					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P02S					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, hvor det er relevant

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	
ISO/IEC 27002:2022	Kontroller: 5.2, 5.3, 5	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EU GDPR	Artikel 5(2), 32	

1. Formål

1.1 Denne politik fastlægger, hvordan ansvar for informationssikkerhedsstyring tildeles, delegeres og styres i organisationen for at sikre fuld overensstemmelse med ISO/IEC 27001:2022 og andre regulatoriske forpligtelser.

1.2 Den sikrer ansvarlighed på alle niveauer og understøtter operationel effektivitet ved klart at fastlægge, hvem der er ansvarlig for hver sikkerhedsrelateret funktion.

1.3 Denne politik styrker revisionsberedskabet og opbygger kundetillid ved at dokumentere formel sikkerhedsstyring, også i organisationer med begrænsede tekniske ressourcer eller outsourcede IT-ydelser.

2. Omfang

2.1 Denne politik gælder for alle personer, der håndterer organisationens systemer eller data, herunder:

2.1.1 Virksomhedsejere og daglige ledere

2.1.2 Medarbejdere og kontraktansatte

2.1.3 Eksterne IT-tjenesteudbydere eller konsulenter

2.2 Den omfatter alle systemer, miljøer og tjenester, der anvendes til at behandle, overføre eller opbevare virksomheds- eller kundeoplysninger, herunder:

2.2.1 Kontor-IT-infrastruktur og enheder til fjernarbejde

2.2.2 Cloudbaserede platforme og e-mailtjenester

2.2.3 Fysiske optegnelser og fællesdrev

2.3 Omfanget omfatter både interne og outsourcede aktiviteter vedrørende informationssikkerhedsstyring.

3. Målsætninger

3.1 Etablere klar ansvarlighed for alle sikkerhedsrelaterede opgaver, herunder politikstyring, adgangskontrol, hændelseshåndtering og overvågning.

3.2 Muliggøre effektiv funktionsadskillelse for at reducere interessekonflikter eller risiko for besvigelser.

3.3 Sikre, at sikkerhedsopgaver og roller er tydeligt dokumenteret og gennemgås regelmæssigt.

3.4 Muliggøre velbegrundet beslutningstagning, eskalering og tilsyn med IT- og sikkerhedsrisici.

3.5 Understøtte certificering efter ISO/IEC 27001:2022 og skabe tillid hos kunder, partnere og revisorer.

4. Roller og ansvar

4.1 Daglig leder/virksomhedsejer

4.1.1 Har det overordnede ansvar for implementering af og tilsyn med denne politik.

4.1.2 Godkender alle sikkerhedsroller, ansvarsområder og beslutninger om delegering.

4.1.3 Overvåger efterlevelse og træffer endelig beslutning om politikundtagelser og eskaleringer.

4.2 Udpeget sikkerhedskoordinator (hvis relevant)

4.2.1 Kan være en medarbejder eller en betroet konsulent.

4.2.2 Rollen kan i mikrovirksomheder varetages af den daglige leder eller en ekstern udbyder.

4.2.3 Bistår med den daglige håndhævelse af adgangskontrol, håndtering af sikkerhedshændelser og grundlæggende tekniske sikkerhedsopgaver.

4.2.4 Rapporterer direkte til den daglige leder om sikkerhedsforhold eller risici.

[... 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 Årlig gennemgang

9.1.1 Denne politik skal gennemgås af den daglige leder hver 12. måned for at sikre, at den fortsat afspejler juridiske forpligtelser, operationelle behov og krav til certificering efter ISO/IEC 27001.

9.2 Løbende gennemgange

9.2.1 Gennemgang skal også gennemføres, når:

9.2.1.1 Der sker væsentlige organisatoriske ændringer

9.2.1.2 En ny udbyder onboardes

9.2.1.3 Der opstår en alvorlig sikkerhedshændelse

9.2.1.4 Regler som GDPR, NIS2 eller DORA opdateres

9.3 Versionsstyring og dokumentation

9.3.1 Alle gennemgange skal omfatte:

9.3.1.1 Dato for gennemgang

9.3.1.2 Resumé af eventuelle ændringer

9.3.1.3 Signatur eller dokumenteret godkendelse fra den daglige leder

9.3.1.4 Arkiverede tidligere versioner til brug ved revision

9.4 Kommunikation af ændringer

9.4.1 Alle opdateringer af politikken skal straks kommunikeres til medarbejdere og udbydere via e-mail, interne portaler eller formelle meddelelser.

10. Relaterede politikker og sammenhænge

10.1 Denne politik bør implementeres sammen med følgende SME-politikker for at sikre fuld effekt:

10.1.1 P4S – Politik for adgangskontrol: Definerer, hvordan adgang tildeles, styres og tilbagekaldes, og er direkte knyttet til tildelte roller og tilsyn.

10.1.2 P8S – Politik for informationssikkerhedsbevidsthed og -uddannelse: Understøtter rollebaserede ansvar og forventninger.

10.1.3 P17S – Politik for databeskyttelse og privatliv: Beskriver juridiske forpligtelser efter GDPR, som er tildelt roller defineret i denne styringspolitik.

10.1.4 P30S – Politik for hændelseshåndtering: Kræver fastlagte ansvarsområder for rapportering, eskalering og håndtering af hændelser.

10.2 Samlet set understøtter disse politikker konsekvent håndhævelse, intern ansvarlighed og ekstern efterlevelse.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3 – Organisatoriske roller, ansvar og beføjelser: Kræver, at roller tildeles tydeligt og understøttes af topledelsen.

11.2 ISO/IEC 27002

11.2.1 Kontroller 5.2–5.4: Kræver tydelig dokumentation af roller inden for informationssikkerhed, funktionsadskillelse og ledelsesmæssigt tilsyn.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Etablerer et overordnet program for informationssikkerhed med definerede ansvarsområder.

11.3.2 PL-1 til PL-4: Kræver planlægningskontroller, herunder udformning af politikker og dokumenterede rolletildelinger.

11.3.3 CA-1: Kræver definerede roller for vurdering og autorisation.

11.3.4 AC-1: Knytter rollebaseret adgangskontrol til tildelte styringsansvar.

11.4 EU GDPR

11.4.1 Artikel 5(2) – Ansvarlighed: Kræver, at organisationer kan dokumentere efterlevelse gennem roller og ansvarsområder.

11.4.2 Artikel 32 – Behandlingssikkerhed: Fremhæver tydelig tildeling af opgaver for at beskytte personoplysninger.

11.5 EU NIS

11.5.1 Artikel 21(2)(a): Kræver styringsstrukturer, der omfatter formaliserede roller til håndtering af cyberrisici og hændelser.

11.6 EU DORA

11.6.1 Artikel 9 og 10: Kræver, at finansielle enheder tydeligt tildeler og fører tilsyn med IKT- og sikkerhedsrelaterede ansvarsområder.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: Kræver veldefinerede roller og eskalationsveje til styring af sikkerhedsrisici.

11.7.2 APO13 – Manage Security: Tildeler strategiske og operationelle sikkerhedsopgaver til personer og roller.

11.7.3 DSS05 – Manage Security Services: Kræver struktur og sporbarhed i ansvarsområder for eksterne og interne sikkerhedstjenester.