					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P06S					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 där så är tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
EU:s NIS2-direktiv	Artikel 21.2 a–d	
EU:s DORA-förordning	Artikel 5	
COBIT 2019	APO12, MEA01	

1. Syfte

1.1 Denna policy fastställer hur organisationen identifierar, bedömer och hanterar risker relaterade till informationssäkerhet, verksamhet, teknik och tredjepartstjänster.

1.2 Den säkerställer att riskhantering utgör en aktiv del av planering, projektgenomförande, leverantörsval och incidenthantering, i enlighet med ISO 27001, ISO 31000 och tillämpliga regulatoriska krav.

1.3 Policyn stödjer välgrundade beslut, skydd av informationstillgångar och motståndskraft i kritiska verksamhetsprocesser.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Samtliga avdelningar, system och användare inom organisationen

2.1.2 All information, alla tjänster och alla tillgångar som hanteras internt eller via tredje part

2.1.3 Riskrelaterade aktiviteter, inklusive projektgranskningar, systemuppgraderingar, outsourcing och regelefterlevnad

2.2 Den omfattar alla typer av risker, såsom:

2.2.1 Cybersäkerhetshot och systemsvagheter

2.2.2 Operativa störningar och tjänsteavbrott

2.2.3 Rättsliga, regulatoriska eller anseenderelaterade exponeringar

2.2.4 Risker kopplade till tredje part och leveranskedjan

2.3 Samtliga anställda, uppdragstagare och tjänsteleverantörer ska följa denna policy vid identifiering eller rapportering av risker.

3. Mål

3.1 Integrera enkla och repeterbara riskbedömningsrutiner i den ordinarie verksamheten.

3.2 Identifiera och prioritera risker som kan påverka konfidentialitet, riktighet, tillgänglighet eller efterlevnad av rättsliga krav.

3.3 Tilldela ägarskap och fastställa riskbehandlingsåtgärder för alla väsentliga risker.

3.4 Upprätthålla ett korrekt och uppdaterat riskregister för att stödja revisionsberedskap och riskuppföljning.

3.5 Säkerställa ledningens medverkan vid godkännande av risktolerans och större riskbehandlingsplaner.

4. Roller och ansvar

4.1 Verkställande direktör

4.1.1 Fastställer organisationens riskaptit och godkänner ramverket för riskhantering.

4.1.2 Godkänner beslut om större riskbehandlingsåtgärder och tillhörande resurser.

4.1.3 Granskar de mest väsentliga riskerna kvartalsvis tillsammans med riskkoordinatorn.

4.2 Riskkoordinator (eller ägare av ledningssystemet för informationssäkerhet)

4.2.1 Samordnar riskbedömningar och upprätthåller riskregistret.

4.2.2 Säkerställer att risknivåer, ägarskap och riskbehandlingsåtgärder dokumenteras.

4.2.3 Organiserar minst en formell riskgranskning per år.

[... 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 Årlig policygranskning

9.1.1 Denna policy ska granskas minst en gång per år av verkställande direktör och riskkoordinatorn för att säkerställa relevans och fullständighet.

9.2 Utlösande faktorer för uppdatering

9.2.1 Tidigarelagd granskning och uppdatering ska ske om:

9.2.1.1 En större incident eller en revisionsiakttagelse visar på brister i riskhanteringen

9.2.1.2 Nya affärsenheter, tekniker eller partnerskap införs

9.2.1.3 Ett regulatoriskt krav eller ett avtalskrav ändras

9.3 Versionshantering

9.3.1 Alla uppdateringar av denna policy ska versionshanteras med följande metadata:

9.3.1.1 Versionsnummer och ikraftträdandedatum

9.3.1.2 Sammanfattning av ändringar

9.3.1.3 Godkännare (verkställande direktör)

9.3.1.4 Arkiverade tidigare versioner för revisionsändamål

9.4 Kommunikation och medvetenhet

9.4.1 Uppdaterade versioner av policyn och större riskbehandlingsplaner ska kommuniceras till berörd personal. Årlig utbildning i säkerhetsmedvetenhet ska omfatta grundläggande principer för riskmedvetenhet.

10. Relaterade policyer och kopplingar

10.1 Denna policy samverkar med flera andra policyer för att säkerställa en heltäckande säkerhetsstyrning:

10.1.1 P2S – Policy för styrningsroller och ansvar: Definierar vem som ansvarar för riskägarskap och beslutsfattande.

10.1.2 P5S – Ändringshanteringspolicy: Kräver riskbedömning före genomförande av tekniska eller processrelaterade förändringar.

10.1.3 P17S – Policy för dataskydd och integritet: Behandlar regulatorisk risk kopplad till behandling av personuppgifter.

10.1.4 P30S – Incidenthanteringspolicy: Säkerställer att riskbehandling fortsätter under och efter säkerhetsincidenter.

10.1.5 P33S – Policy för verksamhetskontinuitet: Identifierar kvarstående risker och återhämtningsåtgärder för kritiska tjänster.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Fastställer en formell process för riskhantering och planering av riskbehandling.

11.1.2 Klausul 6.1.3 – Kräver att organisationer bevarar dokumenterade riskbehandlingsplaner och godkännanden.

11.2 ISO/IEC 27002

11.2.1 Kontroller 5.4 och 5.25 – Ger vägledning för genomförande av riskägarskap, prioritering och livscykelhantering.

11.3 NIST SP 800-53 Rev.

11.3.1 RA-1 till RA-7 – Definierar riskbedömning, responsstrategier, dokumentation och granskningsmekanismer.

11.4 PM-9 – Kräver konsekvent styrning och tillsyn på ledningsnivå av organisationens risker.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 a–d – Ställer krav på obligatorisk riskbedömning, riskreducering och styrningsåtgärder för väsentliga och viktiga verksamhetsutövare.

11.6 EU:s DORA-förordning

11.6.1 Artikel 5 – Kräver att reglerade entiteter definierar och hanterar ramverk för IKT-riskhantering, inklusive identifiering, klassificering och respons.

11.7 COBIT 2019

11.7.1 APO12 – Hantera risker: Integrerar risker i strategisk och operativ planering.

11.7.2 MEA01 – Övervaka, utvärdera och bedöma: Säkerställer effektivitet och efterlevnad i riskprocesser och åtgärder.