					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P06					Dokumenttitel: **Riskhanteringspolicy**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

I linje med standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausulerna 6.1, 8.32, 10	Kärna för riskidentifiering och riskhantering, integration i ändringshantering, kontinuerlig förbättring
ISO/IEC 27005:2024	Fullständig metodik för risklivscykeln	Fullständig riskhanteringsprocess i linje med standarden
ISO 31000:2018	Principer och ramverk för riskhantering	Principer för riskhantering antagna i ramverket
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Vägledning och struktur för riskbedömningar, nivåindelad riskstyrning
EU:s dataskyddsförordning (GDPR)	Artiklarna 24, 25, 32	Riskprocesser och kontroller för dataskydd
EU:s NIS2-direktiv	Artikel 21.2 a–d	Skyldigheter avseende risk- och säkerhetsbedömning
EU:s DORA-förordning	Artiklarna 5, 6	IKT-riskhantering och operativ motståndskraft
COBIT 2019	APO12, MEA	Struktur för riskhantering och tillsyn

1. Syfte

1.1 Denna policy fastställer ett enhetligt och formaliserat ramverk för att identifiera, analysera, utvärdera, behandla, övervaka och granska informationssäkerhetsrisker inom hela organisationen.

1.2 Den säkerställer en konsekvent tillämpning av riskbaserade principer som skyddar informationstillgångars konfidentialitet, riktighet och tillgänglighet, i linje med ISO/IEC 27001:2022 klausul 6.1 och ISO 31000:2018.

1.3 Policyn integrerar informationssäkerhetsriskhantering i organisationens beslutsprocesser för att uppfylla interna strategiska mål och externa regulatoriska krav.

2. Omfattning

2.1 Denna policy gäller för samtliga organisatoriska enheter, verksamhetsprocesser, system, all personal och tredjepartsengagemang som deltar i hantering, utveckling, lagring eller förvaltning av informationstillgångar.

2.2 Omfattningen inkluderar fysiska, digitala och molnbaserade tillgångar, inklusive strukturerade och ostrukturerade data, applikationer, infrastruktur, nätverk och tjänster.

2.3 Den omfattar informationssäkerhetsrisker på strategisk, operativ, projektmässig och teknisk nivå och är obligatorisk för alla anställda, konsulter och tredjepartsleverantörer som deltar i ISMS-aktiviteter.

2.4 Riskhantering ska tillämpas i följande scenarier:

2.4.1 Införande av nytt projekt eller nytt system

2.4.1.1 Betydande förändringar (t.ex. arkitektur, ägarskap, processer)

2.4.1.2 Leverantörsinförande och tredjepartsavtal

2.4.1.3 Incidenthantering och granskningar efter incident

2.4.1.4 Periodiska organisatoriska riskgranskningar eller revisioner

3. Mål

3.1 Att etablera och införa en repeterbar, organisationsövergripande riskhanteringsprocess baserad på metoder enligt ISO/IEC 27005 och ISO 31000.

3.2 Att säkerställa att risker identifieras, analyseras, utvärderas och behandlas med strukturerade och spårbara metoder, inklusive tilldelning av riskägarskap och koppling till kontroller.

3.3 Att upprätthålla ett centraliserat och versionshanterat riskregister och en riskbehandlingsplan som återspeglar aktuell riskstatus, kontrolltäckning och framsteg i riskreducering.

3.4 Att anpassa riskbeslut till dokumenterad riskaptit och fastställda toleransnivåer samt möjliggöra välgrundade styrningsbeslut om riskacceptans, riskreducering, risköverföring eller riskundvikande.

3.5 Att kontinuerligt övervaka risktrender och säkerställa effektiviteten i riskbehandlingar samt möjliggöra proaktiva justeringar baserat på hotutveckling eller verksamhetsförändringar.

4. Roller och ansvar

4.1 Högsta ledningen / styrelsen

4.1.1 Godkänner ramverket för riskhantering och fastställer godtagbar riskaptit och toleranströsklar.

4.1.2 Godkänner riskbehandlingsstrategier för kvarstående risker som överstiger toleransnivån.

4.1.3 Säkerställer resurser och tillsyn för ett effektivt genomförande av riskhanteringsprogrammet.

4.2 ISMS-ansvarig / riskansvarig

4.2.1 Ansvarar för denna policy och säkerställer att den är anpassad till ISO/IEC 27001 och ISO/IEC 27005.

4.2.2 Leder organisationens process för riskbedömning och förvaltar riskregistret och riskbehandlingsplanen.

4.2.3 Säkerställer periodiska granskningar och eskalering av nyckelrisker till högsta ledningen eller styrgruppen för informationssäkerhet (ISSC).

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy och tillhörande ramverk ska granskas årligen eller:

9.1.1 Efter en större riskhändelse eller säkerhetsincident

9.1.2 Efter en betydande organisatorisk eller teknisk förändring

9.1.3 Som svar på revisionsresultat eller nya regulatoriska krav

9.2 ISMS-ansvarig, riskansvarig och regelefterlevnadsfunktionen ansvarar gemensamt för att:

9.2.1 Initiera granskningscykeln

9.2.2 Samla in underlag från verksamhetsenheter

9.2.3 Revidera rutiner och tröskelvärden vid behov

9.3 Alla revideringar ska:

9.3.1 Versionshanteras och loggas

9.3.2 Godkännas av högsta ledningen

9.3.3 Kommuniceras till intressenter

9.3.4 Bevaras i revisionsarkivet i minst fem år

10. Relaterade policyer och kopplingar

10.1 Denna policy har inbördes beroenden med följande informationssäkerhetspolicyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer den övergripande styrningsmodellen för säkerhet inom vilken denna riskpolicy tillämpas.

10.1.2 P2 – Policy för styrningsroller och ansvar: Definierar ansvariga ägare och styrningsnivåer som refereras i riskeskaleringsmatrisen.

10.1.3 P5 – Ändringshanteringspolicy: Utlöser förnyad riskbedömning vid förändringar i infrastruktur och organisation.

10.1.4 P13 – Policy för dataklassificering och märkning: Stödjer konsekvensbedömning vid riskidentifiering.

10.1.5 P33 – Policy för revisions- och efterlevnadsövervakning: Verifierar policyefterlevnad, inklusive fullständighet i riskregistret och underlag för riskbehandlingar.

11. Referensstandarder och ramverk

11.1 Denna policy är uttryckligen anpassad till följande standarder och ramverk för att säkerställa att den uppfyller internationell god praxis och regulatoriska förväntningar för informationssäkerhetsriskhantering:

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1: Fastställer krav för att identifiera risker och möjligheter, inklusive hela livscykeln för bedömning och behandling av informationssäkerhetsrisker. Denna policy omsätter klausulerna 6.1.2 och 6.1.3 i praktiken genom ett strukturerat ramverk som kräver dokumenterade rutiner för riskidentifiering, analys, utvärdering, behandling och acceptans av kvarstående risk.

11.2.2 Klausul 8.32: Integrering av riskbaserat tänkande i ändringshanteringsprocesser säkerställer att alla betydande organisatoriska förändringar utlöser formella förnyade riskbedömningar.

11.2.3 Klausul 10: Kontinuerlig förbättring är inbyggd genom regelbundna policygranskningar, analys av risktrender och uppdateringar av SoA baserade på riskinsikter.

11.3 ISO/IEC 27005:

11.3.1 Ger specialiserad och detaljerad vägledning om informationssäkerhetsriskhantering. Denna policy genomför hela riskprocessmodellen enligt ISO/IEC 27005: etablering av kontext, riskidentifiering, riskanalys, riskutvärdering, riskbehandling, riskacceptans, riskkommunikation samt riskövervakning och granskning.

11.4 ISO 31000:

11.4.1 Denna policy integrerar principer enligt ISO 31000 såsom ledningens åtagande, integrering i beslutsfattande och kontinuerlig förbättring. Den säkerställer att riskhantering är inbyggd i organisationens kultur och verksamhet.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Är anpassad till NIST:s vägledning för genomförande av riskbedömningar, inklusive hotidentifiering, sårbarhetsanalys, bedömning av sannolikhet och fastställande av konsekvens. Policyns struktur speglar NIST:s definierade steg för riskbedömning och anpassar dem till både tekniska processer och verksamhetsprocesser.

11.6 NIST SP 800-39:

11.6.1 Stödjer riskstyrning på organisationsnivå och betonar nivåindelad riskhantering på organisationsnivå, uppdrags-/verksamhetsprocessnivå och informationssystemnivå. Policyn säkerställer att riskägarskap är tydligt definierat på alla nivåer och omfattar behandlingsstrategier på organisationsnivå.

11.7 EU:s dataskyddsförordning (GDPR):

11.7.1 Artikel 24: Kräver att lämpliga tekniska och organisatoriska åtgärder genomförs för att säkerställa att dataskyddsrisker hanteras på rätt sätt, vilket hanteras genom denna policys strukturerade riskprocess.

11.7.2 Artikel 25: ”Dataskydd genom inbyggt dataskydd och dataskydd som standard” är i linje med att integrera riskbehandling i utformningen av system och processer.

11.7.3 Artikel 32: Kräver ett riskbaserat angreppssätt för säkerhetsåtgärder, vilket uppfylls genom konsekvensbaserade riskutvärderingar och val av kontroller.

11.8 EU:s NIS2-direktiv:

11.8.1 Artikel 21.2 a–d: Kräver att organisationer genomför riskbedömningar, inför policyer för riskanalys och säkerställer proportionerliga säkerhetsåtgärder. Denna policy uppfyller dessa skyldigheter genom kontinuerlig tillämpning av risklivscykeln och dokumenterad styrning.

11.9 EU:s DORA-förordning:

11.9.1 Artikel 5: Kräver ett dokumenterat ramverk för IKT-riskhantering, vilket fullt ut täcks av denna policys struktur, inklusive koppling till SoA och KRI:er.

11.9.2 Artikel 6: Kräver att riskhantering integreras i strategier för operativ motståndskraft, vilket hanteras genom eskaleringsmatriser och spårning av kritiska tillgångar.

11.10 COBIT 2019:

11.10.1 APO12 – Hantera risk: Mappas direkt till organisationens införande av ett strukturerat arbetssätt för riskhantering, med tilldelning av roller, uppföljning av behandlingar och säkerställande av ansvarsskyldighet på styrelsenivå.

11.10.2 MEA01 – Övervaka, utvärdera och bedöma prestanda och efterlevnad: Återspeglas i denna policys fokus på trendanalys, övervakning av KRI:er och integrering av återkoppling från revision i arbetet med kontinuerlig förbättring.