					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P02					Dokumenttitel: **Politik for styringsroller og ansvarsområder**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3; bilag A, kontrol 5	
ISO/IEC 27002:2022	Kontrol 5	
NIST SP 800-53 Rev.5	PL-1 til PL-4, PM-1 til PM-13	
EU GDPR	Artikel 5(1)(f), 24, 37	
EU NIS2	Artikel 21(2)(a)	
EU DORA	Artikel 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Formål

1.1 Denne politik fastlægger den styringsmodel, de organisatoriske roller og de ansvarsområder, der er nødvendige for at drive et effektivt ledelsessystem for informationssikkerhed (ISMS).

1.2 Den etablerer klare linjer for ansvar, beslutningskompetence og eskalationsveje for at sikre, at informationssikkerhed er forankret på alle niveauer i organisationen og afstemt med de strategiske forretningsmål.

1.3 Politikken implementerer kravene i ISO/IEC 27001:2022, klausul 5.3 og kontrol A.5.2, og sikrer, at ansvaret for sikkerhedsrelaterede aktiviteter er klart tildelt, dokumenteret, kommunikeret og gennemgås periodisk.

1.4 Denne politik danner også grundlag for integreret styring med andre fagområder såsom risikostyring, efterlevelse, it-drift og juridiske funktioner.

2. Omfang

2.1 Denne politik gælder for alle personer og enheder, der indgår i styring, drift og tilsyn med informationssikkerhed inden for ISMS'ets omfang. Dette omfatter:

2.1.1 Den øverste ledelse, den daglige ledelse og bestyrelsesmedlemmer

2.1.2 ISMS-ansvarlige, CISO'er og kontrolansvarlige

2.1.3 Procesansvarlige og aktivansvarlige

2.1.4 Konsulenter og tredjepartsleverandører med delegerede sikkerhedsansvarsområder

2.2 Den omfatter både interne funktioner og funktioner leveret af eksterne parter (f.eks. outsourcet SOC eller administratorer af cloudplatforme), hvor styringsroller er formelt tildelt eller kontraktuelt fastlagt.

2.3 Politikken gælder også for organisatoriske enheder, afdelinger og projektteams, der forvalter eller påvirker sikkerhedsrelevante aktiver, systemer eller tjenester.

3. Mål

3.1 At sikre, at roller og ansvarsområder for informationssikkerhed er formelt defineret, tildelt, kommunikeret og dokumenteret.

3.2 At opretholde en styringsmodel, der sikrer funktionsadskillelse, eliminerer interessekonflikter og muliggør eskalation af uafklarede sikkerhedsforhold.

3.3 At sikre, at ansvar og beslutningskompetence for sikkerhedsbeslutninger er fordelt i overensstemmelse med forretningsmæssig påvirkning og organisationsstruktur.

3.4 At etablere en ramme for håndtering af delegeringer, rolleændringer og gennemgang af tildelte ansvarsområder.

3.5 At give interessenter — herunder tilsynsmyndigheder, revisorer og kunder — sikkerhed for, at informationssikkerhed styres effektivt og i overensstemmelse med relevante standarder.

4. Roller og ansvarsområder

4.1 Øverste ledelse

4.1.1 Udøver strategisk tilsyn, allokerer ressourcer og sikrer sammenhæng mellem ISMS-mål og forretningsmål.

4.1.2 Godkender central ISMS-dokumentation, herunder informationssikkerhedspolitikken, risikobehandlingsplaner og beslutninger om opfølgning på revisioner.

4.1.3 Deltager i ledelsens gennemgang af ISMS og eskalerer beslutninger, der kræver godkendelse på bestyrelsesniveau.

4.1.4 Fremmer en sikkerhedskultur og understøtter organisatorisk efterlevelse af principperne for sikkerhedsstyring.

4.2 Styregruppe for informationssikkerhed (ISSC)

4.2.1 Fungerer som tværgående styringsorgan for tilsyn med ISMS.

4.2.2 Gennemgår risikobillede, kontrolperformance, revisionsresultater og strategiske sikkerhedsinitiativer.

4.2.3 Understøtter koordinering mellem afdelinger (f.eks. it, jura, HR, risiko, efterlevelse og drift).

4.2.4 Godkender eskalationstærskler, budgetallokeringer og politikændringer, der kræver ledelsesmæssig stillingtagen.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Plan for gennemgang

9.1.1 Denne politik skal gennemgås mindst årligt eller ved indtræden af:

9.1.1.1 Ændringer i organisationsstrukturen eller ledelsesteamet

9.1.1.2 Udvidelse eller omdefinering af ISMS'ets omfang

9.1.1.3 Regulatoriske ændringer, der påvirker rolletildeling eller tilsyn

9.1.1.4 Væsentlige revisionsresultater eller hændelser, der involverer svigt i styringen

9.2 Proces for gennemgang og godkendelse

9.2.1 ISMS-ansvarlig skal igangsætte og lede gennemgangen, herunder indsamling af input fra interessenter og tilbagemeldinger fra revision.

9.2.2 Foreslåede opdateringer skal gennemgås af ISSC og formelt godkendes af den øverste ledelse.

9.2.3 Hver version skal registreres i ISMS-dokumentregistret og indeholde følgende metadata:

9.2.3.1 Politik-id og titel

9.2.3.2 Versionsnummer og ændringsresume

9.2.3.3 Ikrafttrædelsesdato og næste dato for gennemgang

9.2.3.4 Politikejer og godkender

9.2.3.5 Dokumentklassifikationsniveau

9.2.3.6 Opbevarings- og arkivhistorik

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal fortolkes i sammenhæng med følgende politikker:

10.1.1 P1 – Informationssikkerhedspolitik: Etablerer det overordnede sikkerhedsprogram og beskriver ledelsens ansvar for godkendelse af politikker og strategisk tilsyn.

10.1.2 P5 – Politik for ændringsstyring: Sikrer, at ændringer i styringsstrukturer, roller eller ansvarsområder er underlagt dokumenteret godkendelse og risikogennemgang.

10.1.3 P6 – Politik for risikostyring: Identificerer og behandler styringsrisici, der opstår som følge af rollekonflikter, ikke-tildelte opgaver eller manglende eskalation.

10.1.4 P7 – Politik for onboarding og fratrædelse: Sikrer processer for tildeling og tilbagekaldelse af kontroller ved ændringer i personalets livscyklus.

10.1.5 P33 – Politik for revision og overvågning af efterlevelse: Understøtter uafhængig gennemgang af effektiviteten af styringen og håndhæver korrigerende handlinger ved manglende efterlevelse.

10.2 Disse politikker understøtter samlet en ensartet og håndhævelig styringsramme for ISMS.

11. Referencestandarder og rammeværk

11.1 Denne politik er afstemt med globalt anerkendte standarder og rammeværk for styring af informationssikkerhed og ansvar for roller. Den sikrer sporbarhed til regulatoriske krav og certificeringskrav og understøtter en juridisk forsvarlig ISMS-struktur.

11.2 ISO/IEC 27001

11.2.1 Klausul 5.3 – Organisatoriske roller, ansvarsområder og beføjelser: Denne politik opfylder kravet om, at roller med relevans for informationssikkerhed skal være klart tildelt, kommunikeret og dokumenteret.

11.2.2 Klausul 9.3 – Ledelsens gennemgang: Denne politik sikrer ledelsesmæssigt tilsyn med ISMS-roller og styring gennem kvartalsvise og årlige gennemgange.

11.2.3 Bilag A, kontrol 5.2 – Roller og ansvarsområder for informationssikkerhed: Definerer roller på teknisk, operationelt og strategisk niveau for at sikre funktionsadskillelse, risikoejerskab og sporbar ansvarsplacering.

11.3 ISO/IEC 27002:2022 – Kontrol 5

11.3.1 Indeholder vejledning i implementering af tildeling af ansvar for informationssikkerhed i en organisation. Denne politik anvender denne vejledning ved at definere rolletyper, regler for delegering, eskalationsprocedurer og mekanismer for gennemgang.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 til PL-4: Fastlægger behovet for formel planlægningsdokumentation, herunder politikker, der definerer styring og tildeler sikkerhedsansvar.

11.4.2 PM-1 (plan for informationssikkerhedsprogram) og PM-2 (øverste ansvarlige for informationssikkerhed): Afspejles i denne politik gennem tildelingen af CISO/ISMS-ansvarlig og formelle styringsroller.

11.4.3 PM-5 til PM-13: Denne politik opfylder krav til roldokumentation, roller for risikostyring på tværs af organisationen, tilsyn med konfigurationsstyring og integration med missions- og forretningsfunktioner.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 5(1)(f): Kræver, at personoplysninger beskyttes mod uautoriseret eller ulovlig behandling. Denne politik sikrer, at personer med ansvar for databeskyttelse er klart udpeget og underlagt tilsyn.

11.5.2 Artikel 24: Kræver passende organisatoriske foranstaltninger, herunder styringsstrukturer.

11.5.3 Artikel 37: Kræver udpegning af en databeskyttelsesrådgiver (DPO), som skal afspejles i organisationens styringsramme og register over ansvarsområder.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Artikel 21(2)(a): Pålægger enheder at implementere politikker for risikoanalyse og informationssystemsikkerhed, herunder rollespecifikke ansvarsområder. Denne politik definerer sådanne roller og deres styringsmekanismer.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 – Styrings- og intern kontrolramme: Kræver formel tildeling af ansvar for styring af IKT-risici, beslutningsroller og rapporteringskanaler. Denne politik udgør grundlaget for styring af sikkerhedsrelaterede roller i IKT-miljøer.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: Denne politik sikrer, at ISMS har en klart defineret styringsstruktur, der er afstemt med virksomhedens behov.

11.8.2 EDM02 – Ensured Benefits Delivery: Afstemmer rollebaserede sikkerhedsaktiviteter med strategiske og operationelle mål og sikrer ansvar og målbare resultater.

11.8.3 APO01 – Managed I&T Management Framework og APO12 – Managed Risk: Denne politik understøtter struktureret styring af informationssikkerhedsroller inden for en bredere ramme for it-styring og risikostyring.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: Indbygger mekanismer for gennemgang, så det kan verificeres, at styringsroller er effektive, ajourførte og håndhæves.