					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P06					Dokumenttitel: **Politik for risikostyring**							
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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 8.32, 10	Kernekrav til risikoidentifikation og risikostyring, integration i ændringsstyring samt løbende forbedring
ISO/IEC 27005:2024	Fuld metode for risikolivscyklus	Fuld risikostyringsproces i overensstemmelse med standarden
ISO 31000:2018	Principper og rammeværk for risikostyring	Principper for risikostyring indarbejdet i styringsrammen
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Vejledning og struktur for risikovurderinger samt lagdelt risikostyring
EU GDPR	Artikel 24, 25, 32	Processer og kontroller for databeskyttelsesrisici
EU NIS2	Artikel 21(2)(a–d)	Krav vedrørende risiko- og sikkerhedsvurderinger
EU DORA	Artikel 5, 6	IKT-risikostyring og operationel robusthed
COBIT 2019	APO12, MEA	Struktur og tilsyn for risikostyring

1. Formål

1.1 Denne politik fastlægger en ensartet og formaliseret ramme for identifikation, analyse, evaluering, behandling, overvågning og gennemgang af informationssikkerhedsrisici på tværs af organisationen.

1.2 Den sikrer konsekvent anvendelse af risikobaserede principper, som beskytter fortrolighed, integritet og tilgængelighed (CIA) for informationsaktiver i overensstemmelse med ISO/IEC 27001:2022 klausul 6.1 og ISO 31000:2018.

1.3 Politikken integrerer informationssikkerhedsrisikostyring i organisationens beslutningsprocesser for at understøtte interne strategiske målsætninger og eksterne regulatoriske krav.

2. Omfang

2.1 Denne politik gælder for alle organisatoriske enheder, forretningsprocesser, systemer, medarbejdere og tredjepartsengagementer, der indgår i håndtering, udvikling, lagring eller styring af informationsaktiver.

2.2 Omfanget omfatter fysiske, digitale og cloud-hostede systemer og aktiver, herunder strukturerede og ustrukturerede data, applikationer, infrastruktur, netværk og tjenester.

2.3 Den omfatter informationssikkerhedsrisici på strategisk, operationelt, projektmæssigt og teknisk niveau og er obligatorisk for alle medarbejdere, kontrahenter og tjenesteudbydere, der deltager i ISMS-aktiviteter.

2.4 Risikostyring skal anvendes i følgende scenarier:

2.4.1 Implementering af nye projekter eller systemer

2.4.1.1 Væsentlige ændringer (f.eks. arkitektur, ejerskab, processer)

2.4.1.2 Onboarding af leverandører og tredjepartsaftaler

2.4.1.3 Hændelseshåndtering og efterfølgende hændelsesgennemgange

2.4.1.4 Periodiske organisatoriske risikogennemgange eller revisioner

3. Målsætninger

3.1 At etablere og operationalisere en gentagelig, organisationsdækkende proces for risikostyring baseret på metoderne i ISO/IEC 27005 og ISO 31000.

3.2 At sikre, at risici identificeres, analyseres, evalueres og behandles ved hjælp af strukturerede og sporbare metoder, herunder tildeling af risikoejerskab og kobling til kontroller.

3.3 At opretholde et centralt, versionsstyret risikoregister og en risikobehandlingsplan, som afspejler aktuel risikostatus, kontroldækning og status for afhjælpning.

3.4 At tilpasse risikobeslutninger til dokumenteret risikovillighed og toleranceniveauer samt muliggøre velinformerede ledelsesbeslutninger om risikoaccept, risikoreduktion, risikooverførsel eller risiko-undgåelse.

3.5 At overvåge risikotendenser løbende og sikre effektiviteten af risikobehandlinger, samtidig med at proaktive justeringer muliggøres på baggrund af trusselsudvikling eller forretningsmæssige ændringer.

4. Roller og ansvar

4.1 Direktion/bestyrelse

4.1.1 Godkender rammerne for risikostyring og fastlægger acceptabel risikovillighed og tærskler for risikoaccept.

4.1.2 Godkender risikobehandlingsstrategier for restrisiko, der overstiger toleranceniveauet.

4.1.3 Tildeler ressourcer og sikrer ledelsesmæssigt tilsyn med effektiv drift af risikostyringsprogrammet.

4.2 ISMS-ansvarlig/risikoansvarlig

4.2.1 Har ejerskab for denne politik og sikrer dens overensstemmelse med ISO/IEC 27001 og 27005.

4.2.2 Leder organisationens risikovurderingsproces og vedligeholder risikoregistret og behandlingsplanen.

4.2.3 Sikrer periodiske gennemgange og eskalering af væsentlige risici til direktionen eller informationssikkerhedsstyregruppen (ISSC).

[... 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 Denne politik og den tilhørende ramme skal gennemgås årligt eller:

9.1.1 Efter en væsentlig risikohændelse eller sikkerhedshændelse

9.1.2 Efter væsentlige organisatoriske eller tekniske ændringer

9.1.3 Som reaktion på revisionskonstateringer eller nye regulatoriske krav

9.2 ISMS-ansvarlig, den risikoansvarlige og compliance-funktionen er i fællesskab ansvarlige for:

9.2.1 At igangsætte gennemgangscyklussen

9.2.2 At indsamle input fra forretningsenheder

9.2.3 At revidere procedurer og tærskler efter behov

9.3 Alle revisioner skal være:

9.3.1 Versionsstyrede og registrerede

9.3.2 Godkendt af direktionen

9.3.3 Kommunikeret til interessenter

9.3.4 Opbevaret i revisionsarkivet i mindst 5 år

10. Relaterede politikker og sammenhænge

10.1 Denne politik er indbyrdes afhængig af følgende informationssikkerhedspolitikker:

10.1.1 P1 – Politik for informationssikkerhed: Fastlægger den overordnede model for sikkerhedsstyring, som denne risikopolitik er underlagt.

10.1.2 P2 – Politik for styringsroller og ansvarsområder: Definerer ansvarlige ejere og styringsniveauer, som der henvises til i risikoeskalationsmatricen.

10.1.3 P5 – P05 Ændringsstyringspolitik: Udløser fornyet risikovurdering ved ændringer i infrastruktur og organisation.

10.1.4 P13 – Politik for dataklassificering og mærkning: Understøtter konsekvensvurdering under risikoidentifikation.

10.1.5 P33 – Politik for overvågning af revision og compliance: Validerer efterlevelse af politikker, herunder fuldstændigheden af risikoregistret og dokumentation for behandlinger.

11. Referencestandarder og rammer

11.1 Denne politik er udtrykkeligt tilpasset følgende standarder og rammer for at sikre overensstemmelse med international bedste praksis og regulatoriske forventninger til informationssikkerhedsrisikostyring:

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1: Fastlægger kravene til identifikation af risici og muligheder, herunder hele livscyklussen for vurdering og behandling af informationssikkerhedsrisici. Denne politik operationaliserer klausul 6.1.2 og 6.1.3 gennem en struktureret ramme, der kræver dokumenterede procedurer for risikoidentifikation, analyse, evaluering, behandling og accept af restrisiko.

11.2.2 Klausul 8.32: Integration af risikobaseret tænkning i ændringsstyringsprocesser sikrer, at alle væsentlige organisatoriske ændringer udløser formelle fornyede risikovurderinger.

11.2.3 Klausul 10: Løbende forbedring er indarbejdet via regelmæssige politikgennemgange, trendanalyse af risici og SoA-opdateringer baseret på risikoindsigter.

11.3 ISO/IEC 27005:

11.3.1 Giver specialiseret og detaljeret vejledning om informationssikkerhedsrisikostyring. Denne politik implementerer den fulde risikoprocesmodel i ISO/IEC 27005: etablering af kontekst, risikoidentifikation, risikoanalyse, risikoevaluering, risikobehandling, risikoaccept, risikokommunikation samt risikoovervågning og gennemgang.

11.4 ISO 31000:

11.4.1 Denne politik integrerer principperne i ISO 31000, herunder ledelsesmæssig forpligtelse, integration i beslutningstagning og løbende forbedring. Den sikrer, at risikostyring er indarbejdet i organisationens kultur og drift.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Er tilpasset NIST's vejledning til gennemførelse af risikovurderinger, herunder trusselsidentifikation, sårbarhedsanalyse, estimering af sandsynlighed og fastlæggelse af konsekvens. Strukturen i denne politik afspejler NIST's definerede trin for risikovurdering og tilpasser dem til både tekniske processer og forretningsprocesser.

11.6 NIST SP 800-39:

11.6.1 Understøtter risikostyring på organisationsniveau med vægt på lagdelt risikostyring på niveauerne organisation, mission/forretningsproces og informationssystem. Politikken sikrer, at risikoejerskab er klart defineret på alle niveauer og omfatter behandlingsstrategier på organisationsniveau.

11.7 EU GDPR:

11.7.1 Artikel 24: Kræver implementering af passende tekniske og organisatoriske foranstaltninger for at sikre, at databeskyttelsesrisici håndteres korrekt — dette adresseres gennem politikkens strukturerede risikoproces.

11.7.2 Artikel 25: "Databeskyttelse gennem design og som standard" er i overensstemmelse med indarbejdelsen af risikobehandling i design af systemer og processer.

11.7.3 Artikel 32: Kræver en risikobaseret tilgang til sikkerhedsforanstaltninger — opfyldt gennem konsekvensbaserede risikoevalueringer og kontroludvælgelse.

11.8 EU NIS2-direktivet:

11.8.1 Artikel 21(2)(a–d): Kræver, at enheder gennemfører risikovurderinger, implementerer politikker for risikoanalyse og sikrer proportionale sikkerhedsforanstaltninger. Denne politik opfylder disse forpligtelser gennem løbende anvendelse af risikolivscyklussen og dokumenteret styring.

11.9 EU DORA:

11.9.1 Artikel 5: Kræver en dokumenteret ramme for IKT-risikostyring — fuldt dækket af arkitekturen i denne politik, herunder SoA-kortlægning og nøglerisikoindikatorer.

11.9.2 Artikel 6: Kræver integration af risikostyring i strategier for operationel robusthed, hvilket adresseres via eskalationsmatricer og sporing af kritiske aktiver.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: Kortlægges direkte til organisationens etablering af en struktureret tilgang til risikostyring, tildeling af roller, sporing af behandlinger og sikring af ansvarlighed på bestyrelsesniveau.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Afspejles i denne politiks fokus på trendanalyse, overvågning af nøglerisikoindikatorer og integration af revisionsfeedback i løbende forbedringssløjfer.