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: 07-05-2025
Enhed: ISDB-enheden
Sagsbeh.: HBN/ABKN
Sagsnr.: 2024-15445
Akt-id.: 5108911

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

Udkast til referat for møde i CID-udvalg 1-2025

Dato for møde
20. marts 2025

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

Ressourcepersoner
Sarah Michelle Bensley (SMB), BESS, på vegne af Anna Nielsen Kjær, (ANKJ), BESS
Frederik Kastoft-Davidsen (FKD), ISDB

Sekretariat
Uffe Munch Hansen (UMH), ISDB
Helga Brask Nielsen (HBN), DPA

Afbud
Helle Ginnerup-Nielsen (HGN), DPO DEP

Indhold

Dagsorden

1. Velkomst

v/ CLSO

CLSO bød velkommen, herunder til Sarah Michelle Bensley (SMB), BESS som deltog som repræsentant for BESS.

2. Referat fra CID-udvalgsmøde den 13-12-2024

v/ CLSO

Indstilling
Det indstilles, at CID-udvalget godkender referat fra CID-udvalgsmøde den 13-12-2024

Sagsfremstilling:
Referat fra CID-udvalgets møde den 13-12-2024 (bilag 2.1) blev udsendt til godkendelse i skriftlig proces i F2. Referatet blev godkendt uden bemærkninger.

Bilag
2.1. Referat fra CID-udvalgsmøde 13-12-2024

Videre proces
Med udvalgets godkendelse vil referatet blive offentliggjort på intranettet.

Beslutning
Udvalget godkendte referatet.

3. Status på risikovurdering af auto-complete og drøftelse af den videre proces ift. udarbejdelse af risikostyringsproces i departementet

v/ ABKN

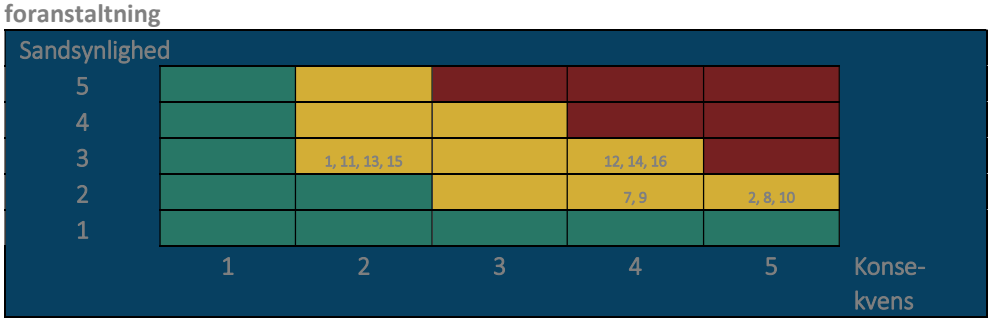
Indstilling
Det indstilles,
at CID-udvalget drøfter erfaringerne med risikostyringsprocessen ift. auto-complete
at CID-udvalget godkender den videre proces ift. udarbejdelse af risikostyringsproces i departementet

Sagsfremstilling
På møde i Q4 blev CID-udvalget orienteret om status på udarbejdelse af risikovurdering i forlængelse af brev af 1.oktober 2024 fra Ministeriet for samfundssikkerhed og beredskab, hvori det understreges, at det er vigtigt, at alle statslige myndigheder foretager en risikovurdering af auto-complete-funktionen og herefter gennemfører eventuelle tekniske foranstaltninger for at mindske risikoen for fejlfremsendelser af oplysninger til uvedkommende.

ISDB har i forlængelse heraf udarbejdet en risikorapport for auto-complete i Outlook og Boxer) (bilag 3.1.) Risikorapporten består af en risikovurdering, en beskrivelse af risikobilledet for hhv. departementet og de registrerede og et afsnit vedr. risikohåndteringsmuligheder.

Det fremgår videre af rapporten, at HR har valgt at implementere en organisatorisk foranstaltning i form af en oplysningskampagne, der modificerer en række risikoscenarier for den registrerede i forbindelse med brugen af auto-complete-funktionen i Outlook. Oplysningskampagnen vedrører e-mailkommunikation om personalesager, som håndteres af chefer og HR. Risikobilledet for departementet og for den registrerede efter implementering af denne foranstaltning fremgår af rapporten og er også indsat her:

Risikobillede for departementet og den registrerede efter implementering af planlagt foranstaltning



Videre proces ift. udarbejdelse af risikostyringsproces i departementet

Risikovurderingen auto-complete og boxer har benyttet sig af det udkast til konsekvens- og sandsynlighedsskalaer for hhv. den registrerede og departementet jf. bilag 3.3. Dette udkast svarer med enkelte tilpasninger til det udkast, der blev fremlagt på mødet den 23. maj 2024. Næste skridt er, at konsekvens- og sandsynlighedsskalaerne skal afstemmes og kvalificeres af de relevante kontorer i departementet. ISDB har påbegyndt dette arbejde og har på nuværende tidspunkt afstemt konsekvens- og sandsynlighedsskalaerne med DPO og IT og vil endvidere inden CID-udvalgsmødet i Q3 2025 færdiggøre afstemningen af konsekvens- og sandsynlighedsskalaerne Presse og kommunikation, KOK og andre relevante kontorer/enheder, herunder Demokrati og Kommunal- og Regional Finansiering i forhold til den operationelle skala.

Konsekvensskalaerne omfatter konsekvenser for den registreredes databeskyttelse, og konsekvenser for departementets omdømme, økonomi og operationelle konsekvenser. Det blev på CID-udvalgsmødet den 23. maj 2024 besluttet *"I forhold til det videre arbejde med risikostyringsproces vil dette tage udgangspunkt både i udkast til risikostyringsproces, som blev drøftet på CID-udvalgsmødet den 23. maj 2024 og de eksisterende risikovurderinger..."*.

ISDB har i forlængelse heraf dannet sig flg. overblik over de eksisterende risikovurderinger, som allerede er udarbejdet i departementet i de kontorer, som var en del af det tidligere Indenrigs- og boligministerium (IBM). De processer og systemer, som er udarbejdet risikovurderinger for, er:

- Det kommunale og regionale udligningssystem (Kommunal og regional finansiering)
- Valg (Demokrati)
- F2 hostet hos Cbrain
- Mailsystemet samt generel drift af it-infrastrukturen hos SIT

De eksisterende risikovurderinger vil indgå i det videre arbejde, når risikovurderingerne skal overføres til det nye koncept for risikostyring.

Bilag
Bilag 3.1 Risikorapport for auto-complete i Outlook og Boxer
Bilag 3.2 Risikovurdering af auto-complete i Outlook og Boxer
Bilag 3.3 Konsekvens- og sandsynlighedsskalaer (version 0.3)

Referat
CLSO indledte med at orientere om baggrunden for iværksættelse af risikovurdering af auto-complete i Outlook, herunder henvendelsen fra MSSB, og gav herefter ordet til FKD. FKD gennemgik risikovurderingen og afsluttede med at oplyse, at der udestår stillingtagen til, om CID-udvalget skal acceptere risikobilledet, som det ser ud nu, eller om risikobilledet skal modificeres yderligere ved at gennemføre en teknisk foranstaltning, der består i, at afsenderen bliver adviseret ved afsendelse af e-mails til eksterne modtagere uden for SIT's domæne, som beskrevet i risikorapporten (se bilag 3.1).

CID-udvalget drøftede, i hvilken enhed/for hvilke brugere det ville give bedst mening at afprøve foranstaltningen for at afdække, hvor forstyrrende det er for brugerne.

FKD supplerede desuden dagsordenspunktet med at præcisere, at konsekvens- og sandsynlighedstabellerne vil blive forelagt CID-udvalget, når de er afstemt med de respektive enheder.

HR v/ TRBR orienterede om status på oplysningskampagnen.

Beslutning
CID-udvalget besluttede endvidere, at ISDB afprøver den tekniske foranstaltning i en periode, og at CID-udvalget på baggrund af ISDB's erfaringer beslutter, om den tekniske foranstaltning skal gennemføres i hele departementet. Den foreslåede videre proces for godkendelse af konsekvens- og sandsynlighedstabeller blev godkendt.

4. Udkast til roller og ansvar i CID-arbejdet i Indenrigs- og Sundhedsministeriets departementet

v/ UMH

Indstilling
Det indstilles,
at CID-udvalget drøfter udkastet til roller og ansvar i CID-arbejdet (vedlagt som bilag 4.1)
at CID-udvalget godkender videre proces, herunder at udkastet anvendes som grundlag for det videre arbejde med risikostyringsproces og udarbejdelse af systemlister

Sagsfremstilling
Det er et grundlæggende krav i ISO-standarden 27001, at roller og ansvar for informationssikkerheden og databeskyttelse i en organisation er veldefineret og kommunikeret. SoA-dokumentet angiver i krav 5.2, at *"Roller og ansvar for informationssikkerhed skal defineres og allokeres i overensstemmelse med organisationens behov."* I vejledning til krav 5.2 står der bl.a.:

"Organisationen bør definere og styre ansvaret for

a) beskyttelse af information og understøttende aktiver
b) gennemførelse af specifikke informationssikkerhedsprocesser
c) informationssikkerhedsmæssige risikostyringsaktiviteter og især accept af restrisiko (fx for risikoejere)
d) alle medarbejdere, der benytter en organisations information og understøttende aktiver."

Udkast til roller og ansvar i CID-arbejdet i Indenrigs- og Sundhedsministeriets departement (bilag 4.1) har til formål at efterleve dette krav.

Nærmere om indholdet af udkast til roller og ansvar (bilag 4.1.)

Dokumentet tydeliggør rollernes betydning i CID-arbejdet og konkretiserer det ansvar, der påhviler den enkelte rolle både i forhold til CID-arbejdet generelt og i risikostyringsprocessen.

Dokumentet trækker for nogle rollers vedkommende på information fra andre definerende dokumenter i ledelsessystemet, som f.eks. CID-politik og kommissorium for CID-udvalget.

For andre roller, som f.eks. rollen som system/procesejer vil dokumentet være definerende og retningsgivende for både det daglige sikkerhedsarbejde og for roller og ansvar i risikostyringsprocessen. Overskriften på disse afsnit er markeret med rødt i udkastet.

Det fremgår bl.a. af udkastet at:

"Alle væsentlige it-systemer og forretningskritiske processer i ISM har en system/procesejer. System/procesejeren vil være den chef, der er ansvarlig for systemet/processen.".

System- og procesejere er risikoejer på de risici, der er tilknyttet systemet/processen.

Risikoejerskab er defineret som:

"Den person eller afdeling som er ansvarlig for at håndtere sikkerheds- og databeskyttelsesmæssige trusler og sårbarheder relateret til et specifikt aktiv, som personen eller afdelingen har ansvaret for og muligheden for at påvirke"

I dokumentet står der endvidere flg.:

"Systemer i staten er i flere tilfælde leveret centralt og obligatoriske for departementet at bruge. Det gælder f.eks. IT-infrastruktur leveret af SIT og fællesstatslige digitale løsninger leveret af Økonomistyrelsen. System- og procesejere vil i disse situationer kun i begrænset omfang eller slet ikke have mulighed for at påvirke eller iagttage ansvaret, som de i dette dokument har som system- og procesejere. I sådanne tilfælde vil iagttagelsen af ansvaret skulle adresseres ifm. leverandørstyring.

Systemejer/procesejer er ansvarlig for:

<u>Generelt</u>

- *at udarbejde retningslinjer for adgang (administrativ/systemadgang og brugeradgang) til systemer og data og administrere disse i det daglige i samarbejde med IT*

- *at sikrer, at systemet løbende sikkerhedsopdateres i samarbejde med IT*
- *at udarbejde it-beredskabsplaner for det pågældende system og teste disse med regelmæssige mellemrum*
- *at inddrage ISDB ved nyanskaffelser af it-systemer.*
- *at inddrage ISDB ifm. ændringer i processer der kan påvirke ledelsessystemet nye datakategorier, nye formål eller væsentlige ændringer i retningslinjer eller procedurer.*
- *at ISDB informeres om væsentlige drifts- eller sikkerhedsmæssige hændelser i systemet.*
- *at udarbejde it-beredskabsplaner for det pågældende system og teste disse med regelmæssige mellemrum*
- *at systemet lever op til eksterne og interne sikkerhedskrav og forventninger som f.eks. de tekniske minimumskrav og andre krav/anbefalinger fra kompetente myndigheder.*
- *at udarbejde og vedligeholde nødvendig dokumentation, herunder systemdokumentation, procesbeskrivelser, mødereferater og skriftliggørelse af aftaler med f.eks. leverandøren*

Leverandørstyring

- *at der føres tilsyn med eksisterende leverandører og at der udføres leverandørstyring ifm. leveringen af konsulentydelser eller systemydelser, herunder screening af nye leverandører*

Risikostyring

- *at gennemføre risikovurderinger og konsekvensanalyser i samarbejde med ISDB for det pågældende system i henhold til departementets risikostyringsproces.*
- *at udarbejde et beslutningsgrundlag for, hvilke sikkerhedsforanstaltninger, der skal gennemføres i relation til de risici, der er blotlagt ifm. risikovurderingen*
- *at godkende restrisici i henhold til departementets risikostyringsproces*

Hændelseshåndtering

- *at der afsættes interne ressourcer til hændelseshåndtering ifm. sikkerhedshændelser, så det er muligt at vurdere og anmelde sikkerhedshændelser i overensstemmelse med krav til rettidig anmeldelse til kompetente myndigheder.*
- *at registrere og følge op på sikkerhedshændelser i det pågældende system, og sikre at sårbarheder adresseres og korrigerende handlinger implementeres.*

Chefers og medarbejderes roller og ansvar er desuden beskrevet særskilt i dokumentet.

Sammenhæng med sikkerhedsorganisering i departementet
I forlængelse af beslutning på AC-møde i november 2024 er der igangsat et arbejde ift. at afklare og etablere en sikkerhedsorganisation i ISM, som bygger på den eksisterende organisering, men som i højere grad definerer en klar rolle- og ansvarsfordeling i relation til sikkerhedsarbejdet, som varetages i en række forskellige kontorer i ISM.

Arbejdsgruppens forslag skal forelægges styregruppen (AC-kredsen) til godkendelse. ISDB vil opdatere dokumentet vedr. roller og ansvar i den forbindelse, således at dokumentet vedrørende roller og ansvar afspejler den vedtagne sikkerhedsorganisation.

ISDB er desuden generelt ansvarlig for opdatering af dokumentet, som vil blive forelagt CID-udvalget ved væsentlige ændringer, dog mindst én gang årligt.

Videre proces

Dokumentet om roller og ansvar skal benyttes i det videre arbejde med risikostyringsprocessen og i forbindelse med udarbejdelse af systemliste.

Inden næste møde i CID-udvalget i Q3 vil ISDB på grundlag af data indsamlet ifm. bestillingen vedr. fortegnelser og efter dialog med IT udarbejde et udkast til liste over de væsentligste systemer i ISM med forslag til tilhørende System/procesejer.

Systemlisten og dokumentet vedr. roller og ansvar for system/proces-ejere vil derefter blive udsendt til de respektive kontorer for kvalificering ift. de oplysninger, som ISDB har indsamlet og vil efterfølgende blive forelagt for CID-udvalget.

Bilag
Bilag 4.1: Udkast til roller og ansvar i CID-arbejdet med i Indenrigs- og Sundhedsministeriets departement v1.0

Referat
UMH gennemgik udkastet, jf. bilag og dagsordenspunkt, og præciserede, at dokumentets primære formål er at beskrive og formidle rolle- og ansvarsfordeling ift. de opgaver, der følger af departementets ledelsessystem. Fx ift. risikostyringsprocessen og i det videre arbejde med udarbejdelse af systemlister.

UMH bemærkede generelt, at en systemejer/procesejer er ansvarlig for at håndtere sikkerheds- og databeskyttelsesmæssige trusler og sårbarheder relateret til en proces eller et system, som personen eller afdelingen har ansvaret for og muligheden for at påvirke.

Det betyder, at man som systemejer/procesejer ikke er forpligtet udover det, som man har mulighed for at påvirke, hvilket har særlig betydning i forhold til IT-infrastruktur leveret af SIT og fællesstatslige digitale løsninger leveret af Økonomistyrelsen.

Systemlisten vil, jf. videre proces, også inkorporere de vigtigste processer fra arbejdet med opdatering af fortegnelserne.

Beslutning
Indstillingen, herunder den foreslåede videre proces, blev godkendt af CID-udvalget.

5. Opfølgning obligatoriske kurser i Campus
v/ UMH

Indstilling
Det indstilles,
at CID-udvalget godkender, at de obligatoriske kurser i Campus skal gennemføres hvert andet år
at CID-udvalget godkender den videre proces

Sagsfremstilling
CID-udvalget besluttede på mødet den 23. maj 2024, at kurset "Cyber- og informationssikkerhed for topledere og ledere i staten" skulle føjes til listen over obligatoriske kurser, og at alle ledere i departementet skulle tage kurset, samt at de nuværende campus-kurser " Cyber- og informationssikkerhed for medarbejdere i staten" og "Databeskyttelse" skulle forblive obligatoriske for alle medarbejdere i departementet.

Det blev endvidere besluttet,

"At ISDB en gang årligt (i efteråret) trækker en liste over, hvem der har/ikke har gennemført kurserne det seneste år med henblik på at listerne kan forelægges CID udvalget listerne på mødet i november måned. CID-udvalget besluttede desuden, at denne status for gennemførsel af kurser skulle forelægges chefgruppen for så vidt angår medarbejdere og AC-gruppen for så vidt angår chefer."

Alle medarbejderne blev tilmeldt kurserne ultimo oktober 2024 med 90 dages frist for gennemførelse. Cheferne blev i mail af 27. november 2024 orienteret om, at kurserne skulle været gennemført med en frist på 90 dage.

ISDB har den 20. februar 2025 fået trukket en liste over gennemførte kurser et år tilbage. Tabellen nedenfor angiver antallet af medarbejdere og ledere, der har bestået eller ikke gennemført de obligatoriske kurser vedr. Informationssikkerhed og databeskyttelse i Campus:

Antal medarbejdere, der har bestået kurset "Introduktion til databeskyttelse"	191
Antal medarbejdere, der ikke har gennemført "Introduktion til databeskyttelse"	168
Antal medarbejdere, der har bestået "Cyber- og informationssikkerhed for medarbejdere i staten"	199
Antal medarbejdere, ikke har gennemført "Cyber- og informationssikkerhed for medarbejdere i staten	172
Antal ledere, der har bestået "Cyber- og informationssikkerhed for topledere og ledere i staten"	19
Antal ledere, der ikke har bestået "E-læring: Cyber- og informationssikkerhed for topledere og ledere i staten"	19

Det bemærkes, at kursisten skal have gennemført evalueringen af kurset før Campus rapporterer et kursus som bestået. En del af de medarbejdere, der står registreret som, at de ikke har gennemført, har således rent faktisk gennemført kurset, men ikke evalueringen.

Tallene er i samarbejde med Koncern-HR renset for fratrådte medarbejdere. Departementet har ca. 350 ansatte. Tallene for ikke gennemførte kurser og beståede kurser summer ikke op til dette antal, da en medarbejder kan bestå det samme kursus flere gange.

Videre proces

Status for gennemførelse af obligatoriske campuskurser forelægges chefgruppen for så vidt angår medarbejdere og AC-gruppen for så vidt angår chefer. Det betyder konkret, at kontorchefer og enhedsledere vi få tilsendt et uddrag af bilag 6.1 med en liste over kontorets/enhedens medarbejdere med status for beståede og ikke gennemførte kurser. Ligeledes vil afdelingschefer få tilsendt en liste med kontorchefers og enhedslederes beståede og ikke gennemførte kurser. Der vil i den forbindelse blive gjort opmærksom på, at kursisten skal have gennemført evalueringen af kurset, før kurset er registeret som bestået i Campus.

ISDB vil på næste CID-udvalgsmøde rapportere på status på gennemførte kurser pr. 1. juni 2025 og eventuelt gentage processen med breve til kontorchefer/enhedslederne.

ISDB vil fremadrettet melde alle medarbejdere til de obligatoriske kurser hvert andet år, næste gang i oktober 2026 med trækning af lister over gennemførte kurser 90 dage senere og afrapportering til CID-udvalget i Q4 2024. Alle nyansatte medarbejdere vil fortsat automatisk tilmeldes kurserne.

Bilag
Bilag 5.1 Liste fra Campus over deltagere i obligatoriske kurser vedr. Informationssikkerhed og databeskyttelse *(medbringes på mødet, sendes ikke med ud)*

Referat
UMH oplyste, at ca. 60 % har gennemført, 40 % har ikke. Det formodes, at mange medarbejdere ikke er bevidste om, at kurset først registreres som gennemført, når evaluering er gennemført. Der vil i lyset af den beskedne gennemførselsprocent blive fulgt op på næste møde.

Beslutning
CID-udvalget godkendte indstillingen.

6. Drøftelse af udkast til SoA-dokument

v/ UMH

Indstilling
Det indstilles,
at CID-udvalget drøfter udkast til SOA
at CID-udvalget godkender videre proces

Sagsfremstilling
SoA står for Statement of Applicability. Det er et krav efter ISO27001-standarden – og dermed obligatorisk for departementet - at udarbejde et SoA-dokument. Et SoA-dokument kan ses som en status og oversigt over organisationens arbejde med informationssikkerhed. Dokumentet indeholder en liste med sikkerhedsforanstaltninger fra ISO 27001, anneks A, som en organisation enten til- eller fravælger i arbejdet med informationssikkerhed.

I forbindelse med drøftelsen af SoA-dokumentet på mødet i Q4-2024 blev det bemærket, at dokumentet ikke indeholdt fem kolonner fra originalen på hjemmesiden "Sikker Digital", som SoA-dokumentet i ISM er udarbejdet på grundlag af. Disse er nu indarbejdet i dokumentet.

Det blev ligeledes på mødet bemærket*, "at en evt. farvelægning (rød-gul-grøn) vil kunne øge overskueligheden."*

SOA-dokumentet er nu udbygget med en farvelægning, som Sundhedsdatastyrelsen (SDS) tidligere har benyttet i koncernen. Farvekoden beskriver graden af implementering ud fra en skala på 5 trin.

- 5 - Implementeret og dokumenteret
- 4 - Implementeret uden dokumentation eller med delvis dokumentation

- 3 - delvist implementeret og dokumenteret
- 2 - delvist implementeret uden dokumentation eller med delvis dokumentation
- 1 - ikke implementeret

Siden sidste møde er SoA-dokumentet opdateret, således at alle foranstaltninger nu er blevet vurderet ift. implementeringsstatus og udeståender (GAP) men ikke fuldt kvalitetssikret med f.eks. IT. Dokumentet er justeret, så det afspejler de opnåede resultater i CID-arbejdet, som f.eks. at der er vedtaget en rejsevejledning.

Videre proces
ISDB vil på baggrund af CID-udvalgets drøftelse arbejde videre med SoA-dokumentet i samarbejde med HR, Intern Administration og IT. Status på SoA-dokumentet vil blive forelagt på kommende møder i CID-udvalget i 2025.

Bilag
Bilag 6.1 Udkast til SOA-dokument med foranstaltninger fra ISO-27002 v.1.1

Beslutning
CID-udvalget godkendte indstillingen.

7. Drøftelse af handleplan for CID-arbejdet i 2025
v/ UMH

Indstilling
Det indstilles, at CID-udvalget godkender udkast til handleplan for Cyber-, informationssikkerheds- og databeskyttelsesarbejdet i 2025 (bilag 8.1)

Sagsfremstilling:
Det blev på CID-udvalgsmødet Q4 besluttet, at en opdateret handleplan vil blive forelagt på hvert CID-udvalgsmøde.

Handleplanen/årshjulet for CID-arbejdet indeholder dels en oversigt over de opgaver, som er fastlagt på forhånd, herunder CID-udvalgsmøder, revision af retningslinjer m.v. som besluttet af CID-udvalget, svar på eksterne kendte bestillinger fra Digitaliseringsstyrelsen, dels de opgaver, som ISDB foreslår at prioritere med henblik på at efterleve ISO 27001 og ISO 27701.

I forhold til senest forelagte handleplan er afrapportering ift. følgende opgaver rykket til næste kvartal (nummeret i parentes henviser til foranstaltningsnummer i SoA-dokumentet):

Phishing (6.3)
Fortegnelser (5.9) e
HR-notat om datakonstruktion færdiggørelse (5.34)
Opfølgning på tekniske minimumskrav (5.36)
Proces for opdatering af specialsoftware PC og anden SW (8.19)
DEP Tilsyn med DEP af Deloitte (5.35).

Bilag
Bilag 7.1 Udkast til revideret handleplan og årshjul for CID-arbejdet i 2025 v1.1

Videre proces

Handleplanen vil blive gennemgået i ISDB forud for hvert CID-udvalgsmøde i 2025 og forelagt CID-udvalget.

Referat og beslutning
Cecilie gav ordet til UMH, der orienterede om, at følgende opgaver er flyttet fra Q1 til Q2 eller senere samt baggrunden herfor:

- Phishing (6.3) – afventet budget for igangsættelse
- HR-notat om datakonstruktion færdiggørelse (5.34) – DPA gav status på mødet.

For så vidt angår Deloittes tilsyn med departementet henvises der til punkt 8.c. For så vidt angår fortegnelser henvises der til punkt 8.e.

CID-udvalget tog orienteringen til efterretning.

8. Orienteringspunkter

8.a Orientering om Implementering af retningslinjer for brug af departementets IT-udstyr på farten og på rejser.

v/ ABKN

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

Sagsfremstilling:
Direktionen godkendte på mødet den 21. februar 2025”Retningslinjer for brug af departementets it-udstyr på farten og på rejser"(bilag 8.a1), som CID-udvalget godkendte på mødet den 13. december 2025.

Direktionen anmodede om at få undersøgt, om det er muligt at få et billigere mobilabonnement til rejse-pc og rejsetelefon end vores nuværende mobilleverandør kan tilbyde, og om det i særlige tilfælde kan lade sig gøre at medbringe eget it-udstyr til højrisikolande, hvilket medarbejdere fra UM har mulighed for.

Retningslinjerne er efterfølgende behandlet på chefmødet den 26. februar 2025, som bl.a. bemærkede, at det er problematisk, at man ikke kan kommunikere med SMS på rejsetelefoner.

ISDB er ved at afklare ovenstående tre punkter og vil orientere om status på mødet.

Retningslinjerne vil herudover blive behandlet på Samarbejdsudvalgsmødet den 18. marts 2025.

Bilag
Bilag 8.a1 ”Retningslinjer for brug af departementets IT-udstyr på rejser"

Videre proces
Retningslinjerne vil blive offentliggjort på intranettet. ISDB vil desuden orientere om retningslinjerne på on-boarding kurser og på afdelings- og kontormøder med fokus på de kontorer, der har stor rejseaktivitet.

”Retningslinjer for informationssikkerhed for medarbejdere i ISM” vil konsekvensrettet iht. de vedtagne rejseretningslinjer ved næste revision medio 2025.

Beslutning
CID-udvalget tog orientering til efterretning.

8.b Retningslinjer for privat brug af arbejdstelefoner og iPads ("blandede telefoner")
v/ ABKN

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

Sagsfremstilling
På CID-udvalgsmødet den 13. december, punkt 7, blev det besluttet, at ISDB i samarbejde med HR skulle udarbejde et oplæg til direktionen, som indebar, at medarbejdere ikke tilbydes at kunne bruge deres arbejdstelefon privat, og at alle medarbejdere informeres om problemstillingerne ved blandet brug af telefoner med henblik på, at medarbejderne kan tage stilling til, om de fortsat ønsker at have blandede telefoner.

Baggrunden for denne beslutning var, at medarbejdere med blandede telefoner kan blive stillet i en uhensigtsmæssig situation, fordi det af sikkerhedsmæssige årsager som udgangspunkt ikke er tilladt at medbringe en blandet arbejds- og privattelefon på rejser udenfor EU/EØS/ NATO.

I forlængelse heraf har direktionen på mødet den 21. februar 2025 besluttet, at nye medarbejdere fremadrettet ikke tilbydes at kunne bruge deres arbejdstelefon privat, og at alle medarbejdere informeres om problemstillingerne ved privat brug af arbejdstelefoner, samt at medarbejdere, der i dag har blandede privat/arbejdstelefon, som udgangspunkt skal forsøge at få dem afviklet inden for 6 måneder.

Beslutningen behandles på SAM-møde den 18. marts 2025.

Videre proces
ISDB og HR vil i fællesskab informere medarbejdere, der allerede har en blandet telefon, om problemstillingen med henblik på, at de som udgangspunkt inden for en periode på 6 måneder får afviklet deres blandede telefoner.
"Retningslinjer for informationssikkerhed for medarbejdere i ISM" vil blive tilrettet iht. ovenstående ved næste revision medio 2025.

Beslutning
CID-udvalget tog orientering til efterretning.
ABKN supplerede med at bemærke, at det i de nuværende retningslinjer for Informationssikkerhed er tilladt at installere MIA (SIT's mobile arbejdsplads på telefoner) på private mobiltelefoner. Der var enighed om, at dette bør ændres i de generelle retningslinjer. ISDB udarbejder forslag til ændringer hertil i forbindelse med, at de generelle retningslinjer skal revideres på næste møde i CID-udvalget.

8.c Orientering om tilsyn med departementet ifm. 2024-tilsynet med Informationssikkerhed og databeskyttelse på ministerområdet
v/ UMH

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

Sagsfremstilling

Departementet har den 19. februar 2025 modtaget tilsynsbrev fra revisionsfirmaet "Deloitte", som fører tilsyn med departementet iht. ministeriets tilsynskoncept, hvoraf det fremgår at:

"Tilsynet med informationssikkerhed og databeskyttelse i departementet gennemføres af en uafhængig auditør. Tilsynet omfatter såvel departementets interne informationssikkerhed og databeskyttelse, som departementets vejledning, tilsyn og kontrol med institutioner på ministerområdet. Tilsynet med de koncernfælles funktioner på HR og økonomiområdet gennemføres som en del af tilsynet med departementet."

Revisionsfirmaet udfører tilsynet på grundlag af de samme tilsynsdokumenter og tilsynsmål, som departementet selv benytter i tilsynet med de underliggende institutioner på ministerområdet.

Tilsynet består af en tredelt spørgeramme:
Del 1: Generelle spørgsmål
Del 2: ISO-modenhedsspørgsmål på baggrund af ISO 27001 og ISO 27701.
Del 3: Opfølgning på tidligere tilsyn.

Tidsplan for tilsynet:

1. Departementets skriftlige besvarelse forventes fremsendt til Deloitte senest den 2. april 2025.
2. Tilsynsmødet afholdes den 30. april 2025 hos departementet.
3. Høringsdato er fastsat til den 9. maj 2025 med høringsfrist den 23. maj 2025.
4. Den endelige rapport for tilsynet forventes fremsendt af Deloitte i uge 23.
5. Resultatet af tilsynet vil blive forelagt på CID-udvalget på mødet i Q2 eller Q3 alt efter, hvornår rapporten modtages.

8.d Orientering om sikkerhedshændelser herunder brud på persondatasikkerheden
v/ HBN

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

Sagsfremstilling
I perioden fra 1. december 2024 til 21. februar 2025 har der været syv sikkerhedssikkerhedshændelser.

Beskrivelse af sikkerhedshændelse	Brud på persondatasikkerhed	Anmeldt til Datatilsynet
Vagten i SHG 12 havde observeret, at der var medarbejdere med adgangskort med blåt bånd som lukkede hinanden ind, da den ene formegentlig havde glemt sig eget kort.	-	Nej
Sikkerhedshændelse - bortkommet notesblok	-	Nej
Borgerhenvendelser anvendt i praktikopgave	Ja	Nej
Cyberangreb på Jan Nygaard A/S og læk af oplysninger om købere af biler, herunder køb af ministerbil.	-	Nej

HR-oplysninger sendt fra anden myndighed til styrelse i koncernen	-	**Nej**
Bruger i DEP fik ikke besked på, at sikker mail afsendt fra F2 var fejlformateret og ikke blev fremsendt eller leveret til modtager.	**Måske**	**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	-	**Afventer afklaring hos SIT**

ISDB har evalueret sikkerhedshændelserne, hvilke har givet anledning til følgende overvejelser:

- Vedr. borgerhenvendelser anvendt i praktikopgave: ISDB har tidligere været i dialog med HR om nødvendigheden af en vejledning til de studerende, der er i praktikophold i ISM, og som skriver praktikopgaver på baggrund af dette. ISDB vil inddrage forvaltningsjura i arbejdet, da der også udestår afklaring af tavshedspligt ift. materiale, der benyttes i opgaverne. Det skal f.eks. tydeliggøres, hvordan den forvaltningsretlige tavshedspligt er, da den er anderledes ift. "anonymisering" end GDPR.

- Den manglende besked om fejl ifm. afsendelse af sikker mail fra F2 skyldes for det første brugen af to forskellige systemer i DEP til sikker post. DPG-plugin benyttes i Outlook (f.eks. hovedpostkassen) til at modtage og sende sikker post. F2 kan sende sikker post, ikke modtage. For det andet skyldes det en praksis i Intern Administration med at oprette alle afsendere som sagsparter i F2 med sikker-mail-adresser hentet fra DPG-plugin. Disse sagsparter kan F2 ikke benytte. ISDB vil i samarbejde med Intern administration og IT drøfte en løsning. Det kunne f.eks. være, at sikker mail fra borger.dk modtages i F2 og ikke i hovedpostkassen (Outlook med DPG-plugin). Den foreløbige vurdering er, at det ikke udgør et brud på persondatasikkerheden.

- Ift. varsel fra CFCS vedr. brug af kompromitteret browser-plugin, har hændelsen givet anledning til flg. overvejelser: I henhold til "Informationssikkerhed for medarbejdere" afsnit 5 er det tilladt for medarbejdere at installere browser plugins. i næste revision af dokument kan dette afsnit revideres, så det f.eks. fremgår, at der skal spørges om konkret tilladelse til at installere et konkret plugin eller opstilles en liste over godkendte plug-ins. Installation af plugins kan også forbydes. Sagen vil blive drøftet med IT.

Bilag
Bilag 8d.1 Sikkerhedshændelsesregister ISM

Referat og beslutning
HBN gennemgik sikkerhedshændelserne, der fremgik af det vedlagte register, og supplerede med, at flere er begyndt at række ud for at få afklaret, om der er brud på persondatasikkerheden. Ofte er der dog ikke tale om brud, men det er generelt positivt, at folk rækker ud, og at der er fokus på behandling af personoplysninger. Udvalget tog orienteringen til efterretning.

8.e Status på arbejdet med opdatering af fortegnelser
v/ HBN

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

Sagsfremstilling
ISDB er i proces med at udarbejde et samlet overblik over behandlingen af personoplysninger og udarbejde den endelige fortegnelse.

Med henblik på at skabe overblik og samle behandlingerne i færre fortegnelser er flg. besluttet:

- Indenrigsafdelingen får egne fortegnelser
- HR er ansvarlig for en stor del af behandlingerne, her vil antallet af fortegnelser blive forsøgt reduceret.
- Tværgående behandlinger mellem flere kontorer vil blive forankret i ét kontor med én fortegnelse.

Der udestår beslutninger vedr. fortegnelser ift. netværksarrangementer. Det er endnu ikke afgjort om, hvis overhovedet, der skal være en risikoejer på disse tvær-aktiviteter.

8.f Orientering om møde i CID-koordinationsforum
v/ CLSO

Der gives en mundtlig orientering på mødet.

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

Referat
CLSO orienterede om, at der på CID-koordinationsforum, som blev afholdt den 7. marts 2025, særligt var tre emner, der blev drøftet: NIS 2, som vi kommer tilbage til under næste punkt, og derudover USA og tredjelandsoverførsler samt endelige koncernfælles kurser.

Vedr. USA og tredjelandsoverførsler efter ny administration
Der var en åben drøftelse af området, hvor der bl.a. sker ændringer i databeskyttelsesregler og AI-regulering. Forummet konstaterede i det store hele, at der ikke pt. er mulighed for at gøre noget for ISM som enkeltaktør. LMST bemærkede, at nogle i EU allerede vender sig forskellige steder hen.

Vedr. koncernfælles kurser
Klaus fra Koncernprogrammer gik i dialog med forummet om emner af tværgående interesse. Der var særlig interesse for at løfte opgaven med at klæde ledelserne på (indkredse ledelsesansvaret og opgaven) ift. at implementere NIS 2.

Behovet for engelsksprogede CAMPUS-kurser blev også drøftet.

8.g Orientering om NIS 2

v/ MRAN

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

Der gives en mundtlig orientering på mødet af status på NIS 2.

Referat
Der blev orienteret om, at NIS 2-lovforslaget er fremsat i Folketinget og har været 1. behandlet den 26. februar 2025. Lovforslaget træder i kraft 1. juli 2025. Fristen for registrering af enheder er den 1. oktober 2025.

MSSB vil udstede en bekendtgørelse, der udpeger tilsynsmyndighederne, og hjemle at tilsynsmyndighederne kan modtage og kommunikere via digital kommunikation, jf. NIS 2-lovens §§ 20 og 31.

Sundhedsdatastyrelsen forventes at blive udpeget til at føre tilsyn med sundhedssektoren og delsektoren for fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik.

MSSB arbejder på at have vejledninger klar til de omfattede enheder. ISM og SDS kommenterer på dette arbejde.

Der har været en regeringssag om midler til tilsyn og dut-kompensation, hvor alle ministeriernes egen efterlevelse ønskes behandlet igen, da der skal tages eksplicit stilling til, om ministeriernes egen efterlevelse skal afholdes indenfor rammerne.

9. Eventuelt

Referat
TRBR understregede behovet for, at departementet indtager en mere proaktiv tilgang til brugen af generativ AI i sagsforberedende arbejde og almindelige skriveopgaver som eksempelvis udarbejdelse af referater. Det blev bemærket, at brugen af generativ AI allerede er udbredt blandt de yngre medarbejdere, og at det – udover potentialet for effektivisering – også er afgørende for departementet at følge med udviklingen for at forblive en attraktiv arbejdsplads.

Behovet for at øge kendskabet til anvendelsen af generativ AI, herunder værktøjer som ChatGPT, blandt både medarbejdere og ledere blev drøftet. Dette omfattede både en indsats for at formidle departementets eksisterende retningslinjer samt nødvendigheden af øget implementering i forbindelse med en bredere implementering af generativ AI i departementet. FKD fremhævede, at der umiddelbart kan være betydelige effektiviseringsgevinster at hente ved en bredere anvendelse af generativ AI i en institution som departementet, da skriftlig formidling udgør en kernekompetence på tværs af alle afdelinger. Den primære risiko – ud over kravet om, at AI-løsningerne skal være sikre og lovlige – vedrører rigtigheden af de skriftlige produkter, så kvalitetsniveauet kan opretholdes ved brug af generativ AI.

FKD orienterede om, at FKD og LRJ deltager i SIT's projekt vedrørende generativ AI, og at SIT nu kan tilbyde løsninger hostet hos SIT i Danmark. Disse løsninger vurderes ikke umiddelbart at have de samme databeskyttelsesmæssige udfordringer som cloudbaserede alternativer.

Det blev besluttet, at der skal gennemføres en afdækning af mulighederne for at integrere generativ AI på tværs af departementet. Afdækningsarbejdet skal varetages af ISDB og IT.

10. Næste møde

Afholdes torsdag den 20. juni 2025 kl. 10.00-11.30.