligt.

- CLSO bad om, at retningslinjerne præsenteres på et kommende chefmøde, hvorefter cheferne kan præsentere dem for deres medarbejdere. Dette skal ske samtidigt med, at retningslinjen offentliggøres på intranettet.

Konklusion
Med de faldne bemærkninger godkendte udvalget retningslinjen.

Indstilling
Det indstilles, at CID-udvalget godkender retningslinje for indberetning af sikkerhedshændelser.

Sagsfremstilling
På CID-udvalgets møde den 13-12-2023 blev udkast til retningslinje for indberetning af sikkerhedshændelser drøftet. Det blev besluttet at udarbejde supplerende bemærkninger ift. indberetning af brud for CPR-enheden og evt. andre fagsystemer.

Forslaget har efterfølgende været drøftet med CPR og IT, og vedlagte reviderede udkast til
./. retningslinje (bilag 3.1) er tilpasset med ændringsmarkeringer.

For at gøre det så enkelt som muligt for brugerne tilstræbes princippet om SPOC (Single Point of Contact) ifm. hændelsesrapportering, men for IM's systemer kan der være supplerende vejledning til de enkelte systemer.

SIT har ansvar for løbende at rapportere indberettede hændelser til departementets sikkerhedsansvarlige, men rapporteringerne er endnu ikke tilfredsstillende, hvilket ISDB-enheden er i dialog med SIT om på vegne af koncernen.

Ifølge retningslinjen vil brugeren i alle tilfælde skulle indberette hændelsen skriftligt til Serviceportalen, men for de systemer, hvor departementer har driftsansvaret (driftsmodel 0), og i de tilfælde, hvor sikkerhedshændelsen ikke er tilknyttet et system men en handling, vil brugeren modtage en kvitteringsmail (i nogle tilfælde en afvisning), som skal videresendes til ISDB-enheden.

Den videre proces
Med udvalgets godkendelse vil retningslinjen blive formidlet til medarbejderne på ISM INTRA. Dialogen med SIT vedr. hændelsesrapportering fortsættes, og udvalget vil løbende blive orienteret.

Bilag
3.1 Revideret udkast til retningslinje for indberetning af sikkerhedshændelser.

4. Privatlivspolitik (oplysningstekst til de registrerede) til ISM's hjemmeside ism.dk

CLSO indledte og præsenterede privatlivspolitikken til Indenrigs- og Sundhedsministeriets hjemmeside.

MRAN bemærkede, at der i højere grad er tale om en oplysningstekst til de registrerede end en decideret "politik", selvom flertallet af ministerierne betegner teksten "Privatlivspolitik" på deres hjemmesider.

MRAN bemærkede videre, at afsnittet "Analyse og Statistik" endnu ikke er fyldestgørende, og afsnittet vil blive opdateret med involvering af pågældende fagchef.

Udvalgets drøftede udkastet og havde følgende bemærkninger:

- HGN bemærkede, at der ikke var tale om en politik i ISO-forstand, men en underretning til borgerne, som er påkrævet efter GDPR, om departementets behandling af personoplysninger om dem. Bortset fra afsnittet om analyse og statistik er denne tekst rettet til den gruppe af borgere, der selv henvender sig til ministeriet. Derudover bemærkede HGN, at der på departementets hjemmeside også er den koncernfælles databeskyttelsespolitik, som pt. er under opdatering (punkt 9 på dagsordenen), og en orientering benævnt "privatlivspolitik", som kun handler om besøg på departementets hjemmeside. Det vil derfor skabe unødig forvirring, hvis nærværende oplysningstekst har tilsvarende betegnelse. Udvalget besluttede at ændre titlen til "Sådan behandles dine personoplysninger i Indenrigs- og Sundhedsministeriets departement" i overensstemmelse med den betegnelse, som den nuværende tilsvarende tekst har.
- FBG havde en tekstnær rettelse til punkt 1, hvor formuleringen "læs mere her om, hvordan du sender sikker e-mail til ministeriet" bør ændres til "læs mere om, hvordan du sender sikkert til ministeriet". Udvalget bakkede op om ændringen.
- CLSO bad om, at alle medarbejdere modtager et opdateret link til deres mail, der henviser til teksten. Evt. via linket "Sådan behandles dine personoplysninger", når den nye oplysningstekst bliver publiceret
- HGN gjorde opmærksom på, at det er et krav efter GDPR, at oplysningsteksten aktivt "gives" til de registrerede, og at det derfor også er vigtigt at sikre, at processerne herfor er fyldestgørende. Bl.a. skal oplysningsteksten også kunne sendes til de borgere, der kontakter ministeriet via fysisk post. HGN bemærkede i den forbindelse, at de links, der er indlejret i den foreliggende tekst, ikke vil kunne ses på en udskrift. HGN mindede desuden om, at der er linket til den nuværende oplysningstekst i medarbejderes mailsignaturer og i autosvaret fra hovedpostkassen, og at det skal sikres, at personer, der henvender sig via Digital Post, også modtager informationen. HGN opfordrede til at koordinere med bl.a. Kontoret for Forebyggelse, Borgerbreve og Strålebeskyttelse, som håndterer borgerhenvendelser.
  Udvalget bakkede op om opmærksomhedspunkterne, og det blev besluttet at udarbejde et auto-svar til henvendelser via digital post og sikre, at teksten foreligger i printvenlig version.
- HGN bemærkede videre, at det er vigtigt, at inddrage relevante kontorer i departementet ift. videre processer ift. opbevaring, sletning mv. med henblik på at sikre, at det anførte er retvisende. Dette er også en del af den kommende indsats med at få gennemgået og opdateret departementets fortegnelse over behandlingsaktiviteter. PBU tilføjede, at det også er relevant at inddrage Kommunikation ift. hjemmeside og de autosvar, der sendes til borgerne, når de kontakter departementet via digital post.
- Udvalget drøftede HR-manager, herunder hvad der står som tekst, når en ansøger har søgt et job. TRBR vil undersøge dette (**HR** følger op).

Konklusion
Med de faldne bemærkninger tiltrådte udvalget indstillingen.

Indstilling
./. Det indstilles, at udvalget drøfter og godkender Udkast til privatlivspolitik for Indenrigs- og Sundhedsministeriets departementets behandling af personoplysninger (bilag 4.1).

Sagsfremstilling:

Indenrigs- og Sundhedsministeriets departement behandler personoplysninger som led i departementets myndighedsopgaver, eksempelvis i forbindelse med en henvendelse fra borgere, aktindsigtsanmodninger, rettighedsanmodninger mv.

Idet der behandles personoplysninger har departementet en oplysningspligt overfor de personer, der behandles personoplysninger om.

Vedlagte udkast til privatlivspolitik (oplysningstekst til de registrerede) er afgørende for at opfylde departements forpligtelse til at give klar og gennemsigtig information til de registrerede. Politikken beskriver blandt andet formålene til behandlingen af personoplysninger, de juridiske grundlag for behandlingen og de rettigheder, de registrerede har i ifølge databeskyttelsesforordningen.

Departementets privatlivspolitik vil udgøre en central del af departementets oplysningspligt over for de registrerede og vil styrke efterlevelsen af databeskyttelsesreglerne, jf. databeskyttelsesforordningens artikel 13 og 14.

Det skal bemærkes, at afsnittet "Analyse og Statistik" ikke er omfattende, da vi stadig mangler fuldstændige oplysninger på dette område. Specifikt mangler vi eksempelvis information om igangværende analyser på kontoret samt varigheden af opbevaringsperioden. Det er dog blevet vurderet, at det er mest hensigtsmæssigt at inkludere afsnittet i privatlivspolitikken for at opfylde en vis grad af oplysningspligt i henhold til artikel 14 end at undlade det.

Den videre proces
Med udvalgets godkendelse vil politikken blive offentliggjort på www.ism.dk og erstatte den nuværende.

Bilag
4.1 Udkast til privatlivspolitik til departements hjemmeside.

5. CID-håndbog

CLSO indledte og gav ordet til FGB.

FGB bemærkede, at formålet med CID-håndbogen er at sikre dokumentationen for at målsætningen for CID-arbejdet, herunder at CID-udvalgets roller og ansvar efterleves og at politikker, retningslinjer og procedurer dokumenteres i et samlet dokument. CID-håndbogen vil endvidere være dokumentationen i forhold til SoA dokumentationen for efterlevelse af kontrollerne og foranstaltningerne i ISO 27001 Annex A og ISO 27701.

Udvalget drøftede håndbogen og havde følgende bemærkninger:

- CLSO bemærkede, at skabelonen er et udkast, der er i gang med at blive udarbejdet. Status på håndbogen vil bliv forlagt på de kommende CID-udvalgsmøder, til orientering og godkendelse.
- HGN spurgte, hvordan håndbogen spiller sammen med NorthGRC (Neupart). FGB svarede, at NorthGRC vil blive brugt til at vedligeholde håndbogen.
- PBU bemærkede, at det var hensigtsmæssigt at inddrage RACI-modellen. PBU spurgte, hvordan det kunne være, at ISDB-enheden ikke fremgik under punkt 5 og 6 ift. ansvarlig enhed. FBG svarede, at dette vil fremgå af status på mødet i maj.

- CLSO spurgte om håndbogen kunne tilgås, mens den var underudarbejdelse. FBG svarede, at medlemmerne af CID-udvalget kan få adgang til håndbogen igennem NorthGRC. På den måde vil udvalget have mulighed for at følge med i status.

Konklusion
CID-udvalget godkendte indstillingen.

Indstilling
Det indstilles, at CID-udvalget godkender, at ISDB-enheden udarbejder CID-håndbog med bidrag fra udvalgets medlemmer.

Sagsfremstilling
./. CID-håndbogen (bilag 5.1) vil understøtte CID-udvalgets og ISDB-enhedens arbejde med at sikre efterlevelse af ISO-standarderne, idet håndbogen sikrer, at der tages stilling til de enkelte kontroller/foranstaltninger i kravstandarderne ISO 27001 og 27701.

Formålet med CID-håndbogen er at beskrive, hvordan departementet efterlever relevante kontroller og foranstaltninger, der styrer informationssikkerheden i forhold til tilgængeligheden, fortroligheden, og integriteten af de systemer og informationer, der benyttes og udveksles.

CID-Håndbogen vil følge kapitalerne i ISO 27001:2013 Annex A, og vil blive udbygget efter vejledningen og anbefalinger i ISO 27002:2017 og ISO 27701:2019.

I vedlagte udgave af CID-håndbogen (bilag 4.1) er teksten i kapitel 5-18 i kursiv fra det daværende Indenrigs- og Boligministeries udgave af håndbogen.

ISDB-enheden vil opdatere håndbogen i samarbejde med HR, IT, Intern Administration og BESS. DPO konsulteres på relevante områder.

Den videre proces
ISDB-enheden koordinerer opdateringen af de enkelte kapitler i CID-håndbogen med relevante CID-udvalgsmedlemmer og afrapporter status på CID-udvalgsmødet den 23-05-2024.

Bilag
5.1 CID-håndbog for Indenrigs- og Sundhedsministeriet.

6. Retningslinje "CID for medarbejdere i departementet"

CLSO indledte og gav ordet til FBG.

FBG præsenterede punktet ved at understrege betydningen af, at alle medarbejdere i departementet bevidstgøres om cyber- og Informationssikkerhed og databeskyttelse. Med baggrund i CID-håndbogen udarbejdes en række retningslinjer for brugen af informationsaktiver i departementet. Der vil f.eks. blive udarbejdet retningslinjer om brug af internet, e-mail, sociale medier, m.m.

CID-udvalget drøftede punktet og havde følgende bemærkninger:
- HGN spurgte, om der ifm. retningslinjerne vil blive henvist til andre områder på hjemmesiden, hvor medarbejderen kan finde mere detaljerede oplysninger. FBG

svarede, at dette ikke var planen, men at retningslinjerne er emner, som den enkelte medarbejder skal være opmærksom på.

Konklusion
CID-udvalget godkendte indstillingen.

Indstilling
Det indstilles, at CID-udvalget godkender, at ISDB-enheden udarbejder retningslinje målrettet medarbejdere, så de får den nødvendige information om cyber-, informationssikkerhed og databeskyttelseskrav.

Sagsfremstilling
Retningslinjen "CID for medarbejdere i departementet" har til formål at give kendskab til cyber-, informationssikkerhed og databeskyttelse, så de kan agere hensigtsmæssigt.

"CID for medarbejdere" vil bl.a. beskrive regler for adgangskoder, brug af internet, e-mail og sociale medier, adgang til din arbejdsplads, fjernearbejde og online-møder. Retningslinjen vil således sætte rammerne for, hvordan den enkelte medarbejder overholde cyber-, informationssikkerhed og databeskyttelseskrav, og vil være et vigtigt referencepunkt både i on-boarding processen samt i medarbejdernes daglige arbejde.

ISDB-enheden vil udarbejde retningslinjen i samarbejde med HR, IT, Intern Administration, BESS og Kommunikation. DPO konsulteres på relevante områder.

Den videre proces
ISDB-enheden koordinerer udarbejdelsen af retningslinjen "CID for medarbejdere" med relevante CID-udvalgsmedlemmer, og vil fremlægge forslag til retningslinje til CID-udvalgsmøde den 23-05-2024.

7. Risikostyring i Indenrigs- og Sundhedsministeriets departement

CLSO indledte med at nævne, at risikostyring er et centralt element i informationssikkerhedsarbejdet og har til formål at definere en struktureret risikostyringsproces.

CID-udvalgets medlemmer drøftede punktet og havde følgende bemærkninger:

- CLSO bemærkede, at det kunne være relevant for ISDB-enheden at drøfte sagen med Kåre Degn fra Koncernøkonomi, da koncernøkonomi er i gang med et lignende projekt.
- Det blev drøftet, at der ikke er defineret en bestemt metode i forhold til risikostyring for offentlige myndigheder, men ISDB-enheden vil bl.a. inddrage anbefalinger fra DIGST samt det arbejde vedr. referencetabeller, som pågår på koncernniveau i regi af CID-organiseringen.

Konklusion
CID-udvalget godkendte indstillingen.

Indstilling
Det indstilles, at CID-udvalget godkender, at ISDB-enheden udvikler risikostyring i departementet, jf. målsætning i CID-politikken.

Sagsfremstilling
Risikostyring definerer og kvantificerer risici, og er et centralt element i ledelsessystemet, der faciliterer informerende ledelsesbeslutninger.

Formålet med risikostyring er at understøtte efterlevelse af kontroller/foranstaltninger i ISO 27001:2013 og 27701:2019 ved at definere en struktureret risikostyringsproces for departementets informationsaktiver. Risikostyringsprocessen vil følge principperne i ISO 27005:2018 standarden, og vil derfor være i overensstemmelse med kravene i ISO 27001:2013 og 27701:2019.

Dette vil støtte CID-udvalget i deres arbejde med risikostyring, herunder med de identificerede risici, så departementet ikke udsætter sig for større risici, end hvad der er acceptabelt.

Arbejdet består af følgende delelementer:
- Interessentanalyse – der faciliterer fastsættelsen af en risikoappetit, dvs. hvad der udgør en acceptabel risiko for departementet.
- Risikostyringsproces – der faciliterer ensartet vurdering og behandling af risici i departementet.
- Rapporteringsproces - der faciliterer at CID-udvalget tager stilling til risici, der overstiger den definerede risikoappetit.

Den videre proces
Som en del af udviklingsarbejdet vil ISDB-enheden indsamle bidrag fra CID-udvalget og øvrige afdelinger i departementet.

ISDB-enheden koordinerer udviklingen af de enkelte delelementer med relevante CID-udvalgsmedlemmer og medarbejdere, og afrapporter status på arbejdet ved CID-udvalgsmødet den 23-05-2024.

8. Drøftelse vedr. fuld decentral koncern it-model

CLSO indledte med at bemærke, at det eftersendte materiale fra mødet i Digitaliseringsboard var den endelig version af den nye koncern it-model.

Udvalget drøftede punktet og havde følgende bemærkninger:
- HGN spurgte, om udvalget vidste, hvilken aftale der henvises til i notatet, side 2, bullet 2, hvor det fremgår, at ”SDS vil fortsat være aftaleholder”.

  CG bemærkede, at hver institution har egen kundeaftale med SIT. SDS giver udtryk for at have en kundeaftale med SIT, som, de øvrige institutioner har en allonge til, hvilket forekommer at være en misforståelse.

  CG bemærkede videre, at han alene er i besiddelse af DEP’s kundeaftale med SIT, men ikke de andre styrelsers. Det blev besluttet at kontakte SDS mhp. at afklare, hvilken aftale SDS præcis henviser til i notatet.

  CG bemærkede videre, at SDS pt. repræsenterer koncernen både i Kundestrategisk Forum og i Kundeforum. De øvrige deltagere i Kundestrategisk Forum kommer fra departementerne, og CG deltogselv i dette forum i det daværende Indenrigs- og Boligministerie.

- MRAN bemærkede, at spørgsmålet vedr. ansvarsfordeling i den nye koncern it-model er koblet til de spørgsmål, som arbejdsgruppen vedr. ansvarsfordelingen for koncernfælles systemer skal se nærmere på i regi af CID-koordinationsforum. MRA bemærkede, at CG bør involveres i arbejdsgruppen som følge af organisationsændringen i DEP, hvilket CG var enig i.

Konklusion
CG og ISDB-enheden følger op på det kontraktuelle grundlag mellem SDS, institutionerne og SIT samt arbejdsgruppen vedr. ansvarsfordeling for koncernfælles systemer.

Indstilling
Det indstilles, at CID-udvalget har en indledende drøftelse af den af reviderede koncern it-model med henblik på foreløbige input til, hvilken betydning ændringen indebærer for informationssikkerhed og databeskyttelse i departementet.

./. Sagsfremstilling
ISM og FM har på baggrund af gennemført analyse indgået aftale om SDS' økonomi for 2024 og frem. Der indgår en række tiltag i aftalen, som medfører ændringer af koncern it-modellen mod en mere decentral model, hvor SDS' rolle ændres og en række fora nedlægges eller ændres (bilag 8.2-8.3).

KLF blev orienteret om den nye model på møde den 5. februar 2024. Efterfølgende er Tværgående Review board blev orienteret, idet udvalget er nedlagt, og der er planlagt drøftelse vedr. den nye model på møde i Digitaliseringsboard den 22. februar 2024.

CID-koordinationsforum besluttede på møde den 2. februar 2024 at sætte den nye model på dagsordenen til drøftelse på forummets møde den 12. april 2024.

Der er desuden nedsat en arbejdsgruppe i regi af CID-koordinationsforum, som har til formål at redegøre for ansvarsfordelingen for tværgående tjenester (DKSund og tværgående Microsoft tjenester som fx Azure, Teams mv.) samt dataflows og governance for tjenesterne. Arbejdsgruppen mødtes første gang den 22. februar 2023.

Det bemærkes i den forbindelse, at DEP ikke pt. har en drifts- og databehandleraftale med SDS ifm. de tjenester, som SDS forvalter for DEP (og koncernen).

Videre proces
Ingen bemærkninger.

Bilag
8.1 Fuld decentral koncern it-model (UDGÅR)
8.2 Udvidet dagsorden og sagsfremstilling til Digitaliseringsboard 220224
8.3 Bilag 1 – Orientering Decentral koncern it-model i ISM

9. Udkast til koncernfælles CID-politik

CLSO gav ordet til MRAN.

MRAN præsenterede baggrunden for udkastet til en koncernfælles politik og de overvejelser, som var blevet drøftet i CID-koordinationsforum. Jacob Gemmer fra NGC har skrevet for med involvering på tværs af koncernen. Udkastet er pt. i høring hos alle institutioner og skal drøftes på møde i CID-koordinationsforum i april.

Udvalget havde ingen bemærkninger til udkast til koncernfælles CID-politik.

Konklusion
Departementet har ingen bemærkninger til den igangværende høring over udkast til koncernfælles CID-politik, som drøftes på næste møde i CID-koordinationsforum med henblik på efterfølgende godkendelse i skriftlig proces.

./. Indstilling
Det indstilles, at CID-udvalget drøfter vedlagte Udkast til koncernfælles CID-politik (bilag 9.1).

Sagsfremstilling
CID-Koordinationsforum besluttede i foråret 2023 at udarbejde en koncernfælles CID-politik. På mødet den 15. september 2023 blev det besluttet at holde politikken på et overordnet niveau, dvs. at den har til formål at tegne de bredere linjer med et passende tværgående ambitionsniveau.

Opgaven med at skrive udkast til den koncernfælles CID-politik blev delegeret til Jacob Drasbeck, NGC, som har udfærdiget vedlagte bilag 10.1 med input fra bl.a. STPS, SSI, DEP og den koncernfælles DPO.

Udkastet til politikken er sendt i skriftlig høring blandt institutionerne i koncernen og vil blive drøftet på mødet i CID-koordinationsforum den 12. april 2024.

Det er planen, at CID-koordinationsforum efterfølgende godkender udkastet i skriftlig proces. Det godkendte udkast til politikken vil blive forelagt KLF til godkendelse, jf. den revidere koncern it-model.

Videre proces
ISDB-enheden viderebringer CID-udvalgets evt. kommentarer til udkastet til CID-Koordinationsforum og sender det endelige udkast til godkendelse blandt udvalgsmedlemmerne.

Bilag
9.1 UDKAST Koncernfælles cyber-, informationssikkerheds- og databeskyttelsespolitik.

10. Orientering

10.a Møde i CID-koordinationsforum 02-02-2024

CLSO gav ordet til MRAN

MRAN orienterede kort fra mødet i CID-koordinationsforum. Drøftelsespunkterne vedr. trusselsbilledet var blevet udskudt til mødet i april grundet frafald. Der havde til gengæld været tid til at drøfte NIS 2, hvor DAICY havde orienteret om status, om end der ikke var meget nyt.

HGN supplerede med at oplyse, at en række problemstillinger vedr. Cloud-løsninger var blevet drøftet på mødet, herunder eksempelvis ift. Microsoft og AI.

Konklusion
Udvalget tog orienteringen til efterretning

Sagsfremstilling
DBV orienterer kort fra mødet.

10.b Modenhedsmåling og tekniske minimumskrav 2024

CLSO gav ordet til MRAN

MRAN orienterede om, at departementet har modtaget bestilling på ISO modenhedsmåling og status på de tekniske minimumskrav. Som noget nyt vil CID-udvalget skulle godkende DEP besvarelserne, inden DC forelægges en samlet sag for hele koncernen.

FBG bemærkede, at ISDB-enheden vil indkalde til møder vedr. status på modenhed i departementet.

Konklusion
CID-udvalget tog orienteringen til efterretning. De udarbejdede besvarelser sendes til udvalgets godkendelse i skriftlig procedure.

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

Sagsfremstilling
Én gang om året skal myndighederne aflægge status på deres ISO-modenhedsniveau. To gange om året, i henholdsvis første og andet halvår, skal myndighederne afrapportere på efterlevelsen af de tekniske minimumskrav.

Digitaliseringsstyrelsen har den 19. februar 2024 udsendt bestillingerne vedrørende ISO-modenhedsmålingen for 2024 og afrapporteringen på de tekniske minimumskrav i første halvår foretages samlet. Begge bestillinger koordineres af ISDB-enheden, som har frist for at indsende den samlede besvarelse for ministerområdet til Digitaliseringsstyrelsen den 23-04-2024.

Fristen for departementets bidrag til den samlede besvarelse er den 4. april 2024.

Videre proces
DEPs bidrag til besvarelse af ISO-modenhedsmåling og de tekniske minimumskrav skal godkendes af CID-udvalget, jf. Kommissorium for CID-udvalget, hvorefter den samlede besvarelse for ministerområdet forelægges DC til godkendelse.

Sekretariatet for CID-udvalget udarbejder DEP-besvarelsen med bidrag fra relevante enheder og sender til godkendelse blandt medlemmerne af CID-udvalget i skriftlig proces.

10.c Brev fra digitaliserings- og ligestillingsminister vedr. Rigsrevisionens beretning om statens it-beredskab II (Beretning nr. 5/2023)

CLSO indledte med at nævne, at digitaliserings- og ligestillingsministeren udtrykker bekymring over Rigsrevisionens beretning om it-beredskabet i staten (Beretning nr. 5/2023).

Det bemærkes, at skrivelsen ikke vedrører DEP.

Konklusion
Udvalget tog orienteringen til efterretning.

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

Sagsfremstilling
./. Digitaliserings- og ligestillingsministeren udtrykker bekymring over Rigsrevisionens beretning om it-beredskabet i staten II (Beretning nr. 5/2023). Ministeren understreger vigtigheden af et effektivt beredskab for, at it-sikkerheden står mål med trusselsbilledet (bilag 10.c).

Krav til it-beredskab fremgår også af sikkerhedsstandarden ISO 27001, som myndighederne siden 2016 har været forpligtet til at implementere. Af Digitaliseringsstyrelsens årlige opfølgninger fremgår det, at it-beredskab er et af de områder, hvor der generelt er størst forbedringspotentiale. Resultatet for den seneste opfølgning fra 2023 viser, at mere end en tredjedel af myndighederne fortsat har udeståender med deres it-beredskab.

Bilag
10.c Brev fra digitaliserings- og ligestillingsministeren vedr. Rigsrevisionens beretning om statens it-beredskab II (Beretning nr. 5/2023)

10.d Nye cyber- og informationssikkerhedskurser i Campus

CLSO gav ordet til FBG.

FBG orienterede om, at Digitaliseringsstyrelsen har offentliggjort to nye kurser i cyber- og informationssikkerhed til hhv. medarbejdere samt topledere og ledere i staten.

MRAN opfordrede CID-udvalgets medlemmer til at gennemføre relevante kurser. Der var enighed om, at det vil være relevant for udvalgets medlemmer at gennemføre kurset målrettet ledere og topledere i staten. FBG bemærkede, at
ISDB-enheden vil udarbejde en indstilling vedr. obligatoriske e-læringskurser på CID-området for medarbejdere og ledere i departementet til drøftelse på udvalgets møde i maj.

Konklusion
Udvalget to orienteringen til efterretning og gennemfører det ene af de to nye kurser frem mod næste møde.

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

Sagsfremstilling
Digitaliseringsstyrelsen har offentliggjort to nye kurser i cyber- og informationssikkerhed for ansatte i staten. Kurserne er tilgængelige via CAMPUS.

Cyber- og informationssikkerhed for topledere og ledere i staten

- e-læringskurset introducerer til grundbegreberne i cyber- og informationssikkerhed og til ledelsens ansvar og opgaver.
  Link til kurset: Cyber- og informationssikkerhed for medarbejdere i staten.

Cyber- og informationssikkerhed for medarbejdere i staten

- e-læringskurset introducerer til de grundlæggende begreber inden for cyber- og informationssikkerhed. Du bliver også ført gennem de rammer, der gælder i staten, og du bliver klædt på til hvordan du skal agere sikkert i omgangen med informationer og data, og hvordan du skal forholde dig, hvis uheldet er ude.
  Link til kurset: Cyber- og informationssikkerhed for ledere i staten.

Den videre proces
Til næste CID-udvalgsmøde i maj vil ISDB-enheden udarbejde indstilling vedr. obligatoriske e-læringskurser på CID-området for medarbejdere og ledere i departementet.

10.e Privatlivspolitik (oplysningstekst) for medarbejdere i departementet

CLSO indledte og orienterede om, at departementet også er forpligtet til at give medarbejderne oplysninger om, hvordan deres personoplysninger bliver behandlet ifm. deres ansættelse i departementet.

Departementet har ikke tidligere haft en oplysningstekst til medarbejdere, men ISDB-enheden og HR er i gang med at udarbejde en.

Konklusion
Udvalget tog orienteringen til efterretning og havde ingen bemærkninger til, at underretningsteksten evt. behandles i skriftlig procedure.

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

Sagsfremstilling
Indenrigs- og Sundhedsministeriets departement behandler personoplysninger om departements medarbejdere. Med denne behandling af personoplysninger følger et ansvar, da medarbejderne har en række rettigheder ifølge databeskyttelsesforordningen.

Departementet har ikke tidligere haft en privatlivspolitik for medarbejdere. For at opfylde vores forpligtelse ifølge databeskyttelsesforordningen er ISDB-enheden i færd med at udarbejde en privatlivspolitik for medarbejdere i departementet med input fra relevante enheder og DPO.

Den videre proces
Såfremt udkastet færdiggøres inden næste møde, vil ISDB-enheden sende det til behandling i skriftlig procedure.

Den godkendte politik vil blive formidlet til medarbejderne på ISM INTRA og indgå i onboarding processen til nyansatte.

11. Eventuelt

CLSO indledte med at spørge om der er punkter til eventuelt.

CLSO gav ordet til DBV. DBV takkede for samarbejdet og oplyste, at hun trak sig fra udvalget, da hun med organisationsændringen ikke længere er koncern-CISO.

12. Næste møde

CLSO bemærkede, at næste møde afholdes den 23. maj 2024 kl. 13:00-14:30.