| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | |
| Dokumentnummer:<br>P06S | | | | | Dokumenttitel:<br>**Risikostyringspolitik** | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>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 6.1, 6.1.3 | |
| ISO/IEC 27002:2022 | 5.4, 5.25 | |
| NIST SP 800-53 Rev. 5 | RA-1 til RA-7, PM-9 | |
| EU NIS2 | Artikel 21(2)(a–d) | |
| EU DORA | Artikel 5 | |
| COBIT 2019 | APO12, MEA01 | |

**1. Formål**

1.1 Denne politik fastlægger, hvordan organisationen identificerer, vurderer og håndterer risici relateret til informationssikkerhed, drift, teknologi og tredjepartstjenester.

1.2 Den sikrer, at risikostyring indgår som en aktiv del af planlægning, projektgennemførelse, leverandørvalg og håndtering af sikkerhedshændelser i overensstemmelse med ISO 27001, ISO 31000 og regulatoriske krav.

1.3 Politikken understøtter et oplyst beslutningsgrundlag, beskyttelse af informationsaktiver og robusthed i kritiske forretningsprocesser.

**2. Omfang**

**2.1 Denne politik gælder for:**

2.1.1 Alle afdelinger, systemer og brugere i organisationen

2.1.2 Alle oplysninger, tjenester og aktiver, der forvaltes internt eller via tredjeparter

2.1.3 Risikorelaterede aktiviteter, herunder projektgennemgange, systemopgraderinger, outsourcing og regulatorisk efterlevelse

**2.2 Den omfatter alle typer risici, herunder:**

2.2.1 cybersikkerhedstrusler og systemsårbarheder

2.2.2 driftsforstyrrelser og serviceafbrydelser

2.2.3 juridiske, efterlevelsesmæssige eller omdømmemæssige eksponeringer

2.2.4 tredjeparts- og forsyningskæderisici

2.3 Alle medarbejdere, kontrahenter og tjenesteudbydere skal følge denne politik ved identifikation og rapportering af risici.

**3. Målsætninger**

3.1 Integrere enkle og ensartede procedurer for risikovurdering i den daglige drift.

3.2 Identificere og prioritere risici, der kan påvirke fortrolighed, integritet, tilgængelighed eller juridisk efterlevelse.

3.3 Tildele ejerskab og fastlægge behandlingstiltag for alle væsentlige risici.

3.4 Opretholde et korrekt og ajourført risikoregister for at understøtte revisionsparathed og risikosporbarhed.

3.5 Sikre ledelsens involvering i godkendelse af risikotolerance og væsentlige behandlingsplaner.

**4. Roller og ansvar**

**4.1 Daglig leder**

4.1.1 Fastlægger organisationens risikovillighed og godkender rammerne for risikostyring.

4.1.2 Godkender væsentlige beslutninger om risikobehandling og tilhørende ressourceallokering.

4.1.3 Gennemgår de væsentligste risici kvartalsvist sammen med risikokoordinatoren.

**4.2 Risikokoordinator (eller ISMS-ejer)**

4.2.1 Faciliterer risikovurderinger og vedligeholder risikoregisteret.

4.2.2 Sikrer, at risikoscore, risikoejerskab og behandlingstiltag er dokumenteret.

4.2.3 Gennemfører mindst én formel risikogennemgang årligt.

[ ... 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 af politikken**

9.1.1 Denne politik skal gennemgås mindst én gang årligt af den daglige leder og risikokoordinatoren for at sikre relevans og fuldstændighed.

**9.2 Udløsere for opdatering**

**9.2.1 Tidligere gennemgang og opdatering skal gennemføres, hvis:**

9.2.1.1 En væsentlig hændelse eller en revisionskonstatering afdækker mangler i risikostyringen

9.2.1.2 Nye forretningsenheder, teknologier eller partnerskaber introduceres

9.2.1.3 Et regulatorisk eller kontraktuelt krav ændres

**9.3 Versionsstyring**

**9.3.1 Alle opdateringer til denne politik skal versionsstyres med følgende metadata:**

9.3.1.1 Versionsnummer og ikrafttrædelsesdato

9.3.1.2 Resumé af ændringer

9.3.1.3 Godkender (daglig leder)

9.3.1.4 Arkiverede tidligere versioner til revisionsformål

**9.4 Kommunikation og bevidstgørelse**

9.4.1 Opdaterede versioner af politikken og væsentlige risikobehandlingsplaner skal kommunikeres til berørte medarbejdere. Årlig awareness-træning skal omfatte grundlæggende principper for risikobevidsthed.

**10. Relaterede politikker og sammenhænge**

**10.1 Denne politik fungerer i samspil med flere andre politikker for at sikre en samlet sikkerhedsstyring:**

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Definerer, hvem der er ansvarlig for risikoejerskab og beslutningstagning.

10.1.2 P5S – P05 Ændringsstyringspolitik: Kræver risikovurdering før implementering af tekniske ændringer eller procesændringer.

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Adresserer regulatorisk risiko forbundet med behandling af personoplysninger.

10.1.4 P30S – Politik for hændelseshåndtering (P30): Sikrer, at risikobehandling fortsætter under og efter sikkerhedshændelser.

10.1.5 P33S – Politik for forretningskontinuitet: Identificerer restrisici og genopretningstiltag for kritiske tjenester.

## 11. Referencestandarder og styringsrammer

### 11.1 ISO/IEC 27001:

11.1.1 Klausul 6.1 – Etablerer en formel proces for risikostyring og planlægning af risikobehandling.

11.1.2 Klausul 6.1.3 – Kræver, at organisationer opretholder dokumenterede behandlingsplaner og godkendelser.

### 11.2 ISO/IEC 27002:

11.2.1 Kontroller 5.4, 5.25 – Giver vejledning om implementering af risikoejerskab, prioritering og livscyklusstyring.

### 11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 til RA-7 – Definerer risikovurdering, responsstrategier, dokumentation og gennemgangsmekanismer.

11.4 PM-9 – Kræver konsekvent ledelsesmæssigt tilsyn med organisationens risici.

### 11.5 EU NIS2-direktivet

11.5.1 Artikel 21(2)(a–d) – Pålægger væsentlige og vigtige enheder obligatoriske kontroller for risikovurdering, afbødning og styring.

### 11.6 EU DORA

11.6.1 Artikel 5 – Kræver, at regulerede enheder definerer og håndterer styringsrammer for IKT-risikostyring, herunder identifikation, klassificering og respons.

### 11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Integrerer risiko i strategisk og operationel planlægning.

11.7.2 MEA01 – Overvågning, evaluering og vurdering: Sikrer effektivitet og efterlevelse i risikoprocesser og handlinger.