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: 29-11-2024
Enhed: ISDB-enheden
Sagsbeh.: HBN
Sagsnr.: 2023-2167
Akt-id. nr.: 260801

Version: 1.1
Godkendt af: CID-udvalg
Gældende fra: 13-12-2024

Politik for Cyber-, Informationssikkerhed og Databeskyttelse i Indenrigs- og Sundhedsministeriets departement (CID-politikken)

1. Indledning

Denne politik for cyber-, informationssikkerhed og databeskyttelse i Indenrigs- og Sundhedsministeriets departement (CID-politikken) udgør en central del af departementets samlede ledelsessystem for cyber-, informationssikkerhed og databeskyttelse. Det samlede ledelsessystem omfatter tillige de retningslinjer, procedurer og vejledninger mv., som departementet fastsætter på området.

CID-politikken sætter rammerne for, hvordan arbejdet med cybersikkerhed, informationssikkerhed og databeskyttelse tilrettelægges og styres. Formålet med arbejdet er at sikre **fortrolighed**, **integritet** og **tilgængelighed** for de informationer og data herunder personoplysninger, som departementet (DEP) har ansvar for inden for rammerne af relevante lov-, myndigheds- og kontraktkrav. Dette er forudsætningen for en stabil varetagelse af opgaver i DEP, og for at DEP kan opfylde sine forpligtelser over for borgere, andre myndigheder og samarbejdspartnere.

2. Formål

CID-politikken har til formål:

1) At fastlægge de **overordnede rammer** for arbejdet med cybersikkerhed, informationssikkerhed og databeskyttelse.
2) At fastlægge en række **målsætninger** for departementets CID-arbejde med et tidssvarende og tilstrækkeligt højt niveau.
3) At fastlægge **ansvar og organisering** vedr. cybersikkerhed, informationssikkerhed og databeskyttelse.

3. Omfang og gyldighed

CID-politikken gælder i alle sammenhænge, hvor informationer og data behandles, herunder opbevares og anvendes, uanset i hvilken form af eller på vegne af Indenrigs- og Sundhedsministeriet departement og den selvstændige myndighed[1] under Indenrigs- og Sundhedsministeriet, Benchmarkingenheden[2].

CID-politikken gælder for:

- Alle medarbejdere i departementet og Benchmarkingenheden, uanset ansættelsesform og arbejdsopgaver, samt eksterne konsulenter

[1] Jf. konklusionen i notatet "Databeskyttelsesrådgiver efter ressortomlægningen", af 9. februar 2023, WZ sagsnr. 2300657

[2] Departementet sekretariatsbetjener Benchmarkingenheden på alle områder, denne politik gælder for, jf. notatet "Databeskyttelsesrådgiver efter ressortomlægningen", af 9. februar 2023, WZ sagsnr. 2300657.

- Alle systemer, alle data og øvrige informationsaktiver som departementet og Benchmarkingheden har ansvar for
- Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til departementets og Benchmarkingenhedens systemer og data.

4. Overordnede rammer

CID-arbejdet i departementet tager afsæt i god praksis for informationssikkerhed og implementeringen af ISO 27001-kravstandarden, med en risikobaseret tilgang til styring af informationssikkerhed. Som den øvrige ISM-koncern implementerer departementet desuden kravstandarden i ISO 27701.

Det primære lovgrundlag for sikkerhedsarbejdet og denne politik er databeskyttelsesforordningen og databeskyttelsesloven. Behandlingen af data og personoplysninger i DEP er også reguleret i andre love. Det gælder bl.a. forvaltningsloven, offentlighedsloven og NIS2.

Endelig refererer sikkerhedsarbejdet i departementet til nationale strategier, krav og anbefalinger på cyber-, informationssikkerhed og databeskyttelsesområdet. Her tænkes eksempelvis på Den fællesoffentlige digitaliseringsstrategi, National strategi for cyber- og informationssikkerhed 2022-2024 samt Digitaliseringsstyrelsens tekniske minimumskrav og øvrige anbefalinger fra CFCS, FE og PET.

5. Målsætninger

CID-udvalget har fastsat en række målsætninger for departementets arbejde med cyber-, informationssikkerhed og databeskyttelse, herunder for at sikre et tidssvarende og tilstrækkeligt højt sikkerhedsmæssigt niveau:

1. Departementets ledelsessystem for cyber-, informationssikkerhed og databeskyttelse er velfungerende og følger kravstandarderne ISO 27001 og ISO 27701, herunder bl.a. ift. løbende godkendelse og vedligehold af:
    a. systemoversigt over departements systemer og processer, herunder departementets artikel 30-fortegnelser.
    b. departementets retningslinjer for arbejdet med risici og trusselskatalog.
    c. departementets SoA (Statement of Applicability), hvor relevante kontroller og foranstaltninger udvælges og vurderes med henvisning til væsentlig dokumentation og afvigelser.
2. Ledere og medarbejderes viden og bevidsthed om cyber-, informationssikkerhed og databeskyttelse understøttes og øges vha. awareness-tiltag.
3. Der er klarhed om roller, ansvar og opgaver blandt departementets forskellige aktører i CID-arbejdet.
4. Efterlevelse af de tekniske minimumskrav, skærpede krav til kontrakt- og leverandørstyring for kritisk it-infrastruktur og tiltag for styrket cybersikkerhed.
5. Status for den samlede implementering af ISO27001 og ISO 27701 rapporteres til CID-udvalget mindst en gang om året.
6. Status for den samlede implementering af ISO27001 og ISO27701 rapporteres til departementschefen mindst en gang om året.

For at understøtte arbejdet med at realisere målsætningerne og med henblik på at prioritere indsatserne udarbejder CID-udvalget étårige handleplaner.

CID-udvalget følger mindst en gang årligt op på, om målsætningerne realiseres.

CID-udvalget følger løbende op på gældende handleplan og reviderer ved behov.

6. Ansvar og organisering

Det øverste ansvar for cybersikkerhed, informationssikkerhed og databeskyttelse i departementet påhviler departementschefen.

Den løbende overvågning og udvikling af området varetages af CID-udvalget. Departementschefen har den 10. oktober 2023 godkendt Kommissorium for CID-udvalget, der beskriver indhold, roller og ansvar for arbejdet i udvalget.

CID-udvalget har ansvaret for, at målsætningerne i nærværende politik samt indsatserne i handleplanen realiseres, og for at departementschefen inddrages i nødvendigt omfang.

Beslutninger på CID-området skal så vidt muligt træffes tæt på de berørte forretningsområder. Dette hensyn afspejles bl.a. i sammensætningen af CID-udvalget, idet væsentligste forretningsområder er repræsenteret. Udvalgets beslutninger skal bygge på et afvejet helhedshensyn, hvor bl.a. cyber- og informationssikkerhed, brugervenlighed og økonomi balanceres. Det er centralt, at indsatsen er proportional med truslerne for organisationen, de registrerede og samfundet. Udvalgets medlemmer medvirker aktivt til at formidle de trufne beslutninger til organisationen.

Departementets uafhængige databeskyttelsesrådgiver (DPO) har en rådgivende og overvågende funktion i relation til departementets behandling af personoplysninger og inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.

7. Dispensation

Dispensationer fra politikker, retningslinjer eller procedurer i departementet, kan alene ske efter inddragelse af CID-udvalget og på baggrund af konkret risikovurdering. Dispensationer, herunder risikovurderinger, skal dokumenteres skriftligt. CID-udvalget registrer alle dispensationer.

Departementets øvrige politikker, retningslinjer og procedurer kan indeholde mere specifikke regler vedrørende dispensation på bestemte områder, som i givet fald går forud for ovenstående.

8. Opfølgning

CID-politikken skal revideres ved større ændringer.

9. Versioner

Version	Godkendt af	Gyldig fra dato	Status	Bemærkninger/ændringer
1.0	CID-udvalget	13-12-2023		
1.1	CID-udvalget	13-12-2024	Gældende	Tilføjet Benchmarkingenheden, flyttet punktet omfang og gyldighed fra punkt 6 til punkt 3