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: 17-09-2024
Enhed: ISDB-enheden
Sagsbeh.: UMH
Sagsnr.: 2024-5241
Akt-id.: 195341

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

Referat fra møde i CID-udvalg 3-2024

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

Dato for møde
10. september 2024

Deltagere

Medlemmer

Cecilie Louise Svane Olesen (CLSO), Økonomi og koncernstyring, forperson
Annette Baun Knudsen (ABKN), ISDB-enheden
Trine Brøbecher (TRBR), HR
Pernille Seaton (PSE), Intern Administration
Lene Jensen (LJE), IT

Observatører
Helle Ginnerup-Nielsen (HGN), DPO DEP

Ressourceperson
Frederik Kastoft-Davidsen (FKD), ISDB-enheden

Sekretariat
Uffe Munch Hansen, ISDB-enheden (referent)

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
2. Referat fra CID-udvalgsmøde den 23-05-2024.
3. Ny sammensætning af CID-udvalg
4. Retningslinjer for brug af departementets it-udstyr på ferier
5. Opdatering af vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens i departementet.
6. Vurdering af revisionserklæringer for ISM-hjemmesider i drift hos Béru
7. Orienteringspunkter
    a. Brud på persondatasikkerheden
    b. Status på arbejdet med fortegnelser.
    c. Orientering om awarenessaktiviteter.
    d. Orientering om møde i CID-koordinationsforum den 20. juni 2024
    e. Koncernfælles CID-politik – skriftlig godkendelse og videre proces.
    f. Statusmåling vedr. tekniske minimumskrav og opfølgning på ISO-modenhedsmåling.
8. Eventuelt
9. Næste møde

Referat

1. Velkomst og meddelelser

v/CLSO.

CLSO bød velkommen til de to nye medlemmer af CID-udvalget Pernille Seaton, Intern Administration og Lene Jensen, IT, som er indtrådt efter at IT-chef, Carsten Grage ikke længere er en del departementet, da CPR-kontoret er ressortoverført til Digitaliseringsministeriet pr. 29.august 2024.

2. Referat fra CID-udvalgsmøde den 23-05-2024

v/ CLSO

Indstilling
. / . Det indstilles, at CID-udvalget godkender referat fra CID-udvalgsmøde den 23-05-2024 (bilag 2.1).

Sagsfremstilling:
Referat fra CID-udvalgets møde den 23-05-2024 er udsendt til udvalgets medlemmer den 4. juli 2024. Der er ikke modtaget bemærkninger til referatet.

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

Bilag
2.1. Referat fra CID-udvalgsmøde 23-05-2024.

Beslutning
Udvalget godkendte referatet uden yderligere bemærkninger.

3. Ny sammensætning af CID-udvalg

V/CLSO

Indstilling
Det indstilles, at CID-udvalget godkender den nye sammensætning af udvalget (bilag 3.1)

Sagsfremstilling:
Som følge af at ressortansvaret for CPR-administrationen er overført til Digitaliseringsministeriet ved kongelig resolution af 29. august 2024 udtræder Carsten Grage af CID-udvalget.

Pernille Seaton og Lene Jensen indtræder som ordinære medlemmer i CID-udvalget som ansvarlige for IT.

Bilag
Bilag 3.1 Medlemmer af CID-udvalget pr. 10-09-2024

ABKN bemærkede, at Philip Joen Bujnoch (PJB) vil udtræde af CID-valget som observatør, da det ifm. resortomlægningen er besluttet at arbejde henimod at koncernfælles DPO, Helle Ginnerup-Nielsen, bliver DPO for Benchmarkingenheden i stedet for PBJ, og departementets DPA også bliver DPA for Benchmarkingenheden. ABKN oplyste, at Helga Nielsen (HBN) starter i ISDB-enheden pr. 1. oktober som DPA for departementet, DKEtik og Benchmarkingenheden. HBN vil desuden sammen med Uffe Munch Hansen, ISDB-enheden, fremover være sekretariat for CID-udvalget.

Beslutning
Udvalget godkendte den nye sammensætning af CID-udvalget. Det blev endvidere besluttet, at ABKN går videre med at få det formelle på plads i forhold til, at Benchmarkingenheden som beskrevet bliver en del af den koncernfælles DPO-ordning.

4. Drøftelse vedr. retningslinjer for brug af departementets it-udstyr på ferier

/CLSO

Indstilling
Det indstilles, at CID-udvalget drøfter og beslutter, om og i hvilket omfang medarbejdere må medbringe departementets it-udstyr på ferier.

Sagsfremstilling
På udvalgets møde den 23. maj 2024 blev Retningslinjer for medarbejdere om informationssikkerhed i departementet godkendt. Ved den efterfølgende præsentation i chefgruppen den 12. juni 2024 blev det besluttet, at retningslinjerne vedrørende brug af departementets it-udstyr på rejser skulle præciseres og formidles, så der ikke opstår tvivl om, hvordan man som medarbejder skal forholde sig.

ISDB-enheden er i forlængelse heraf i færd med at udarbejde nye retningslinjer for medarbejderes brug af it-udstyr på rejser m.v. Inden CID-udvalget kan præsenteres for udkastet til retningslinjer, er der behov for at drøfte, hvilken linje det vil være mest hensigtsmæssigt at lægge ift. brug af it-udstyr på ferier.

Til baggrund for drøftelsen vedlægges ISDB-enhedens udkast til risikoanalyse (bilag 1), som også skal danne grundlag for de kommende retningslinjer for brug af departementets it-udstyr på rejser.

Det fremgår heraf, at ISDB-enheden vurderer, at indenrigsrejser kan sidestilles med rejser til andre EU/ EØS-lande samt NATO-lande, herunder ift. hvilke forholdsregler medarbejder skal tage undervejs. ISDB-enheden vurderer videre, at medarbejdere bør medbringe særligt rejseudstyr på tjenesterejser udenfor EU, EØS og NATO-lande.

CFCS fremhæver centralt placerede embedsmænd og ministre som oplagte mål for spionage og cyberspionage, hvorfor ISDB-enheden udarbejder supplerende retningslinjer for denne medarbejdergruppe, herunder ift. træning og awareness. AC og DC's sikkerhedshærdede enheder bør f.eks. ikke medbringes udenfor EU, EØS og NATO-lande.

Fra et rent cyber- og informationssikkerhedsmæssigt perspektiv ville det være mest hensigtsmæssigt, hvis departementets it-udstyr ikke måtte medbringes på ferier, bl.a. fordi udstyret i reglen vil være mindre under opsyn. I øvrigt bemærkes det, at

medarbejder vil være kontaktbar via privat telefon.

Som det fremgår af CID-politikken, pkt. 5, skal CID-udvalgets beslutninger bygge på et afvejet helhedshensyn, hvor bl.a. cyber- og informationssikkerhed, brugervenlighed og økonomi balanceres, og det er centralt, at indsatsen er proportional med truslerne for organisationen, de registrerede m.v.

ISDB-enheden foreslår på den baggrund, at udvalget drøfter behovet for, at medarbejdere har tilgang til departementets it-udstyr på ferier (udenfor hjemmet og sommerhuset), herunder:

- Evt. behov for at differentiere retningslinjerne efter medarbejderindplacering.
- Evt. behov for at lade AC og DC medbringe rejseudstyr på ferier uden for EU/EØS og NATO-lande.

Videre proces

ISDB-enheden indarbejder udvalgets beslutning vedr. medarbejderes brug af it-udstyr på ferier i de kommende retningslinjer for medarbejderes brug af departementets it-udstyr på rejser, som vil blive forelagt til godkendelse for CID-udvalget.

ISDB-enheden vil desuden på et kommende møde lægge op til en særskilt drøftelse vedr. informationssikkerhed og medarbejdertelefoner, der benyttes til både private- og tjenesteformål.

Bilag

Bilag 4.1. Udkast til Risikovurdering vedr. medarbejders brug af departementets it-udstyr på farten og på rejser

CLSO indledte med at ridse baggrunden op, herunder ønsket fra chefgruppen om at få præciseret retningslinjer for it-udstyr på rejser.

CLSO gav herefter ordet til ABKN, der bemærkede, at punktet er til drøftelse, og at det alene handler om retningslinjer for brug af departementets it-udstyr på ferier.

TRBR bemærkede, at det er trygt for husets medarbejdere, at der kommer fælles og entydige retningslinjer for anvendelse af it-udstyr på ferie og på tjenesterejser.

Der var herefter en længere drøftelse på mødet om praksis i det tidligere IM og SUM ift. private rejser og en mulig skitse til fremtidige retningslinjer.

Der var enighed om, at departementets it-udstyr ikke medbringes på ferierejser, medmindre der er et arbejdsbetinget behov for, at it-udstyret medbringes. Det betyder, at der skal tages konkret stilling til, om it-udstyr kan medbringes på ferier. Der var endvidere enighed om, at retningslinjerne både for ferier og for tjenesterejser skal være enkle og overskuelige at finde rundt i, og at der bør differentieres efter følgende kategorier:

Tjenesterejse /privat ferie
Udstyrstype (SIA-PC, telefon, ipad)
Geografi
Medarbejder/Chef

Drøftelsen vedr. medtagelse af departementets it-udstyr på private ferier er her samlet op i skemaform:

Rejsezone	Iphone/Ipad	SIA-PC
Hvid zone (Hjem/Sommerhus)	Kan medbringes	Kan medbringes
Gul Zone (DK, EU/EØS/NATO)	Chefer m.fl.[1] kan medbringe, hvis arbejdsbetinget behov Medarbejdere: Kun efter aftale med nærmeste chef. Chef kan give tilladelse, hvis der er et arbejdsbetinget behov, eller medarbejderen har valgt at anvende sin arbejdstelefon privat.	Chefer kan medbringe, hvis arbejdsbetinget behov. Medarbejdere: Som altovervejende hovedregel kan medarbejdere ikke medbringe SIA-PC på ferier. Nærmeste chef kan dog give tilladelse, hvis der er et arbejdsbetinget behov.
Rød	Chefer m.fl.: Der var ønske om, at ISDB-enheden undersøger muligheden for, at chefer i særlige tilfælde og under iagttagelse af særlige foranstaltninger kan medbringe Iphone/Ipads. Medarbejdere: Som udgangspunkt ikke tilladt Der var enighed om, at det skal undersøges nærmere, hvordan man forholder sig til medarbejdere, der bruger deres arbejdstelefon privat.	SIA-PC kan ikke medbringes på ferier i rød zone. Hvis chefer – eller medarbejdere efter aftale med chefer - i helt ekstraordinære tilfælde har behov for at medbringe en computer, skal ISDB-enheden og Intern-IT kontaktes og særlig rejseudstyr rekvireres
Mørkerød	Iphone/ipads kan ikke medbringes. Chefer kan få stillet rejsemobil til rådighed under ferien, hvis arbejdsbetinget behov.	Arbejdscomputer (SIA-PC) kan ikke medbringes. Chefer kan efter aftale med ISDB og Intern IT få stillet rejse PC til rådighed under ferien, hvis arbejdsbetinget behov.

Beslutning/videre proces:
Det blev besluttet, at ISDB-enheden indarbejder udvalgets beslutning vedr. medarbejderes brug af it-udstyr på ferier i de kommende retningslinjer for medarbejderes brug af

[1] Chefer m.fl. kan f.eks. omfatte: Sektionsledere, kontorchefer, afdelingschefer, departementschef, minister og særlig rådgiver. Den nærmere afgrænsning besluttes på næste møde

departementets it-udstyr både for tjenesterejser og for ferierejser, som vil blive forelagt til godkendelse for CID-udvalget på næste møde. ISDB-enheden undersøger i den forbindelse, om der kan træffes foranstaltninger, som gør det muligt at medbringe iphone/ipad i rød zone. Efter vedtagelse i CID-udvalget skal retningslinjerne behandles i Samarbejdsudvalget med tidlig inddragelse af tillidsrepræsentanter.

ISDB-enheden vil på næste møde også lægge op til en særskilt drøftelse vedr. informationssikkerhed og medarbejdertelefoner, der benyttes til både private- og tjenesteformål. TRBR vil til brug herfor undersøge, om det er muligt at trække en liste over medarbejdere, som bliver beskattet af privat brug af arbejdstelefon med henblik på at få belyst, hvor stor en gruppe, der kan være tale om.

5. Opdatering af vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens i departementet

V/CLSO

Indstilling

Det indstilles, at CID-udvalget godkender:

- Opdatering af 'Vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens i departementet'.

Sagsfremstilling

Den nuværende vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens i departementet har givet anledning til, at en ansat har efterspurgt en nærmere beskrivelse af, hvilke oplysninger der er beskyttelsesværdige ift. brug af generativ AI. Vejledningen er derfor blevet opdateret med en henvisning til det relevante afsnit i Indenrigs- og Sundhedsministeriets retningslinjer om informationssikkerhed.

ISDB-enheden foreslår desuden, at der i retningslinjerne indsættes et nyt krav om, at medarbejdere skal benytte ikke-personhenførbare e-mailadresser ved brug af generativ kunstig intelligens. Denne foranstaltning vurderes at reducere risikoen for, at personoplysninger om ansatte i departementet bliver videregivet til tredjemand.

De foreslåede ændringer fremgår med TC i vedlagte bilag 5.1.

Den videre proces

Efter godkendelse vil de opdaterede retningslinjer blive sendt til Samarbejdsudvalget til orientering og desuden blive offentliggjort på ISM-intra

Bilag

Bilag 5.1 Vejledning til medarbejdere om departementets retningslinjer for brug af generativ AI med TC i Track v1.1

ABKN indledte med at bemærke, at vejledningen er ændret efter en konkrete henvendelse ifm. med brugen af de nuværende regler, samt at der udestår en grundlæggende risikovurdering af departementets brug af generativ kunstig intelligens.

HGN bemærkede, at det – også i lyset af tidligere sikkerhedsbrud i bl.a. departementet – er forventeligt, at de fleste medarbejdere ikke har den fornødne viden om, hvornår oplysninger er personhenførbare og dermed i henhold til retningslinjen ikke må deles med AI-værktøjer. HGN anbefalede derfor, at dette tydeliggøres direkte i vejledningen vedr. AI i

stedet for blot at have en henvisning til det relevante afsnit vedr. persondata og fortrolighed i Indenrigs- og Sundhedsministeriets generelle retningslinjer til medarbejdere om Informationssikkerhed. HGN bemærkede i øvrigt, at denne retningslinje ikke som forudsat indeholder en beskrivelse af, hvad persondata er.

Beslutning
ISDB-enheden tilretter vejledningen og sender til skriftlig godkendelse sammen med referatet. Den foreslåede videre proces blev godkendt, dvs. at retningslinjerne sendes til Samarbejdsudvalget til orientering og efterfølgende bliver de offentliggjort på ISM-intra.

6. Vurdering af revisionserklæringer for ISM-hjemmesider i drift hos Béru

v/ABKN

Indstilling: Det indstilles,
at CID-udvalget behandler revisionserklæringen med henblik på at vurdere, om der er forhold, der skal løftes over for leverandøren Béru på næstkommende driftsmøde.

Sagsfremstilling:
Revisionserklæringen fra Béru udføres årligt som en del af kontraktgrundlaget. CID-udvalgets gennemgang udgør departementets tilsyn med databehandlerenBéru.

Det bemærkes, at ISM generelt kun behandler almindelige personoplysningerne på hjemmesiderne – f.eks. ministerens profil. Résumedatabasen (afgørelser på om kommunalfuldmagten) anvender anonymiserede afgørelser.

ISAE 3000 type-II erklæringen gælder for perioden februar 2023 til januar 2024 og dækker over omfanget af behandlingen af personoplysninger som Beru varetager i deres rolle som databehandler for departementet. Erklæringen indeholder kun en bemærkning om, at test af reetablering sidst er udført i november 2022, og planlægges udført i november 2024. I øvrigt er den fri for anmærkninger
Den videre proces: CID-udvalgets vurdering føres til referat. Det er Kommunikation og Presse, som er ansvarlig for kontrakten med Béru.

Bilag:
Bilag 6.1 Beru´ - Ledelseserklæring ISAE 3000 om informationssikkerhed 2024
Bilag 6.2 Beru´ - Uafhængig revisors ISAE 3000 erklæring om persondata 2024.

ABKN indledte med at bemærke, at det ikke er hensigten, at CID-udvalget fremadrettet skal godkende revisionserklæringer som led i departementets tilsyn med databehandlere. ISDB-enheden vil udarbejde forslag til proces for tilsyn med databehandlere, som formentlig vil indebære en årlig orientering af CID-udvalget om gennemførelse af tilsyn med databehandlere, bortset fra tilsynet med SIT, som fortsat vil blive forelagt CID-udvalget til godkendelse.

Beslutning
Udvalget godkendte tilsynet og revisionserklæringen uden bemærkninger.

7. Orientering

7.a Brud på persondatasikkerheden
v/ABKN

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

Sagsfremstilling
I perioden fra 1 maj 2024 til 1. september 2024 har der været syv hændelser

Beskrivelse af hændelse	Brud på persondatasikkerhed	Anmeldt til Datatilsynet
1) Dokumenter med persondata tilgængelig på fælles drev.	Ja	**Nej**
2) Manglende kryptering af SMS-data opbevaret hos SIT	**Ja**	**Nej**
3) Sikkerhedshændelse: AskCody – brugere blev omdirigeret til falsk hjemmeside.	Nej	
4) Sikkerhedshændelse: Oplysninger om arbejdsskade sendt fra AES til forkert kontor i ISM	Nej	
5) Mail sendt til forkert person i DEP.	Ja	**Nej**
6) Mistet PC /Telefon	**Ja**	**Nej**
7) Sikkerhedshændelse: SIT – netværksnedbrud med manglende tilgængelighed	Nej	**Nej**

Alle sager er lukkede undtagen sagen om kryptering af SMS data, som afventer svar fra SIT. Sagen blev drøftet på sidste CID-udvalgsmøde (se pkt. 7 i referatet af CID-udvalgsmødet den 23. maj). Forespørgslen angår om data er krypterede.

Der har ikke været systematisk genkommende sikkerhedsbrud, der har givet anledning særskilt læring eller ændret praksis. Ingen af sagerne er anmeldt til Datatilsynet. Det er ISDB-enhedens vurdering, at der er et mørketal, idet ikke alle medarbejdere er opmærksomme på, hvornår en sikkerhedshændelse skal indberettes. ISDB-enheden har et særligt fokus på at informere om dette ifm. awarenessaktiviteter, jf. pkt. 7. c.

ABKN oplyste indledningsvis, at overskriften "Databrud" skal rettes til "Brud på persondatasikkerheden". *Dette er efterfølgende ændret i boksen ovenfor.*

LJE oplyste, at sagen vedr. hændelse nummer 2) Evt. manglende kryptering af SMS-data opbevaret hos SIT kan lukkes, idet SIT er vendt tilbage med oplysning om, i hvilket omfang, der har ligget ukrypterede SMS-data på fælles drev hos SIT.

HGN foreslog, at der ved næste afrapportering kommer flere informationer om de respektive brud med i orienteringen til CID-udvalget. HGN bemærkede desuden, at en enkelt af de hændelser, som fremgår af oversigten, muligvis bør omkategoriseres til at være brud på persondatasikkerheden. Det blev i den forbindelse kort drøftet, hvordan Datatilsynet vejledning "Håndtering af brud på persondatasikkerheden", Juli 2024 skal

forstås i relation til tilfælde, hvor it-udstyr med krypterede data er tabt, da vejledningen ikke er entydig efter den seneste opdatering. ABKN oplyste, at ISDB-enheden i lyset af bemærkningerne vil se nærmere på afrapporteringens indhold og form, herunder kategorisering af hændelserne.

ISDB-enheden har efter mødet lukket sagen vedr. ukrypterede SMS-data, efter at SIT har fjernet de SMS-backupfiler fra ISM, der ikke var krypterede. Det fremgår af CTJ's tilsynsrapport, at ansatte i SIT ikke har tilgået kundernes SMS backup-data. Der henvises i den forbindelse til pkt. 7 i referat fra CID-udvalgsmøde afholdt den 23. maj 2024. ISDB-enheden vurderer på den baggrund, at der har været et brud på persondatasikkerheden, men at dette ikke skal anmeldes til Datatilsynet. Dette er efterfølgende ændret i oversigten ovenfor. Hændelse nr. 6 er desuden ændret til at være kategoriseret som et brud på persondatasikkerheden. Ændringer er markeret med fed. ISDB-enheden har samtidig opdateret hændelserne i enhedens interne sag vedr. sikkerhedshændelser.

7.b Status for opdatering af fortegnelser

v/ABKN

Indstilling

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

Sagsfremstilling

ISDB-enheden har påbegyndt et projekt med opdatering af Indenrigs- og Sundhedsministeriets departements fortegnelser. I den forbindelse har enheden udarbejdet en overordnet projektplan der beskriver påbegyndelsen af projektet i Q3 2024 til afslutning af projektet ved udgangen af Q1 2025.

Projektet er inddelt i tre delprojekter:

1. Forberedelse Q3 – Q4 2024
2. Opdatering af fortegnelse Q4 2024
3. Udvikling og implementering af kontrolforanstaltninger Q1 2025

Hvert delprojekt er brudt ned i konkrete operationelle opgaver, hvor roller og ansvar er beskrevet. Der vil løbende blive afrapporteret om fremdrift til CID-udvalget. Da arbejdet med opdatering også vil involvere fagkontorer, vil ISDB-enheden informere om opstart af projektet på et chefmøde.

Bilag

Bilag 7.b.1 – Opdatering af fortegnelse 2024 – Projektplan

ABKN gav ordet til FKD, som orienterede om, at ISDB har udarbejdet en projektplan for opdatering af fortegnelserne i departementet. Projektplanen er inddelt i tre delprojekter og brudt ned i opgaver, produkter og relevante interessenter. ISDB-enheden har påbegyndt forberedelser i overensstemmelse med projektplanen og har bl.a. konsolideret eksisterende fortegnelser fra IM og SUM, valgt skabelon og vurderet formkrav. Det videre arbejde vil blive overdraget til ISDB-enhedens nye DPA, som vil forestå og koordinere det videre arbejde i overensstemmelse med projektplanen.

FKD bemærkede, udvikling og implementering af kontrolforanstaltninger for kontinuerlig opdatering af fortegnelser, som beskrevet i delprojekt 3, kunne være udfordrende og

ressourcekrævende i departementet, som følge af det decentrale risikoejerskab i departementet ifm. indkøb af systemer og nye projekter. Delprojektet var derfor placeret i Q1 2025.

TRBR bemærkede, at to måneder er kort tid til at opdatere fortegnelser, så HR vil gerne betænkes med hjælp og vejledning, når bestillingen sendes ud.

HGN bemærkede, at der i forbindelse med opdateringer af fortegnelser som en positiv bivirkning typisk sker det, at man opdager mangler/afvigelser ift. andre krav i GDPR – f.eks. oplysningspligten – som man dog ikke nødvendigvis kan rette op på med det samme.

HGN anbefalede derfor, at systematisk registrering af og overblik over sådanne afvigelser indtænkes i både fortegnelsesprojektet og mere generelt, så de kan indgå i departementets samlede prioritering af opgaver på CID-området.

7.c Orientering om awarenessaktiviteter
v/ABKN

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

Sagsfremstilling
ISDB-enheden har som en del af arbejdet med efterlevelsen af ISO27001 og ISO27701-standarderne, udviklet en kommunikationsstrategi vedr. informationssikkerhed og databeskyttelse for 2024. Som følge af denne strategi, har ISDB-enheden i de første tre kvartaler i 2024 fokuseret på følgende bevidsthedsskabende tiltag i Indenrigs- og Sundhedsministeriets departement:

- Formidling af retningslinjer og vejledninger i departementet
- Bevidsthed omkring ISDB-enheden og dens arbejdsopgaver samt snitflader til resten af departementet

I den forbindelse har ISDB-enheden udviklet og dokumenteret en række bevidsthedsskabende produkter (præsentationer, intranetopslag, og plakater), samt afholdt fysiske præsentationer for chefgruppen, afdelinger, samt kontorer (Bilag 7.c.1).

Resten af året vil ISDB-enheden fortsætte arbejdet med at realisere kommunikationsstrategien, samt udbygge strategien med en kampagne ifm. den nationale cybersikkerhedsmåned, til afvikling oktober 2024.

Bilag 7.c.1 Awarenessoverblik 2024

ABKN oplyste, at ISDB-enheden har informeret om retningslinjer for informationssikkerhed på flere kontormøder og et afdelingsmøde, jf. bilag 7.c., og at der p.t. er planer om at besøge yderligere to kontorer. Informationsmøderne har givet anledning til både at præsentere ISDB-enheden og de vedtagne retningslinjer for Informationssikkerhed. ISDB-enheden er også blevet en del af introduktionsprogrammet for nye medarbejdere med en 45 minutters præsentation af ISDB-enheden og retningslinjerne.

TRBR kvitterede med, at det gav tryghed i huset at medarbejderne er informerede om retningslinjerne.

FKD bemærkede, at plakaterne kommer i flere udgaver, som også har til hensigt at henlede opmærksomheden på ISDB-enheden som en ny enhed i DEP.

7.d Orientering om møde i CID-koordinationsforum den 20. juni 2024
v/ABKN

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

7.e Koncernfælles CID-politik.
v/ABKN

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

Sagsfremstilling:
Den overordnede koncernfælles CID-politik er godkendt i skriftlig proces af CID-udvalget. Når den koncernfælles CID-politik er godkendt af alle institutioner i koncernen, vil den blive forelagt KLF/Styringsforum.

ABKN oplyste, at den koncernfælles CID-politik er en overordnet politik, og at de enkelte institutioner herudover skal have deres egen CID-politik, ligesom vi også har i departementet.

Orienteringen vedr. pkt. 7.d og 7.e. blev taget til efterretning.

7.f Statusmåling vedr. tekniske minimumskrav samt opfølgning på ISO-modenhedsmåling.
v/ABKN

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

Sagsfremstilling:
I regi af den nationale strategi for cyber- og informationssikkerhed følger Digitaliseringsstyrelsen op på implementeringen af de tekniske minimumskrav og ISO 27001 i de statslige myndigheder. Digitaliseringsstyrelsen har ved brev af 2. septemer 2024 varslet, at bestillingen for 2. halvår 2024 forventes at blive udsendt d. 9. september med svarfrist 11. oktober. Det vil være første gang, der afrapporteres på de 29 tekniske minimumskrav, som er trådt i kraft 1. juli. Bestillingen vedr. ISO 27001 vil rette sig mod de ministerier, der i foråret 2024 ikke var i mål og derfor har fremsendt handleplaner. Disse ministerier skal give en status på, hvordan det går med tiltagene til Digitaliseringsstyrelsen. Departementet, ekskl. CPR-kontoret meldte i foråret ind, at vi var i mål med 2 ud af 9 spørgeområder og af handleplanen fremgår det, at departementet forventer at være på modenhedsniveau 4 på hovedparten af spørgeområderne i 2024 og alle spørgeområder i 2025.

ISDB-enheden vil inddrage IT i besvarelse af bestillingen for departementet og

besvarelsen vil blive forelagt CID-udvalget til godkendelse i skriftlig proces, da svarfristen er før næste ordinære møde i CID-udvalget.

Orienteringen blev taget til efterretning

8. Eventuelt

ABKN orienterede om, at BESS i samarbejde med Intern administration, ISDB og IT er ved at udforme et snitfladepapir mellem de kontorer i ISM, der arbejder med sikkerhed og beredskab. CLSO oplyste, at dette navnlig har til formål at give direktion et overblik over, hvem man skal gå til ift. hændelser og spørgsmål.
PSE oplyste, at der er et projekt i gang omkring fysisk sikkerhed på Slotsholmen

9. Næste møde

Næste møde afholdes torsdag den 12-12-2024 kl. 10.00-11.30 (flyttet fra 13-11-2024 som meddelt i særskilt mail).