Informationssikkerhedspolitik

Klassifikation	Offentlig
Politik	Informationssikkerhedspolitik
Procedure	

MedComs informationssikkerhedspolitik for Systemforvaltningen

1. Formål

Formålet med denne politik er at fastlægge de overordnede mål og principper for informationssikkerheden i MedComs systemforvaltning.

Politikken skal sikre, at alle informationer og systemer, som MedCom forvalter, beskyttes på et passende niveau i forhold til deres betydning og risiko.

Retningslinjerne tager udgangspunkt i den internationale standard ISO/IEC 27001 samt gældende lovgivning, herunder NIS2-direktivet og databeskyttelsesforordningen (GDPR). Lovkravene er strategisk forankret i MedComs risikostyring og overordnede Informationssikkerhedsstyring

Selvom MedCom ikke er direkte omfattet af NIS2, er MedCom indirekte berørt, da særligt Sundhedsdatanettet understøtter NIS2-omfattede parter. MedCom arbejder derfor i overensstemmelse med NIS2-principperne for at understøtte de tilsluttede parters forpligtelser og et højt samlet sikkerhedsniveau i sundhedssektoren.

Politikken skal samtidig understøtte MedComs mission og vision samt sikre tillid til de fællesoffentlige sundheds-it-løsninger, som MedCom forvalter.

2. Anvendelsesområde

Politikken dækker de fire fællesoffentlige systemer, som MedCom forvalter:

- Sundhedsdatanettet (SDN)
- Videoknudepunktet (VDX)
- Hjemmemonitoreringsdatabasen (KIH)
- National Prøvenummer-service (NPN)

Politikken omfatter alle tekniske, organisatoriske og administrative forhold, der har direkte eller indirekte indflydelse på drift, vedligehold og anvendelse af disse systemer.

Dette gælder også behandling af personoplysninger, herunder følsomme helbredsoplysninger, som MedCom behandler som databehandler for sundhedssektoren.

3. Ledelsesforankring og ansvar

Det overordnede ansvar for Informationssikkerheden ligger hos MedComs styregruppe.

Det daglige ansvar ligger hos MedComs direktør - og med MedComs Informationssikkerhedsudvalg som den strategiske og operationelle ramme for MedComs arbejde med Informationssikkerhed.

MedComs Informationssikkerhedsudvalg består af:

- MedComs direktør
- MedComs sikkerhedsansvarlige
- MedComs DPO (Databeskyttelsesrådgiver)
- Ledelsen for Intern IT og systemforvaltning
- Informationssikkerhedskoordinatorer

Disse sikrer, at sikkerhedsindsatsen er risikobaseret, systematisk og dokumenteret – og at der sker opfølgning og ledelsesrapportering.

4. Grundprincipper for Informationssikkerhed

MedComs arbejde med Informationssikkerhed tager udgangspunkt i følgende overordnede principper:

- Risikobaseret tilgang: Alle sikkerhedsforanstaltninger baseres på vurdering af trusler, sårbarheder og konsekvenser
- Proportionalitet: Kontroller skal stå i rimeligt forhold til risici og lovkrav
- Ledelsesforankring: Ledelsen skal løbende sikre prioritering, opfølgning og forbedring
- Systematik og dokumentation: Alle væsentlige aktiviteter dokumenteres og evalueres
- Awareness og kompetencer: Medarbejdere og leverandører skal forstå deres ansvar for sikkerhed
- Kontinuerlig forbedring: Informationssikkerheden skal løbende vurderes og tilpasses ændringer i risikobilledet
- Pålidelig systemforvaltning: Systemer skal være robuste, stabile og forvaltes sikkert og ansvarligt

5. Mål for Informationssikkerhed

MedComs mål for Informationssikkerhed er at beskytte data og systemer på et højt og tidssvarende niveau i overensstemmelse med gældende lovgivning og standarder:

- Fortrolighed: Kun autoriserede personer må få adgang til data
- Integritet: Data og systemer skal være korrekte og pålidelige
- Tilgængelighed: Systemer og data skal være tilgængelige, når der er behov for dem.
- Forretningsunderstøttelse: Sikkerheden skal understøtte effektiv drift og patientsikkerhed uden at hindre autoriseret adgang til nødvendige oplysninger
- Lovmæssig overholdelse: MedCom skal efterleve GDPR, NIS2 og øvrige relevante krav.

Da sundhedspersonale potentielt træffer kritiske beslutninger på baggrund af de data, der løber igennem SDN, VDX og KIH er fortrolighed, integritet og tilgængelighed afgørende for at sikre både databeskyttelse og kontinuitet i behandlingen. Disse faktorer er samtidig fundamentale for tilliden til MedCom og samarbejdet i sundhedsvæsenet.

6. Risikostyring

MedCom anvender en systematisk risikostyringsproces, hvor:

- Risici identificeres, vurderes og behandles ud fra ISO 27005-principper
- Risikovurderinger gennemføres mindst én gang årligt
- Resultater anvendes til prioritering af sikkerhedsforanstaltninger, investeringer og forbedringer
- Risikostyringen dokumenteres og indgår i ledelsesrapporteringen

7. Sikkerhed i drift og leverandørstyring

Alle leverandører og samarbejdspartnere, der håndterer informationer eller systemer på vegne af MedCom, skal:

- Overholde MedComs Informationssikkerhedspolitik og gældende lovgivning
- Have indgået en databehandleraftale, hvor relevant
- Kunne dokumentere overholdelse af relevante standarder (f.eks. ISO 27001, ISAE 3402/3000)
- Have etableret beredskabsplaner og hændelsesprocedurer

Disse forhold indgår i leverandørkontrakterne. Manglende overholdelse af Informationssikkerhedskravene håndteres i overensstemmelse med kontraktens bestemmelser.

Der udføres tilsyn og løbende opfølgning og rapportering på leverandørernes efterlevelse.

8. Hændelseshåndtering og beredskab

MedCom har etableret procedurer for:

- Identifikation, registrering og klassificering af hændelser
- Eskalering, herunder til DPO
- Kommunikation og gendannelse
- Evaluering og læring
- Beredskabsøvelser og dokumentation

Beredskabet vedligeholdes og testes minimum årligt.

Der skal gennemføres monitorering og rapportering af sikkerhedshændelser.

9. Awareness, træning og sikkerhedsbevidsthed

Alle relevante medarbejdere skal have viden om Informationssikkerhed i relation til deres rolle. MedCom gennemfører:

- Introduktion til Informationssikkerhed ved ansættelse
- Løbende awareness-aktiviteter og træning
- Ledelsesorientering

Effekten af awareness-indsatsen evalueres årligt.

10. Overvågning, audit og compliance

Der gennemføres løbende audits og ledelsesevalueringer i henhold til ISO/IEC 27001:2022.

Dette omfatter:

- Ledelsens gennemgang
- Evaluering af overholdelse af ISO 27001, GDPR og NIS2
- ISAE 3000-erklæring for SDN og VDX
- Systematiske revurderinger med fokus på forbedring af ledelsessystemet og informationssikkerheden

11. Dispensation fra informationssikkerhedspolitikken

Dispensation fra denne politik kan kun ske efter:

- En risikovurdering
- Implementering af kompenserende foranstaltninger
- Godkendelse fra MedComs ledelse

Dispensation må aldrig være i strid med gældende lovgivning.

Overtrædelser af politikken og de heraf afledte retningslinjer behandles efter gældende personaleretlige regler og MedComs personalehåndbog.

12. Revision, gyldighed og kommunikation

Politikken revideres minimum én gang årligt og altid ved væsentlige ændringer i:

- Organisation
- Teknologi
- Lovgivning (fx NIS2, GDPR)
- Risikobilledet

Revisionen behandles af Informationssikkerhedsudvalget og godkendes ved væsentlige ændringer af MedComs styregruppe.

Informationssikkerhedspolitikken gøres tilgængelig på MedComs website.

Behandlet i MedComs styregruppe den 01.12.25

Revisions Historik

Version	Forfatter	Dato	Bemærkning
2.2		20.02.17	
2.3	TGJ	01.06.18	Justering under punkt 4 med indførelse af Databeskyttelsesloven i stedet for Persondataloven.
2.4	LAH/TGJ	18.08.21	Sproglige ændringer og præciseringer.
2.4	TGJ	28.08.22	Behandlet i MedComs styregruppe. Ingen ændringer.
2.4	TGJ	14.12.23	Behandlet i MedComs styregruppe. Ingen ændringer.
2.4	TGJ	07.03.24	Behandlet i MedComs styregruppe. Ingen ændringer.
2.5	TGJ	27.11.24	Behandlet i MedComs styregruppe. Der er under pkt. 4 indsat reference til NIS2 under lovgivning, som MedCom i relevant omfang skal overholde.
2.6	TGJ	20.10.25	En gennemgående omskrivning af Informationspolitikken med henblik på at øge overskueligheden – og at adressere MedComs roller og forpligtigelser i relation til NIS2. Behandlet på møde i Informationssikkerhedsudvalg 28.10.25. Behandlet på møde i MedComs styregruppe 01.12.25