					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P02S					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 regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	
ISO/IEC 27002:2022	Kontroller: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EU:s GDPR	Artiklar 5.2, 32	

1. Syfte

1.1 Denna policy fastställer hur ansvar för styrning av informationssäkerhet ska tilldelas, delegeras och hanteras inom organisationen för att säkerställa efterlevnad av ISO/IEC 27001:2022 och andra tillämpliga regulatoriska krav.

1.2 Policyn säkerställer ansvarsskyldighet på alla nivåer och stödjer operativ effektivitet genom att tydliggöra vem som ansvarar för respektive säkerhetsrelaterad funktion.

1.3 Denna policy stärker revisionsberedskapen och bygger kundförtroende genom att påvisa formell säkerhetsstyrning, även i organisationer med begränsade tekniska resurser eller outsourcad IT.

2. Omfattning

2.1 Denna policy gäller för alla personer som hanterar organisationens informationssystem eller data, inklusive:

2.1.1 verksamhetsansvariga och verkställande ledning

2.1.2 anställda och uppdragstagare

2.1.3 externa IT-tjänsteleverantörer och konsulter

2.2 Den omfattar alla system, miljöer och tjänster som används för att behandla, överföra eller lagra verksamhetsinformation eller kundinformation, inklusive:

2.2.1 kontors-IT-infrastruktur och utrustning för distansarbete

2.2.2 molnbaserade plattformar och e-posttjänster

2.2.3 fysiska register och delade lagringsenheter

2.3 Omfattningen inkluderar både interna och outsourcade aktiviteter som avser styrning av informationssäkerhet.

3. Mål

3.1 Fastställa tydlig ansvarsskyldighet för alla säkerhetsrelaterade uppgifter, inklusive policyhantering, åtkomstkontroll, incidenthanteringsprocesser och övervakning.

3.2 Möjliggöra effektiv funktionsuppdelning för att minska risken för intressekonflikter eller bedrägeri.

3.3 Säkerställa att säkerhetsuppgifter och roller dokumenteras tydligt och granskas regelbundet.

3.4 Möjliggöra välgrundat beslutsfattande, eskalering och tillsyn av IT- och säkerhetsrisker.

3.5 Stödja certifiering enligt ISO/IEC 27001:2022 och bygga förtroende hos kunder, partner och revisorer.

4. Roller och ansvar

4.1 Verkställande chef/verksamhetsansvarig

4.1.1 Har det övergripande ansvaret för införande och tillsyn av denna policy.

4.1.2 Godkänner samtliga säkerhetsroller, ansvarsområden och delegeringsbeslut.

4.1.3 Övervakar efterlevnaden och fattar slutliga beslut om policyundantag och eskaleringar.

4.2 Utsedd säkerhetssamordnare (om tillämpligt)

4.2.1 Kan vara en intern medarbetare eller en betrodd konsult.

4.2.2 Rollen kan innehas av den verkställande chefen eller en extern leverantör i mikroföretag.

4.2.3 Stödjer den dagliga tillämpningen av åtkomstkontroll, incidenthantering och grundläggande tekniska säkerhetsuppgifter.

4.2.4 Rapporterar direkt till den verkställande chefen om säkerhetsfrågor och risker.

[... 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 granskning

9.1.1 Denna policy ska granskas av den verkställande chefen var tolfte månad för att säkerställa att den fortsatt återspeglar rättsliga skyldigheter, operativa behov och krav för certifiering enligt ISO/IEC 27001.

9.2 Granskning utanför ordinarie cykel

9.2.1 Granskning ska även genomföras när:

9.2.1.1 större organisatoriska förändringar inträffar

9.2.1.2 en ny leverantör onboardas

9.2.1.3 en allvarlig säkerhetsincident inträffar

9.2.1.4 regelverk såsom GDPR, NIS2 eller DORA uppdateras

9.3 Versionshantering och dokumentation

9.3.1 Alla granskningar ska omfatta:

9.3.1.1 datum för granskning

9.3.1.2 sammanfattning av eventuella ändringar

9.3.1.3 signatur eller dokumenterat godkännande av den verkställande chefen

9.3.1.4 arkiverade tidigare versioner som revisionsunderlag

9.4 Kommunikation av ändringar

9.4.1 Samtliga policyuppdateringar ska utan dröjsmål kommuniceras till medarbetare och leverantörer via e-post, interna portaler eller formella meddelanden.

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med följande SME-policyer för full effekt:

10.1.1 P4S – Policy för åtkomstkontroll: Definierar hur åtkomst beviljas, hanteras och återkallas, direkt kopplat till tilldelade roller och tillsyn.

10.1.2 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Förstärker rollspecifika ansvar och förväntningar.

10.1.3 P17S – Policy för dataskydd och integritet: Beskriver rättsliga skyldigheter enligt GDPR, vilka tilldelas roller som definieras i denna styrningspolicy.

10.1.4 P30S – Policy för incidenthantering: Kräver definierade ansvarsområden för rapportering, eskalering och hantering av incidenter.

10.2 Tillsammans möjliggör dessa policyer en enhetlig tillämpning, internt ansvarstagande och extern regelefterlevnad.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3 – organisatoriska roller, ansvar och befogenheter: Kräver att roller tilldelas tydligt och stöds av högsta ledningen.

11.2 ISO/IEC 27002

11.2.1 Kontroller 5.2–5.4: Kräver tydlig dokumentation av roller inom informationssäkerhet, funktionsuppdelning och ledningens tillsyn.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Etablerar ett övergripande program för informationssäkerhet med definierade ansvarsområden.

11.3.2 PL-1 till PL-4: Kräver planeringsåtgärder, inklusive policyutformning och dokumenterade rolltilldelningar.

11.3.3 CA-1: Kräver definierade roller för bedömning och auktorisation.

11.3.4 AC-1: Kopplar rollbaserad åtkomstkontroll till tilldelade styrningsansvar.

11.4 EU:s GDPR

11.4.1 Artikel 5.2 – ansvarsskyldighet: Kräver att organisationer kan visa efterlevnad genom roller och ansvar.

11.4.2 Artikel 32 – säkerhet i behandlingen: Betonar tydlig tilldelning av uppgifter för att skydda personuppgifter.

11.5 EU:s NIS-direktiv

11.5.1 Artikel 21.2 a: Kräver styrningsstrukturer som omfattar formaliserade roller för hantering av cyberrisker och incidenter.

11.6 EU:s DORA-förordning

11.6.1 Artiklarna 9 och 10: Kräver att finansiella entiteter tydligt tilldelar och utövar tillsyn över IKT- och säkerhetsrelaterade ansvarsområden.

11.7 COBIT 2019

11.7.1 EDM03 – Säkerställ riskoptimering: Kräver väl definierade roller och eskaleringsvägar för hantering av säkerhetsrisker.

11.7.2 APO13 – Hantera säkerhet: Tilldelar strategiska och operativa säkerhetsuppgifter till individer och roller.

11.7.3 DSS05 – Hantera säkerhetstjänster: Kräver struktur och spårbarhet i ansvarsområden för externa och interna säkerhetstjänster.