					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P01					Dokumenttitel: **Informationssäkerhetspolicy**							
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**

1. Syfte

1.1 Denna policy fastställer organisationens övergripande åtagande för informationssäkerhet genom att etablera ett formellt ledningssystem för informationssäkerhet (ISMS).

1.2 Den anger den strategiska inriktningen och de grundläggande kraven för att skydda konfidentialitet, riktighet, tillgänglighet och motståndskraft hos samtliga informationstillgångar i fysiska, digitala och molnbaserade miljöer.

1.3 Policyn uppfyller ISO/IEC 27001:2022 klausul 5.2 och 5.1 genom att uttrycka ledningens avsikt, högsta ledningens åtagande och anpassningen av säkerhetsaktiviteter till organisationens mål.

1.4 Den utgör det styrande referensdokumentet för alla underordnade policyer, standarder och rutiner inom ISMS och är grundläggande för att möjliggöra en riskbaserad, efterlevnadsstyrd och kontinuerligt förbättrad säkerhetsmiljö.

2. Omfattning

2.1 Denna policy gäller för alla individer, tillgångar och processer som omfattas av ISMS, inklusive:

2.1.1 samtliga affärsenheter, avdelningar, dotterbolag och filialer

2.1.2 anställda, entreprenörer, tillfälligt anställda, konsulter och tredjepartsleverantörer

2.1.3 alla data, informationssystem, applikationer, infrastrukturer och kommunikationskanaler

2.1.4 alla fysiska, molnbaserade, fjärranslutna och hybrida miljöer där organisationens data behandlas eller nås

2.2 Policyn är bindande för alla enheter som hanterar organisationens information och gäller för samtliga steg i informationens livscykel, från skapande och överföring till lagring och bortskaffande.

2.3 Eventuella undantag eller begränsningar i denna omfattning ska dokumenteras i ISMS-omfattningsbeskrivningen och motiveras genom formellt godkännande från verkställande ledning.

3. Mål

3.1 Att etablera ett ISMS som överensstämmer med ISO/IEC 27001:2022 och som stödjer riskbaserat beslutsfattande i hela organisationen.

3.2 Att säkerställa att säkerhetsprinciperna konfidentialitet, riktighet och tillgänglighet integreras i alla organisatoriska aktiviteter, system och samarbeten.

3.3 Att möjliggöra efterlevnad av regulatoriska krav och avtalskrav genom att fastställa mätbara, policystyrda säkerhetsmål och integrera dem i verksamheten.

3.4 Att minimera sannolikheten för och konsekvenserna av informationssäkerhetsincidenter genom effektiva förebyggande, detekterande och korrigerande kontroller.

3.5 Att driva kontinuerlig förbättring av organisationens mognad inom informationssäkerhet genom definierade prestandaindikatorer, revisionsresultat och ledningens genomgångar.

3.6 Att främja en kultur av ansvarstagande, medvetenhet och motståndskraft där säkerhetsansvar förstås och fullgörs av all personal.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner och fastställer informationssäkerhetspolicyn och ISMS-ramverket.

4.1.2 Säkerställer anpassning mellan säkerhetsmål och affärsstrategi.

4.1.3 Föregår med gott exempel och främjar en stark informationssäkerhetskultur.

4.1.4 Granskar och godkänner större förändringar av ISMS-omfattning, riskbehandling och styrningsstruktur.

4.2 Informationssäkerhetschef (CISO) / ISMS-ansvarig

4.2.1 Ansvarar för ISMS och upprätthåller denna policy i enlighet med ISO/IEC 27001.

4.2.2 Leder riskbedömning, implementering av kontroller och processer för kontinuerlig förbättring.

4.2.3 Säkerställer tvärfunktionell samordning av säkerhetsarbetet och övervakar underordnade policyer.

4.2.4 Rapporterar ISMS-status, incidenter, revisionsresultat och mätetal till högsta ledningen.

4.2.5 Säkerställer att policygranskningar och uppdateringar genomförs i enlighet med avsnitt 9 i detta dokument.

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

9. Krav på granskning och uppdatering

9.1 Granskningsfrekvens

9.1.1 Denna policy ska granskas minst årligen eller vid något av följande utlösande förhållanden:

9.1.1.1 betydande förändringar av rättsliga, regulatoriska eller avtalsmässiga skyldigheter

9.1.1.2 väsentliga förändringar i organisationens riskprofil

9.1.1.3 resultat från interna eller externa revisioner

9.1.1.4 större incidenter eller kontrollbrister

9.2 Ansvar och process för granskning

9.2.1 CISO eller utsedd ISMS-ansvarig ska leda granskningsprocessen.

9.2.2 Underlag för granskningen ska omfatta:

9.2.2.1 resultat från internrevision

9.2.2.2 trender i riskbedömningar

9.2.2.3 förändringar i verksamhetsprocesser och teknik

9.2.2.4 utfall mot KPI:er och risktrösklar

9.2.3 Alla uppdateringar ska:

9.2.3.1 versionshanteras och dokumenteras

9.2.3.2 godkännas av verkställande ledning

9.2.3.3 distribueras till alla berörda parter genom officiella kommunikationskanaler

9.2.3.4 föranleda nödvändiga uppdateringar av underordnad dokumentation och utbildning

10. Relaterade policyer och kopplingar

10.1 Denna övergripande policy är direkt kopplad till följande säkerhetspolicyer och ramverk inom organisationen:

10.1.1 P2 – Policy för styrningsroller och ansvar: definierar styrningsstrukturen och den befogenhetshierarki som hänvisas till i detta dokument.

10.1.2 P3 – Policy för godtagbar användning: säkerställer beteendemässig efterlevnad och korrekt hantering av informationstillgångar.

10.1.3 P4 – Åtkomstkontrollpolicy: operationaliserar åtkomstrelaterade kontroller som följer av denna övergripande policy.

10.1.4 P6 – Riskhanteringspolicy: anger den riskbaserade kontexten för val av kontroller och acceptans av kvarstående risk.

10.1.5 P33 – Policy för övervakning, revision och regelefterlevnad: beskriver hur interna säkerställandemekanismer validerar tillämpningen av policyn.

10.2 Dessa inbördes beroenden säkerställer en heltäckande anpassning och spårbarhet inom ISMS och stödjer en sammanhållen styrning av risk och regelefterlevnad.

11. Referensstandarder och ramverk

11.1 Denna informationssäkerhetspolicy är formellt anpassad till följande standarder och ramverk för att säkerställa full efterlevnad, revisionsberedskap och regulatorisk försvarbarhet:

11.2 ISO/IEC 27001

11.2.1 Klausul 5.1 – Ledarskap och åtagande: denna policy visar högsta ledningens åtagande för informationssäkerhet och definierar ansvar och resursfördelning för ISMS.

11.2.2 Klausul 5.2 – Informationssäkerhetspolicy: detta dokument utgör organisationens formella säkerhetspolicy och är anpassat till fastställda säkerhetsmål, affärsstrategi och efterlevnad av ISO/IEC 27001.

11.2.3 Klausul 6.1 – Åtgärder för att hantera risker och möjligheter: den riskbaserade ansats som återspeglas i denna policy säkerställer att säkerhetsresurser används proportionerligt i förhållande till hot.

11.2.4 Klausul 9.2 – Intern revision och klausul 10 – Förbättring: denna policy är integrerad i organisationens livscykel för kontinuerlig förbättring och omfattas av validering genom internrevision.

11.2.5 ISO/IEC 27002:2022 – Kontroll 5.1: anger vägledning för att etablera och upprätthålla säkerhetspolicyer. Denna policy återspeglar rekommendationerna i ISO/IEC 27002 avseende hierarkisk dokumentation, granskningscykler och bindande tillämpning.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Policy och rutiner för säkerhetsplanering): denna policy uppfyller kravet på att utveckla, kommunicera och granska en formell, organisationsövergripande informationssäkerhetspolicy.

11.3.2 PM-1 till PM-5: behandlar styrning på programnivå, inklusive informationssäkerhetsroller, resursfördelning, riskstrategi och integration av säkerhetsplanering i organisationens verksamhet.

11.4 GDPR (EU) 2016/679

11.4.1 Artikel 5.2: genomför ansvarsskyldighetsprincipen. Denna policy definierar ansvariga roller och spårbara åtgärder för efterlevnad.

11.4.2 Artikel 24: kräver genomförande av tekniska och organisatoriska åtgärder, inklusive policyer anpassade till risk.

11.4.3 Artikel 32: stödjer genomförandet av lämpliga åtgärder för att säkerställa säkerheten för personuppgifter under hela deras livscykel.

11.5 NIS2-direktivet (EU) 2022/2555

11.5.1 Artikel 21.2 a: ålägger verksamheter att införa en dokumenterad säkerhetspolicy som omfattar riskhantering och styrning. Denna policy uppfyller detta krav och stödjer bredare cybersäkerhetsberedskap och skydd av kritisk infrastruktur.

11.6 DORA-förordningen (EU) 2022/2554

11.6.1 Artikel 5.2: kräver ett dokumenterat ramverk för intern kontroll för hantering av IKT-risker. Denna policy stödjer efterlevnad inom den finansiella sektorn genom att tilldela roller, kontroller och tillsynsfunktioner i linje med DORA-förordningens styrningskrav.

11.7 COBIT 2019

11.7.1 EDM01 – Etablering av styrningsramverk: denna policy stödjer bolagsstyrning genom att definiera ISMS-roller, ledningens åtaganden och strategiska mål.

11.7.2 APO01 – Ledningsramverk: stödjer etablering och drift av ett strukturerat ISMS.

11.7.3 APO12 – Riskhantering: ger grunden för styrning av informationssäkerhetsrisker.

11.7.4 MEA01/MEA03 – Mätning, utvärdering och analys: förstärker kontinuerlig utvärdering av prestanda och övervakning av intern kontroll genom säkerställd policyefterlevnad.