INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
F +45 7226 9001
M
W

Dato: 13-01-2025
Enhed: ISDB-enheden
Sagsbeh.: UMH
Sagsnr.: 2024-9812
Akt-id.: 281776

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

Referat fra møde i CID-udvalg 4-2024

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

Dato for møde
13. december 2024

Deltagere
Medlemmer
Cecilie Louise Svane Olesen (CLSO), Økonomi og koncernstyring, forperson (Deltog i mødet fra punkt 6)
Annette Baun Knudsen (ABKN), ISDB-enheden
Trine Brøbecher (TRBR), HR
Lene Jensen (LRJ), IT

Observatør
Helle Ginnerup-Nielsen (HGN), DPO DEP

Ressourcepersoner
Katja Roitmann (KROI), BESS
Mette Rye Andersen (MRAN), ISDB-enheden
Frederik Kastoft-Davidsen (FKD), ISDB-enheden

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

Afbud
Pernille Seaton (PSE), Intern Administration

Dagsorden

1. Velkomst
2. Referat fra CID-udvalgsmøde den 10-09-2024
3. Årlig status for arbejdet med cyber-, og informationssikkerhed og databeskyttelse i departementet
4. Vedtagelse af handleplan og årshjul for CID-arbejdet i 2025
5. Forslag til ændringer af Politik for cyber-, og informationssikkerhed og databeskyttelse i departementet og CID-udvalgets kommissorium
6. Retningslinjer for brug af departementets it-udstyr på farten og på rejser
7. Retningslinjer for privat brug af arbejdstelefoner og Ipads ("blandede telefoner")
8. SoA-dokument
9. Mødeplan for 2025
10. Orienteringspunkter
    a. Møder i CID-koordinationsforum
    b. Brud på persondatasikkerheden.
    c. Obligatoriske kurser i Campus.
    d. Status på arbejdet med opdatering af fortegnelser
    e. Risikovurdering vedr. brugen af funktionen auto-complete i Outlook.
    f. Justitsministeriets retningslinjer vedr. SMS-beskeder
    g. Status på M365
11. Næste møde

Dagsorden

1. Velkomst

v/ABKN

ABKN bød velkommen, herunder til Katja Roitmann (KROI) BESS, som fremover vil deltage i CID-udvalgets arbejde som ressourceperson og repræsentant for BESS.

KROI oplyste på mødet, at BESS er ansvarlig for sikkerhedscirkulæret, samt at antallet af sikkerhedsgodkendte i DEP øges. BESS bliver fremover en del introprogrammet.

2. Referat fra CID-udvalgsmøde den 10-09-2024

v/ ABKN

Indstilling
Det indstilles, at CID-udvalget godkender referat fra CID-udvalgsmøde den 10-09-2024I

Sagsfremstilling:
Referat fra CID-udvalgets møde den 10-09-2024 (bilag 2.1) blev udsendt til godkendelse i skriftlig proces i F2 sammen med "Vejledning til medarbejdere om retningslinjer for brug af generativ kunstig intelligens i departementet". Referat og vejledning blev godkendt uden bemærkninger.

Bilag
2.1. Referat fra CID-udvalgsmøde 10-09-2024

Videre proces
Med udvalgets godkendelse vil referatet blive offentliggjort på intranettet (på samme måde som tidligere referater nu er offentliggjort på intra).

Beslutning
Udvalget godkendte referatet.

3. Årlig status for arbejdet med cyber-, og informationssikkerhed og databeskyttelse i departementet.

v/ABKN

Indstilling
Det indstilles, at CID-udvalget godkender den afgivne status (bilag 3.1) og den foreslåede videre proces.

Sagsfremstilling:
Det følger af CID-politikkens punkt 4, at CID-udvalget og departementschefen mindst én gang om året modtager en status på den samlede implementering af ISO27001 og ISO 27701, herunder de fire målsætninger i CID-politikken.

I forlængelse heraf vedlægges statusnotat (bilag 3.1), herunder status på awarenessaktiviteter (bilag 3.2).

Bilag
Bilag 3.1: Status for den samlede implementering af Iso 27001 og 27701 for 2024, jf. målsætninger - udkast
Bilag 3.2: Awareness overblik 2024

Videre proces
Med CID-udvalgets godkendelse vil statusnotatet blive forelagt departementschefen til orientering i januar 2025.

ABKN indledte med at bemærke, at det fremgår af CID- politikken, at ISDB-enheden skal udgive en årlig status for CID-arbejdet i departement. Dokumentet har ikke fundet sin endelige form, så der vil blive arbejdet videre med formatet. Statusnotatets fokus er at give en status for aktiviteterne i 2024.

HGN bemærkede, at det i coveret til DC bør fremhæves, hvor meget der udestår, så det fremstår tydeligt, hvor vigtigt det er, at CID-arbejdet har de nødvendige ressourcer.

Beslutning
Udvalget godkendte statusnotatet og den videre proces.

4. Vedtagelse af handleplan for CID-arbejdet i 2025
v/ABKN

Indstilling
Det indstilles, at CID-udvalget godkender udkast til handleplan for Cyber-, informationssikkerheds- og databeskyttelsesarbejdet i 2025 (bilag 4.1)

Sagsfremstilling:
Det fremgår af CID-politikkens punkt 4, at CID-udvalget udarbejder étårige handleplaner for at realisere målsætningerne og med henblik på at prioritere indsatserne.
I forlængelse heraf forelægges udkast til handleplan for CID-udvalgets arbejde i 2025.

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-enheden foreslår at prioritere med henblik på at efterleve ISO 27001 og ISO 27701.

Opgaverne er søgt grupperet, således at det fremgår om opgaverne vedr. efterlevelse af databeskyttelsesretlige krav eller informationssikkerhed, eller begge dele. Handleplanen er et levende dokument og vil løbende blive justeret både med hensyn til, hvilke opgaver der skal prioriteres og med hensyn til handleplanens form.

Bilag
Bilag 4.1 Udkast til handleplan/årshjul for CID-arbejdet i 2025

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

ABKN indledte med at bemærke, at dokumentet både er en handleplan og et årshjul, og at formålet er, at CID-udvalget kan følge, hvad ISDB-enheden forventer, der kommer til drøftelse på møderne i 2025. Der er tale om et levende dokument, som løbende forventes tilpasset.

TRBR bemærkede, at formatet giver godt overblik. Et mere detaljeret indblik bør være til ISDB-enhedens eget brug. TRBR anbefalede i øvrigt, at HR, af hensyn til intern planlægning, bliver inddraget tidligt ift. de opgaver, der planlægges i Q3 og Q4, der vedrører ressourcer fra deres side.

HGN anbefalede, at der bliver arbejdet med opdelingen af opgaver mellem "Infosec" og GDPR, da de fleste opgaver vedr. informationssikkerhed har et persondataretsligt aspekt.

ABKN oplyste, at en opdateret handleplan vil blive forelagt på hvert CID-udvalgsmøde.

Beslutning
Udvalget godkendte udkast til handleplan.

5. Årlig revision af Politik for cyber-, og informationssikkerhed og databeskyttelse i departementet og revision af CID-udvalgets kommissorium

v/ABKN

Indstilling
Det indstilles, at CID-udvalget godkender udkast til revideret CID-politik og udkast til revideret kommissorium for CID-udvalget.

Sagsfremstilling
CID-politikken og CID-kommissorium gælder allerede i dag for departementet og for Benchmarkingenheden, men det fremgår ikke tydeligt, at CID-politikken også gælder for Benchmarkingenheden. Det foreslås derfor i afsnittet om omfang og gyldighed at præcisere, at politikken også gælder for Benchmarkingenheden. Udkast til revideret CID-politik med TC er vedlagt som bilag 5.1.

I forlængelse af orientering under punkt 3 på CID-udvalgsmødet den 10. september 2024 bemærkes i øvrigt, at Benchmarkingenheden efterfølgende formelt har besluttet at overgå til den koncernfælles DPO-ordning, og at departementets DPA derfor nu er blevet tilknyttet Benchmarkingenheden

Som bilag 5.2 er desuden vedlagt et udkast til revideret kommissorium for CID-udvalget, der dels indeholder de opdateringer af CID-udvalgets sammensætning, der blev besluttet på CID-udvalgsmødet den 10. september 2024, dels et forslag til i punkt 3.2at fastsætte, at ISDB-enhedens leder har ansvaret for at udarbejde vejledninger til medarbejdere inden for rammerne af retningslinjer godkendt af CID-udvalget. Baggrunden for forslaget er at give mulighed for, at ISDB-enheden løbende kan tilpasse vejledninger efter behov på baggrund af tilbagemeldinger fra brugere. Nye vejledninger vil blive forelagt CID-udvalget til orientering. Det foreslås endvidere at præcisere i punkt 3.1, at CID-udvalget orienteres om høringssvar og indberetninger.

Bilag
Bilag 5.1 Udkast til revideret CID-politik for Indenrigs- og Sundhedsministeriets departement v1.1 med TC

Bilag 5.2 Udkast kommissorium for CID-udvalget i ISM's departement v1.3 med TC

Videre proces
Revideret CID-Politik og kommissorium for CID-udvalget vil efter godkendelse blive offentliggjort på intranettet.

ABKN indledte med at bemærke, at CID-politikken ifølge punkt 8 i politikken kun skal revideres ved væsentlige ændringer.

Den foreslåede ændring i CID-politikken skyldes et ønske om, at præcisere, at CID-politikken også gælder for Benchmarkingenheden.

HGN spurgte, hvilken betydning det har, at Benchmarkingenheden fremadrettet får administrativt ophæng til VIVE.

ABKN oplyste, at der vil blive taget stilling hertil, når det bliver aktuelt, og at dette sker senest den 1. januar 2026.

ABKN bemærkede endvidere, at baggrunden for forslaget om ændring af kommissorium for CID-udvalget er at give mulighed for, at ISDB-enheden løbende kan tilpasse vejledninger efter behov på baggrund af tilbagemeldinger fra brugere. Som eksempel kan nævnes awarenessplakater og folder, som ISDB-enheden har udarbejdet inden for rammerne af de vedtagne retningslinjer for informationssikkerhed.

Beslutning
Udvalget godkendte udkast til revideret CID-politik og udkast til revideret kommissorium for CID-udvalget.

6. Retningslinjer for brug af departementets it-udstyr på farten og på rejser

v/ MRAN

Indstilling
Det indstilles, at CID-udvalget godkender:
Udkast til retningslinjer for brug af departementets it-udstyr på rejser (bilag 6.1)

- Udkast til ansvarsfordeling ifm. brug af it-udstyr på farten og på rejser (bilag 6.5, som medbringes på mødet)
- Forslag til videre proces, herunder
    - forslag til intern formidling i departementet ifm. implementering af retningslinjerne
    - forslag til, at ISDB-enheden udarbejder supplerende vejledning til medarbejdere
    - forslag om at afdække udgifterne forbundet med brug af mobiltelefonen som hotspot i udlandet nærmere
    - forslag om, at retningslinjerne og ressourcetrækket ifm. rejser til udlandet evalueres med udgangen af Q2 2025.

Sagsfremstilling
Brug af departementets it-udstyr på tjeneste- såvel som private rejser kan, afhængig af geografi og formål, udgøre en risiko for informationssikkerheden. Udkast til retningslinjer for brug af it-udstyr på rejser (bilag 6.1) har til formål at sikre, at departementets

medarbejdere kender og tager de nødvendige forbehold vedr. brug af departementets it-udstyr på rejser, så risici mod informationssikkerheden minimeres.

ISDB-enheden har, bl.a. med input fra CFCS, PET og Intern IT, udarbejdet vedlagte risikovurdering af brug af departementets it-udstyr på farten (bilag 6.2), som ligger til grund for udkastet til retningslinjer. I udkastet skelnes mellem fire situationer, hvor it-udstyr benyttes uden for departementet: 1) fra hjemmearbejdspladsen, 2) på farten i Danmark, 3) på tjenesterejser i udlandet samt 4) på ferierejser i udlandet.

Der er tale om en opdatering af tidligere SUM-koncernfælles retningslinjer "Vejledning om sikker brug af it-udstyr på farten", version 1.0 (bilag 6.3), som blev vedtaget i 2020, hvor SDS varetog driften af koncernens it, dvs. før transitionen til Statens It (SIT). I den mellemliggende periode er transitionen til SIT gennemført, det er blevet væsentlig mere udbredt at arbejde på distancen, der er sket en markant teknologisk udvikling og den geopolitiske situation er blevet skærpet.

I vedlagte Notat om brug af it-udstyr på rejser og på farten (bilag 6.4) redegøres nærmere for de forhold og hensyn, som ISDB-enheden har afvejet i forbindelse med opdateringen af retningslinjerne.

I bilag 5, som medbringes på mødet, præsenteres forslag til fordeling af roller og ansvar ifm. forberedelse af rejser til lande uden for EU/EØS og NATO. Medarbejder der skal ud at rejse, dennes nærmeste leder, IT-afdelingen og ISDB-enheden skal bidrage i forskellige dele af processen med at risikovurdere den konkrete rejse, klæde medarbejder på samt bestille og teste relevant it-udstyr.

Retningslinjerne vurderes at svare til generel best practice i staten, sådan som reglerne er beskrevet i vejledninger fra CFCS, PET og SIT.

Den videre proces

Implementering

Det foreslås, at enhedschefen for ISDB-enheden orienterer om retningslinjerne på et kommende chefmøde, hvorefter retningslinjerne annonceres og lægges på Intra.

Vejledning

Det foreslås, at ISDB-enheden udarbejder en vejledning til retningslinjerne med henblik på at gøre det så tydeligt som muligt for medarbejderne, hvad de enkelte punkter indebærer og hvordan de følges i praksis. Vejledningen udarbejdes med involvering af Intern IT og vil være klar, når retningslinjerne præsenteres. Vejledningen skal godkendes af enhedschefen for ISDB-enheden og forelægges CID-udvalget til orientering. ISDB-enheden vil løbende holde vejledningen opdateret.

Mobilabonnementer

Det forslås, at udgifterne forbundet med brug af mobiltelefonen som hotspot i udlandet undersøges nærmere i første halvdel af 2025 med henblik på at sikre, at departementet har den bedst mulige abonnementsaftale til formålet.

Evaluering

Det er samtidig relevant at følge implementeringen af de nye retningslinjer, herunder ift. ressourcetræk og brugervenlighed. Det foreslås derfor at gennemføre en evaluering af retningslinjerne efter sommerferien 2025, hvor første lukkeperiode med de nye retningslinjer er afholdt.

Konsekvenstilretning i øvrige retningslinjer
Med CID-udvalgets godkendelse, vil ISDB-enheden desuden konsekvensrette relevante afsnit i de gældende Retningslinjer om informationssikkerhed med henvisning til de nye Retningslinjer for brug af it-udstyr på rejser og på farten.

- Bilag 6.1: Udkast til Retningslinjer for brug af it-udstyr på farten og på rejser
- Bilag 6.2: Risikovurdering vedr. brug af it-udstyr på farten og rejser
- Bilag 6.3: SDS Vejledning: It-udstyr på farten – okt. 2020
- Bilag 6.4: Notat om brug af it-udstyr på rejser og på farten
- Bilag 6.5: Udkast til ansvarsfordeling ifm. brug af it-udstyr på farten og på rejser (medbringes på mødet)

CLSO indledte punktet med at bemærke, at de seneste retningslinjer var de koncernfælles retningslinjer for brug af it-udstyr på rejser og på farten fra SDS, hvilket understreger behovet for at departementet godkender egne, opdaterede retningslinjer på området. I forlængelse af drøftelserne på sidste møde i udvalget er det bl.a. centralt, at der fremover skelnes mellem private ferierejser og tjenesterejser.

CLSO bemærkede videre, at ISDB-enheden er i færd med at foretage en risikovurdering vedr. brug af departementets it-udstyr uden for SIT's netværk, og at dette arbejde er i gang, men adskiller sig fra øvrige risikovurderinger i og med de tekniske løsninger er givet fra Statens It's side.

MRAN præsenterede de fire situationer for brug af it-udstyr, som udkastet til retningslinjer tager udgangspunkt i og præsenterede forslaget om at evaluere retningslinjerne efter sommerferien 2025 med henblik på at vurdere ressourcetrækket og rejseaktiviteten. MRAN bemærkede, at ISDB-enheden vil udarbejde en vejledning til retningslinjerne, hvor det bl.a. vil blive tydeliggjort, hvad hhv. "fremmede" og "sikre" netværk er, hvordan sikkerhedsposer anvendes mv.

Udvalget drøftede udkastet og havde følgende bemærkninger:

1) Under punkt 1 afsnit 2.2 var der enighed om hhv. at tilføje og slette:
"Undlad f.eks. <u>så vidt muligt</u> at arbejde med fortrolige og følsomme oplysninger på offentlige steder, såsom i en lufthavn eller på toget.

"Undlad at have mobile lagringsenheder som USB-stik fremme~~, og slå internetforbindelsen fra, når du ikke bruger den~~."

2) Under punkt 4 afsnit 2.2 blev følgende ændring besluttet:
"Du må <u>altid</u> ~~dog gerne~~ bruge SIT-<u>prod</u>~~s netværk~~, hvis [..]"

3) Under punkt 6 afsnit 2.2:
Det blev besluttet, at ISDB-enheden genovervejer nødvendigheden af punktet, idet det vil være vanskeligt at implementere, særligt for de medarbejdere som har blandede telefoner.

4) Punkt 12 under afsnit 2.2 vedr. hændelser:
Det blev besluttet at give uheld og hændelser et selvstændigt afsnit med henblik på at fremhæve punktet. Videre skal kontaktoplysningerne til SIT fremgå tydeligt, da de kan lukke abonnementer, hvis udstyr bortkommer.

5) Under punkt 1 afsnit 2.3.2 blev følgende ændringer godkendt:
Hvis du har brug for at medbringe PC, skal du bestille en "Rejsecomputer" samt "Rejsetelefon" på Statens-IT serviceportal. Kontakt ISDB-enheden før du bestiller udstyret. Bestillingen skal godkendes af nærmeste leder ~~og konteres på kontorbudgettet~~."

Rejsecomputeren kan tilgå nettet via det indbygget SIM-kort, alternativt ved at benytte ~~mobiltelefonen~~ rejsetelefonen som hotspot, ~~og~~ så du kan tilgå din virtuelle arbejdsplads (VIA), dvs. de applikationer (f.eks. mail, kalender og F2), som normalt er tilgængelige på VIA.

6) Under afsnit 2.4 blev følgende ændringer besluttet:
Der er som udgangspunkt ikke behov for ~~tilladt~~ at medbringe departementets it-udstyr på private ferierejser ~~udenfor Danmark~~.

7) Det skal fremgå af vejledningen, at den skal medbringes på farten, så medarbejder har den ved hånden.

8) HGN opfordrede til at retningslinjerne gennemskrives med henblik på at gøre dem så nemme at formidle som muligt, hvilket udvalget bakkede op om.

Beslutning
Med de faldne bemærkninger blev indstillingen godkendt, herunder at ISDB-enheden tilretter ordlyden i retningslinjerne og udarbejder en supplerende vejledning, som rundsendes i kredsen med henblik på eventuelle bemærkninger, hvorefter materialet forelægges 1) AC-kredsen, 2) chefgruppen og 3) samarbejdsudvalget og efterfølgende implementeres.

7. Retningslinjer for privat brug af arbejdstelefoner og Ipads ("blandede telefoner")

v/ABKN

Indstilling
Det indstilles,
at CID-udvalget drøfter de nuværende retningslinjer for Informationssikkerhed for medarbejdere ift. privat brug af mobile enheder udleveret af departementet, herunder installation af MIA på private telefoner.

Sagsfremstilling
CID-udvalget traf den 10. september 2024 følgende beslutning: *"ISDB-enheden vil på næste møde .. 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."*

TRBR har efterfølgende oplyst at der p.t. er 24 medarbejdere i departementet, der bliver beskattet af privat brug af tjenestetelefon.

De gældende retningslinjer for Informationssikkerhed for medarbejdere i Indenrigs-og Sundhedsministeriets departement indeholder i punkt 14 regler for anvendelse af mobile enheder, herunder regler om sletning af SMS-beskeder m.v.:

*”**14.1. Anvendelse af mobile enheder udleveret af departementet***
Departementet udleverer mobile enheder (mobiltelefoner og i visse tilfælde iPads) til medarbejderne, som på forhånd er registreret hos Statens It og installeret med Statens It´s mobile it-arbejdsplads (MIA), som giver sikker adgang til bl.a. mails og F2. Departementet kan uden varsel låse og slette alle data på enheden, hvis den f.eks. tabes, stjæles eller bortkommer, eller sikkerhedskopiere telefonens indhold, hvis den f.eks. skal indgå i en kommissionsundersøgelse. Medarbejderen skal sørge for, at enheden altid er sikkerhedsopdateret til seneste version. Den mobile enhed skal være beskyttet af adgangskode eller fingeraftryk. Opstår der mistanke om, at uvedkommende har fået kendskab til koden, skal denne straks skiftes på alle relevante enheder.

Medarbejdere i departement må som udgangspunkt kun sende arbejdsrelaterede SMS-beskeder mv. på udstyr, der er udleveret af departementet. Nogle beskedtjenester har redigerings- og slettefunktioner, der betyder, at afsenderen kan redigere og slette i beskeder, som slår igennem på modtagerens telefon, og den oprindelige besked derved slettes eller ændres på både afsenderens og modtagerens telefon. Der må ikke anvendes sådanne redigerings- og slettefunktioner. SMS-beskeder og beskeder på andre beskedtjenester må ikke slettes på mobile enheder udleveret af departementet, medmindre • beskederne er private • beskederne er modtaget ved en åbenlys fejl • der er tale om beskeder, der udelukkende har et personalerelateret indhold, eksempelvis en SMSbesked om, at man holder fri, beskeder til og fra en tillidsrepræsentant (i kraft af dennes funktion) eller beskeder mellem medarbejder og chef om rent personlige forhold, f.eks. en sygemelding. • beskeden er journaliseret (men kun fra det tidspunkt, hvor beskeden er journaliseret). Arbejdsrelaterede SMS-beskeder og beskeder på andre beskedtjenester opbevares i øvrigt af departementet i overensstemmelse med Justitsministeriets retningslinjer herom.

14.2. Private enheders adgang til data
En privat enhed kan anvendes til at tilgå bl.a. mails og F2. Dette forudsætter installation af MIA, og medarbejderen accepterer herved, at departementet uden varsel kan låse og slette alle data på enheden, hvis den f.eks. tabes, stjæles eller bortkommer, eller sikkerhedskopiere telefonens indhold, hvis den f.eks. skal indgå i en kommissionsundersøgelse. Enheden skal i øvrigt behandles på linje med en af departementet udleveret enhed. De data, der synkroniseres til private enheder, er forretningsdata. Derfor må mobile enheder, hvortil der er etableret synkronisering til arbejdsmail mv., ikke anvendes af eller udlånes til andre, jf. afsnit 13.2. Informationssikkerhed. Medarbejderen bærer selv eventuelle omkostninger til datatransmission på private enheder, herunder ved rejser til udlandet. Der ydes fra ministeriets side ikke support til private enheder - herunder opsætning af synkronisering mv.

14.3. Tjenesterejser og private rejser med udstyr der synkroniserer med F2 og mail
Ved tjenesterejser uden for EU eller private rejser uden for EU skal departementets Intern IT kontaktes med henblik på vejledning om IT-sikkerhedsmæssige forhold, hvis der medbringes og anvendes enheder, udleveret af arbejdspladsen, eller som tilgår eller synkroniserer med F2, mail mv.” Se eventuelt link til retningslinjer her:
Informationssikkerhed

De nuværende retningslinjer for Informationssikkerhed tillader således i et vist omfang privat brug af tjenestetelefoner, ligesom retningslinjerne heller ikke udelukker, at private enheder kan anvendes til at få adgang til data.

Vedtagelse af de foreslåede retningslinjer for brug af it-udstyr på rejser, jf. punkt 6, vil indebære, at der opstår en problemstilling ift. tjenestetelefoner, der samtidig bruges privat (blandede telefoner), når sådanne telefoner medbringes af medarbejdere på rejser udenfor EU/EØS/NATO. Ud fra hensyn til informationssikkerhed vil MIA før afrejsen skulle afinstalleres på blandede telefoner, men MIA vil ikke kunne reinstalleres ved hjemkomsten, da udstyret potentielt kan være kompromitteret.

CLSO indledte med at bemærke at problemstillingen er – som også blev drøftet på seneste CID-udvalgsmøde – at medarbejdere, der benytter deres telefon både til private og til tjenesteformål, (blandede telefoner), med vedtagelse af reviderede retningslinjer for brug af departementets it-udstyr på rejse vil blive stillet i en uhensigtsmæssig situation ved private rejser udenfor EU/EØS/NATO, idet MIA før udrejsen skal afinstalleres, og telefonen skal resettes/reinstalleres og i nogle tilfælde destrueres ved hjemkomsten, da telefonen potentielt kan være kompromitteret. Medarbejdere kan dermed

TRBR bemærkede, at der udover de 24 registrerede ansatte, som bruger deres tjenestetelefon privat, må antages at være et skyggetal og foreslog, at kendskabet til problemstillingen ifm. rejser udenfor EU/EØS/NATO udbredes blandt medarbejderne. TRBR bemærkede i lyset af ovennævnte, at tilbud om blandede telefoner til nye medarbejdere bør genovervejes.

Beslutning
Udvalget besluttede, at ISDB-enheden i samarbejde med HR udarbejder et oplæg til beslutning i direktionen, som indebærer, at nye 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.

8. Drøftelse af udkast til SoA-at 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.
Hvis en foranstaltning er fravalgt, skal dette begrundes.

I SoA-dokumentet skal organisationen som minimum forholde sig til sikkerhedsforanstaltningerne, der er listet i ISO 27001 anneks A. Dette er en slags tjekliste, der sikrer, at organisationen kommer hele vejen rundt i sine valg af foranstaltninger. Der kan være andre foranstaltninger, som er relevante for organisationen, og som vil skulle tilføjes.

Færdiggørelse af SoA- dokumentet vil kræve inddragelse af HR, IT og Intern Administration. SoA-dokumentets afsnit 6 vedrører således personrelaterede foranstaltninger, som f.eks. fortrolighedsklausuler, der skal drøftes og afklares med HR, SoA-dokumentets afsnit 7 vedr. fysiske foranstaltninger, som skal drøftes og afklares med Intern Administration. SoA-dokumentets afsnit 8 om tekniske foranstaltninger, som f.eks. backup eller tildeling af administrative rettigheder, skal drøftes og afklares med IT.

Udkast til SoA-dokumentet mangler således bl.a. stillingtagen til flere af de tekniske foranstaltninger i kapitel 8, herunder fravalg af foranstaltninger, der ikke er relevante i en organisation, der har begrænset egen udvikling af IT-programmer/systemer.

Videre proces
ISDB-enheden 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 8.1 Udkast til SOA-dokument med foranstaltninger fra ISO-27002

UMH oplyste, at udkastet til Soa-dokument er udarbejdet på grundlag af den skabelon, der er offentliggjort på Sikker Digital, og at vi fremadrettet vil medtage de fem kolonner, der i den nuværende version er udeladt ift. originalen fra "Sikker Digital".
HGN bemærkede, at en evt. farvelægning (rød-gul-grøn) vil kunne øge overskueligheden
UMH svarede, at dette forslag vil blive taget med i det videre arbejde med Soa-dokumentet, og at dokumentet vil blive fremlagt på de kommende CID-udvalgsmøder næste år.

Beslutning
Indstillingen, herunder den foreslåede videre proces, blev godkendt.

9. Mødeplan for 2025

v/CLSO

Indstilling
Det indstilles, at flg. 4 datoer godkendes.

Torsdag den 20. marts 2025 kl. 10.00-11.30
Torsdag den 19. juni 2025 kl. 10.00-11.30
Tirsdag den 16. september kl. 14.00-15-30
Torsdag den 11. december kl. 10.00-11.30

Mødeindkaldelserne er udsendt.

Næste møde
Torsdag den 20. marts 2025 kl. 10.00-11.30

Beslutning
Udvalget godkendte mødeplanen uden bemærkninger.

10. Orientering

10.a Orientering om møde i CID-koordinationsforum 8-10-2024 og 5-12-2024
v/CLSO

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

Punk 10.a udgik

10.b Brud på persondatasikkerheden
v/HBN

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

Sagsfremstilling
I perioden fra 1. september 2024 til 1. december 2024 har der været tre sikkerhedsbegivenheder, og ingen brud på persondatasikkerheden.

Beskrivelse af sikkerhedshændelse	Brud på persondatasikkerhed	Anmeldt til Datatilsynet
1) PC medtaget på tjenesterejse til Indien (rød zone) - Ved hjemkomst kontaktes IT-support, da brugeren havde problemer med at komme på netværket. Udstyret blev straks inddraget af IT og PC blacklistet hos SIT. Der blev vurderet, at der ikke er brud på persondatasikkerheden, da det ikke medførte adgang til personoplysninger.	Nej	Nej
2) Undersøgelse af nedlægning af brugere i MitID. NGC har delt med CID-erfa-netværket, at SIT ikke af sig selv nedlægger brugere i MitID-erhverv. ISDB-enheden foretog på baggrund af henvendelsen en undersøgelse af, hvordan det håndteres i departementet og fandt, at departementets IT-afdeling har en procedure for at nedlægge MitID-erhvervsbrugere ifm. fratrædelse.	Nej	Nej
3) Spammail fra kommune Flere i JURA modtog en mail fra en afsender i en kommune. En medarbejder trykkede på linket. Computeren blev hurtigt scannet, og det viste sig, at der ikke var tegn på 'infektion'.	Nej	Nej

Alle sager er lukket.

ISDB-enheden har evalueret sikkerhedsbegivenhederne, hvilke har givet anledning til følgende overvejelser:

- PC-medtaget på tjenesterejse understreger behovet for udarbejdelse af retningslinjer for brug af departementets it-udstyr på farten og på rejser og efterfølgende vejledninger og kommunikation om retningslinjerne.

- Adgangsstyring er en del af handleplanen for næste år, herunder en udarbejdelse af dokumenteret proces for regelmæssig gennemgang af brugere for at dokumentere, at fratrådte ansatte korrekt bliver slettet i alle systemer.
- ISDB-enheden planlægger en awarenesskampagne ift. phishing- og spammail i Q1, 2025, jf. handleplan.

ISDB-enheden har – bl.a. i lyset af bemærkningerne til afrapporteringen vedr. brud på persondatasikkerheden på CID-udvalgsmødet den 10. september 2024 – set nærmere på form og indhold for afrapportering af sikkerhedshændelser, samt på hvordan sikkerhedshændelser håndteres og registreres i ISDB-enheden. ISDB-enheden har på den baggrund påbegyndt udviklingen af en række produkter:

- Der er udarbejdet et nyt *register til registrering af hændelser* - Sikkerhedsbegivenheder / Sikkerhedshændelser / Brud på persondatasikkerheden (bilag 10b.1)
- Der er udarbejdet et nyt *informationsskema,* som skal udfyldes af de, som indmelder en sikkerhedshændelse - ISDB-enheden fremsender ved indmeldelse/henvendelse vedr. brud (bilag 10b.2)
- Der bliver arbejdet på en *intern procesbeskrivelse* til ISDB-enheden, således at alle hændelser bliver håndteret ensartet, jf. handleplan for 2025.

Bilag
Bilag 10b.1 Sikkerhedshændelsesregister ISM
Bilag 10b.2 Informationsskema - Sikkerhedshændelser

HBN fremlagde de enkelte hændelser. Der bliver arbejdet med at finde et fornuftigt snit for, hvor meget der registreres og dermed skal medtages på fremtidige CID-udvalgsmøder.

LRJ supplerede ifm. den hændelse, der vedrørte åbning af en vedhæftning (hændelse nr. 3), at scanningen af PC'en blev foretaget i samarbejde med SIT, og at åbningen af vedhæftningen ikke havde inficeret PC'en.

HBN oplyste endvidere, at der er udarbejdet et skema (vedlagt som bilag 10b2), der fremadrettet sendes til de, som indmelder en hændelse. Formålet er, at skemaet skal understøtte arbejdet med at belyse sagen, således, at der både kan foretages korrekt logning af databrud, og at der kan oparbejdes datagrundlag ift. awareness-kampagner.

Beslutning
Udvalget tog orienteringen til efterretning

10.c Opfølgning på obligatoriske kurser i Campus.
V/ABKN

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

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

kurser ” Cyber- og informationssikkerhed for medarbejdere i staten” og ”Databeskyttelse” forbliver obligatoriske for alle medarbejdere i departementet.

CID-udvalget besluttede samtidig, at ISDB-enheden en gang årligt (i efteråret) trækker en liste over, hvem der har/ ikke har gennemført kurserne det seneste år med henblik på at listerne kunne forelægges CID-udvalget listerne på mødet i november måned.

Da medarbejderne først er blevet tilmeldt kurserne ultimo oktober 2024 med 90 dages frist for gennemførelse, vil ISDB-enheden først i marts måned trække liste over gennemførte kurser og forelægge listerne for CID-udvalget på mødet den 20. marts 2025.

Beslutning
CID-udvalget tog orienteringen til efterretning.

10.d Status på arbejdet med opdatering af fortegnelser
V/HBN

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

Sagsfremstilling;

HBN vil give en kort status på arbejdet med at opdatere fortegnelser.

Bilag
Bilag 10d.1 Præsentation på chefmøde

Punkt 10.d udgik som mundtligt orienteringspunkt.

10.e Risikovurdering vedr. brugen af funktionen auto-complete i Outlook.
V/FKD

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

Sagsfremstilling
Ministeriet for samfundssikkerhed og beredskab har fremsendt brev af 1. oktober 2024 vedr. brug af auto-complete på alle ministerområder. I brevet understreges, at det er ”[..] *vigtigt, at alle statslige myndigheder – uagtet om man er kunde hos Statens It eller ej – foretager en risikovurdering af auto-complete-funktionen og herefter gennemfører eventuelle tekniske foranstaltninger for at mindske risikoen for fejlfremsendelse af oplysninger til uvedkommende*.”

For så vidt angår departementet er status, at auto-complete-funktionen er aktiveret i hele departementet, og der er ikke tidligere gennemført en risikovurdering af denne funktionalitet. Derfor er der ikke indført specifikke tekniske foranstaltninger for at reducere de potentielle risici forbundet med brugen af Outlook.

Departementet har imidlertid overordnede organisatoriske foranstaltninger, der administrativt begrænser anvendelsen af Outlook til overførsel af beskyttelsesværdige informationer. For eksempel anvender Borgerbrevsenheden, som er en af de enheder i

departementet, der systematisk behandler personoplysninger, primært F2 som værktøj til at sende eksterne mails.

Som opfølgning på bestillingen er ISDB-enheden i samarbejde med relevante fagkontorer i gang med at udarbejde en scenariebaseret risikovurdering. ISDB-enheden vil på CID-udvalgsmødet orientere om indholdet af risikovurderingen, herunder videre proces.

FKD oplyste supplerende på mødet, at risikovurderingen af auto-complete-funktionen i departementets almindelige e-mail-systemer, (front-end-applikationerne Boxer og Outlook), er under udarbejdelse. Risikovurderingen er en scenariebaseret kvalitativ vurdering, baseret på det udkast til risikostyringsproces, som blev præsenteret for CID-udvalget i Q2 2024. Vurderingen omfatter risici for både departementet og den registrerede.

ISDB-enheden har identificeret en række interne processer og tilknyttede risikoscenarier i organisationen, hvor der behandles følsomme og beskyttelsesværdige oplysninger. Disse processer er blevet knyttet til relevante fagkontorer der agerer som risikoejere for de respektive processer. Efterfølgende har ISDB-enheden faciliteret møder med fagkontorerne. Her har risikoejerne vurderet og scoret de enkelte scenarier ud fra sandsynlighed og konsekvens med udgangspunkt i departementets udkast for konsekvens- og sandsynlighedsskalaer.

ISDB-enhedens facilitering af processen vedr. scoring af risici, i samarbejde med fagkontorerne pågik operationelt smidigt og effektivt.

Den iboende risiko er dermed blevet kortlagt, og en række risikoscenarier, der ligger uden for departementets risikoappetit, er blevet identificeret.

Disse risikoscenarier omfatter følgende:

- Iboende risiko for den registrerede i forbindelse med HR- og chefgruppens kommunikation om personalesager.
- Iboende risiko for departementet relateret til Ledelsessekretariatets og Presse- og Kommunikations interne kommunikation om regeringssager og pressehåndtering.

Risikohåndteringen af den iboende risiko for både den registrerede og departementet vil blive behandlet som led i en skriftlig proces. Dette omfatter også accept af residualrisiko efter håndtering.

FKD bemærkede, at det var hensigtsmæssigt at udarbejde en separat risikovurdering for auto-complete-funktionen i F2, baseret på samme proces. ISDB-enheden forventer, at denne risikovurdering vil blive gennemført i første kvartal 2025.

Beslutning
Udvalget tog orienteringen til efterretning

10.f Justitsministeriets retningslinjer vedr. SMS-beskeder

V/ABKN

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

Sagsfremstilling
Justitsministeriet har ved brev af 10. oktober 2024 anmodet om status på implementering af Justitsministeriets opdaterede retningslinjer for opbevaring af SMS-beskeder inden for Indenrigs- og Sundhedsministeriets ressortområde.

ISDB-enheden har i forlængelse heraf gennemført en undersøgelse i departementet og blandt ministeriets institutioner. Institutionerne er blevet bedt om at redegøre for, hvorvidt de opdaterede retningslinjer er blevet implementeret, og – i tilfælde af manglende implementering – oplyse, hvornår implementeringen forventes gennemført.

Status er, at departementet og syv ud af ministeriets ni institutioner på nuværende tidspunkt har implementeret Justitsministeriets opdaterede retningslinjer.

Punk 10.f blev ikke behandlet på mødet.

10.g Status vedr. M365

V/ABKN

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

Sagsfremstilling

Statens IT (SIT) meddelte i en e-mail den 27. september 2024 til sine kunder, at det nu er muligt at overgå til M365 i en cloudversion. I samme forbindelse anmodede SIT om en bindende tilkendegivelse af departementets interesse med en svarfrist den 1. december 2024. SIT har desuden oplyst, at en anden bølge af overgange vil blive mulig, og det forventes, at der i løbet af 2025 vil blive fremsendt nye tilbud til dem, der afslår det aktuelle tilbud.

IT og ISDB-enheden har udarbejdet et baggrundsnotat med henblik på at vurdere de forretningsmæssige fordele og de databeskyttelsesmæssige opgaver, som en overgang til M365 vil indebære (bilag 10g.1).

Sagen er med udgangspunkt i baggrundsnotatet blevet behandlet i direktionen mandag den 25. november, som tiltrådte ITs og ISDB-enhedens indstilling om, at departementet inden 1. december 2024 meddeler SIT, at vi ikke ønsker at gå over til M365 på nuværende tidspunkt, at departementet tager stilling på ny ifm. SITs tilbud om overgang i 2. bølge (formentlig i 2025), at ISDB og IT først i den forbindelse igangsætter analyser/teknisk implementering

Beslutningen er efterfølgende meddelt til SIT.

Bilag
Bilag 10g.1 - Notat vedr. M365 til brug for direktionsmøde d. 25. nov.

Beslutning

Udvalget tog orienteringen til efterretning. ABKN oplyste supplerende til sagsfremstillingen, at direktionen ønsker at arbejde henimod at få Tems gjort tilgængelig for medarbejderne fra det tidligere IBM.

ISDB-enheden planlægger i den forbindelse at gennemføre en compliancevurdering og en risikovurdering af Teams, som vil blive forelagt direktionen i løbet af første kvartal 2024. ABKN oplyste desuden, at Skype har end of life oktober 2025.

LRJ føjede til, at det teams-modul, der skal stilles til rådighed for det tidligere IM, kun kan benyttes til at holde on-linemøder.

11. Eventuelt

v/CLSO

HGN bemærkede, at der er meget plads i top-menu på ISM-intra, som evt. kan benyttes til en mere fremtrædende plads på til informationssikkerhed, herunder retningslinjerne, som er svære at finde.
ABKN svarede, at ISDB-enheden tidligere har været i dialog med kommunikation vedr. design, og at ISDB-enheden gerne på ny tager en dialog om placering af informationssikkerhed på intra.
FKD oplyste, at han og LJE har været til møde hos SIT, som havde oplyst, at de nu kan tilbyde at hoste egne AI-løsninger til en overkommelig pris. Borgerbrevsenheden deltog også i mødet.

TRBR bemærkede, at koncern-HR forbereder et kursus vedr. brug AI for hele koncernen, hvor ISDB-enheden vil blive inddraget i planlægningen

12. Næste møde

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