INDENRIGS- OG
SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

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

Dato: 29-07-2025
Enhed: IT & ISDB
Sagsbeh.: FKD
Sagsnr.: 2023-2167
Akt-id. nr.: 53482

Version: 1.0
Godkendt af: CID-udvalget
Gældende fra: 01-09-2025

Politik for risikostyring i Indenrigs- og Sundhedsministeriets departement (Politik for risikostyring)

1. Indledning

Denne politik udgør den overordnede ramme for risikostyring af cyber, informationssikkerhed og databeskyttelse i Indenrigs- og Sundhedsministeriets departement (ISM-DEP).

2. Omfang for risikostyring

Politik for risikostyring skal omfatte følgende ISO-standarder og lovgivning, der stiller krav om styring af risiko af ISM-DEP´s informationsaktiver:

ISO-standarder

- ISO/IEC 27001:2023.
- ISO/IEC 27701:2019.

Lovgivning

- Databeskyttelsesforordningen (GDPR)[1] og databeskyttelsesloven[2].
- NIS 2-direktivet[3] og NIS 2-loven[4] (NIS 2).

Krav til risikostyring

ISM-DEP risikovurderer relevante processer og systemer (informationsaktiver). Risikovurderinger genbesøges med faste intervaller og i øvrigt efter behov.

Som led i risikovurderinger foretages en konkret vurdering af trusler og sårbarheder og de konsekvenser, som et brud på fortroligheden, integriteten, tilgængeligheden og autenticiteten vil have for departementet, den registrerede og/eller for samfundet. Konsekvenserne holdes op imod sandsynligheden for, at et brud finder sted.

På baggrund af de enkelte risikovurderinger vælges relevante risikohåndteringsmuligheder (acceptér, modificér, del, undgå). Dette skal sikre, at de identificerede risici ved et informationsaktiv har eller får et acceptabelt niveau i overensstemmelse med ISM-DEP's risikotolerance.

Alle identificerede risici ved et informationsaktiv skal accepteres eller undgås før risikostyringen af et informationsaktiv er gennemført.

ISM-DEP's samlede risikobillede skal rapporteres til Cyber-, informationssikkerhed- og databeskyttelsesudvalg (CID-udvalget) mindst én gang årligt.

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

[2] LOV nr 502 af 23/05/2018 - Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

[3] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet).

[4] LOV nr 434 af 06/05/2025 - Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven).

3. Roller og ansvar

CID-udvalget fastlægger konsekvens- og sandsynlighedstabeller på baggrund af en konkret anbefaling fra ISDB & IT.

Direktionen fastlægger på baggrund af en konkret anbefaling fra CID-udvalget rammer for ISM-DEP´s risikotolerance, herunder de ledelsesniveauer som kan acceptere en identificeret risiko.

For hvert system eller proces er der udpeget en ejer hos ISM-DEP, som er ansvarlig for at sikre informationsaktivers tilstrækkelige sikkerhedsniveau.

4. Udmøntning af politikken

Denne politik udmøntes af CID-udvalget i relevant omfang gennem fastsættelse af regler og udarbejdelse af retningslinjer, der skal sikre ensartethed, tilstrækkelighed og sporbarhed i forbindelse med varetagelsen af de opgaver, der er fastsat i denne politik. CID-udvalget kan jf. politik for cyber- informationssikkerhed og databeskyttelse, i relevant omfang delegere ansvaret for udmøntning af denne politik til ISDB & IT.

5. ISO/IEC-referencer

Dette afsnit omhandler alene departementets dokumentation af efterlevelse af relevante ISO-standarder. Det skal i den forbindelse bemærkes, at ISO 27701:2019 er en komplimenterende standard til ISO 27001:2023, hvilket betyder at efterlevelsen af ISO 27701:2019 flere steder dokumenteres i ISO 27001:2023.

ISO/IEC 27001:2023
6.1, 6.1.2, 6.1.3, 6.2, 8.3, A.5.19, A.5.20, A.5.21.

6. Versionsstyring

Version	Godkendt af	Dato	Status	Bemærkninger/ændringer
1.0	CID-udvalget	29-08-2025	Godkendt	Godkendt på CID-udvalgsmøde d. 29-08-2025