					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P02					Dokumenttitel: **Policy för styrningsroller och ansvar**							
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 regleringar

Standard/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3; bilaga A kontroll 5	
ISO/IEC 27002:2022	Kontroll 5	
NIST SP 800-53 Rev. 5	PL-1 till PL-4, PM-1 till PM-13	
EU:s GDPR	Artiklarna 5.1 f, 24, 37	
EU:s NIS2-direktiv	Artikel 21.2 a	
EU:s DORA-förordning	Artikel 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Syfte

1.1 Denna policy definierar den styrningsmodell samt de organisatoriska roller och ansvar som krävs för att upprätthålla ett effektivt ledningssystem för informationssäkerhet (ISMS).

1.2 Den fastställer tydliga ansvarslinjer, beslutsmandat och eskaleringsvägar för att säkerställa att informationssäkerhet integreras på alla nivåer i organisationen och är anpassad till verksamhetens strategiska mål.

1.3 Policyn genomför kraven i ISO/IEC 27001:2022 klausul 5.3 och kontroll A.5.2 samt säkerställer att ansvar för säkerhetsrelaterade aktiviteter tilldelas tydligt, dokumenteras, kommuniceras och granskas periodiskt.

1.4 Denna policy utgör även en grund för integrerad styrning med andra områden såsom riskhantering, regelefterlevnad, IT-drift och juridik.

2. Omfattning

2.1 Denna policy gäller för alla individer och enheter som deltar i styrning, drift och uppföljning av informationssäkerhet inom ISMS omfattning. Detta omfattar:

2.1.1 Högsta ledningen, den operativa ledningen och styrelseledamöter

2.1.2 ISMS-ansvariga, informationssäkerhetschef (CISO) och kontrollägare

2.1.3 Processägare och tillgångsägare

2.1.4 Entreprenörer och tredjepartsleverantörer med delegerat säkerhetsansvar

2.2 Den omfattar både interna och externt tillhandahållna funktioner (t.ex. outsourcad SOC och administratörer av molnplattformar) där styrningsroller är formellt tilldelade eller avtalsreglerade.

2.3 Policyn gäller även organisatoriska enheter, avdelningar och projektteam som hanterar eller påverkar säkerhetsrelevanta tillgångar, system eller tjänster.

3. Mål

3.1 Att säkerställa att roller och ansvar inom informationssäkerhet är formellt definierade, tilldelade, kommunicerade och dokumenterade.

3.2 Att upprätthålla en styrningsmodell som säkerställer funktionsuppdelning, motverkar intressekonflikter och möjliggör eskalering av olösta säkerhetsfrågor.

3.3 Att säkerställa att ansvarsskyldighet och mandat för säkerhetsbeslut fördelas i linje med verksamhetspåverkan och organisationsstruktur.

3.4 Att etablera ett ramverk för hantering av delegering, rolländringar och granskning av tilldelat ansvar.

3.5 Att ge intressenter, inklusive tillsynsmyndigheter, revisorer och kunder, tillräcklig säkerhet för att informationssäkerheten styrs effektivt och i enlighet med tillämpliga standarder.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Tillhandahåller strategisk styrning, fördelar resurser och säkerställer samordning mellan ISMS mål och verksamhetsmål.

4.1.2 Godkänner central ISMS-dokumentation, inklusive informationssäkerhetspolicyn, riskbehandlingsplaner och beslut om revisionsåtgärder.

4.1.3 Deltar i ledningens genomgång av ISMS och eskalerar beslut som kräver godkännande på styrelsenivå.

4.1.4 Främjar en säkerhetskultur och verkar för att organisationen följer principer för säkerhetsstyrning.

4.2 Styrgrupp för informationssäkerhet (ISSC)

4.2.1 Utgör det tvärfunktionella styrningsorganet för övervakning av ISMS.

4.2.2 Granskar riskläge, kontrollernas effektivitet, revisionsiakttagelser och strategiska säkerhetsinitiativ.

4.2.3 Säkerställer samordning mellan avdelningar (t.ex. IT, juridik, HR, risk, regelefterlevnad och drift).

4.2.4 Godkänner eskaleringströsklar, budgettilldelning och policyändringar som kräver underlag från verkställande ledning.

[... 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 Granskningsschema

9.1.1 Denna policy ska granskas minst årligen eller när något av följande inträffar:

9.1.1.1 Förändringar i organisationsstrukturen eller den verkställande ledningen

9.1.1.2 Utvidgning eller omdefiniering av ISMS omfattning

9.1.1.3 Regulatoriska förändringar som påverkar rolltilldelning eller övervakning

9.1.1.4 Betydande revisionsiakttagelser eller incidenter som involverar bristande styrning

9.2 Process för granskning och godkännande

9.2.1 ISMS-ansvarig ska initiera och leda granskningsprocessen, inklusive inhämtning av synpunkter från intressenter och återkoppling från revision.

9.2.2 Föreslagna uppdateringar ska granskas av ISSC och formellt godkännas av verkställande ledning.

9.2.3 Varje version ska följas upp i ISMS-dokumentregistret och innehålla följande metadata:

9.2.3.1 Policy-ID och titel

9.2.3.2 Versionsnummer och ändringssammanfattning

9.2.3.3 Ikraftträdandedatum och nästa granskningsdatum

9.2.3.4 Policyägare och godkännare

9.2.3.5 Dokumentets klassificeringsnivå

9.2.3.6 Historik för bevarande och arkivering

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tolkas tillsammans med följande policyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer det övergripande säkerhetsprogrammet och beskriver ledningens ansvar för godkännande av policyer och strategisk styrning.

10.1.2 P5 – Policy för ändringshantering: Säkerställer att förändringar i styrningsstrukturer, roller eller ansvar omfattas av dokumenterat godkännande och riskgranskning.

10.1.3 P6 – Riskhanteringspolicy: Identifierar och hanterar styrningsrisker som uppstår till följd av rollkonflikter, otilldelade uppgifter eller utebliven eskalering.

10.1.4 P7 – Policy för introduktion och avslut: Säkerställer processer för kontrolltilldelning och återkallelse vid förändringar i personalens livscykel.

10.1.5 P33 – Policy för övervakning av revision och regelefterlevnad: Stödjer oberoende granskning av styrningens effektivitet och säkerställer korrigerande åtgärder vid bristande efterlevnad.

10.2 Dessa policyer stöder tillsammans ett enhetligt och bindande ramverk för ISMS-styrning.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till globalt erkända standarder och ramverk för styrning av informationssäkerhet och ansvarsskyldighet för roller. Den säkerställer spårbarhet mot regulatoriska krav och certifieringskrav samt stöder en robust ISMS-struktur.

11.2 ISO/IEC 27001

11.2.1 Klausul 5.3 – organisatoriska roller, ansvar och befogenheter: Denna policy uppfyller kravet att roller som är relevanta för informationssäkerhet ska vara tydligt tilldelade, kommunicerade och dokumenterade.

11.2.2 Klausul 9.3 – ledningens genomgång: Denna policy säkerställer ledningens övervakning av ISMS-roller och styrning genom kvartalsvisa och årliga granskningar.

11.2.3 Bilaga A kontroll 5.2 – roller och ansvar inom informationssäkerhet: Definierar roller på teknisk, operativ och strategisk nivå för att säkerställa funktionsuppdelning, riskägarskap och spårbar ansvarsskyldighet.

11.3 ISO/IEC 27002:2022 – kontroll 5

11.3.1 Ger vägledning för genomförande av tilldelning av ansvar för informationssäkerhet i en organisation. Denna policy tillämpar denna vägledning genom att definiera rolltyper, regler för delegering, eskaleringsprocedurer och granskningsmekanismer.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1 till PL-4: Betonar behovet av formell planeringsdokumentation, inklusive policyer som definierar styrning och tilldelar säkerhetsansvar.

11.4.2 PM-1 (plan för informationssäkerhetsprogram) och PM-2 (senior informationssäkerhetsansvarig): Återspeglas i denna policy genom tilldelningen av CISO/ISMS-ansvarig och formella styrningsroller.

11.4.3 PM-5 till PM-13: Denna policy uppfyller krav på rolldokumentation, verksamhetsövergripande riskroller, övervakning av konfigurationshantering och integration med verksamhetsfunktioner.

11.5 EU:s GDPR (2016/679)

11.5.1 Artikel 5.1 f: Kräver att personuppgifter skyddas mot obehörig eller olaglig behandling. Denna policy säkerställer att personer med ansvar för dataskydd är tydligt utsedda och följs upp.

11.5.2 Artikel 24: Kräver lämpliga organisatoriska åtgärder, inklusive styrningsstrukturer.

11.5.3 Artikel 37: Kräver att ett dataskyddsombud (DPO) utses, vilket ska återspeglas i organisationens styrningsramverk och ansvarregister.

11.6 EU:s NIS2-direktiv (2022/2555)

11.6.1 Artikel 21.2 a: Kräver att entiteter inför policyer för riskanalys och säkerhet i informationssystem, inklusive rollspecifikt ansvar. Denna policy definierar sådana roller och deras styrningsmekanismer.

11.7 EU:s DORA-förordning (2022/2554)

11.7.1 Artikel 5 – styrning och ramverk för intern kontroll: Kräver formell tilldelning av ansvar för hantering av IKT-risker, beslutsroller och rapporteringskanaler. Denna policy utgör grunden för styrning av säkerhetsrelaterade roller i IKT-miljöer.

11.8 COBIT 2019

11.8.1 EDM01 – etablerat ramverk för styrning: Denna policy säkerställer att ISMS har en tydligt definierad styrningsstruktur anpassad till verksamhetens behov.

11.8.2 EDM02 – säkerställd nyttorealisering: Anpassar säkerhetsaktiviteter baserade på roller till strategiska och operativa mål och säkerställer ansvarsskyldighet samt mätbara utfall.

11.8.3 APO01 – hanterat ramverk för styrning av information och teknik och APO12 – hanterad risk: Denna policy stödjer strukturerad hantering av roller inom informationssäkerhet inom ett bredare ramverk för IT-styrning och riskhantering.

11.8.4 MEA01 – övervaka, utvärdera och bedöma prestanda: Inför granskningsmekanismer för att verifiera att styrningsroller är effektiva, aktuella och tillämpas.