					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P01S					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**

Anpassad till standarder och regelverk

Standard/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 5.2, 5.3, 6.1, 6.2, 8	Anger ledningens åtagande, policykrav, rolltilldelning, riskbedömning och operativ styrning
ISO/IEC 27002:2022	Kontroller 5.1–5.5	Anger krav på dokumenterade informationssäkerhetspolicyer, tilldelning av roller, funktionsuppdelning och ledningens ansvar
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Krav på säkerhetsprogramplan, policy för säkerhetsplanering, bedömning och auktorisering samt åtkomstkontroll
EU:s dataskyddsförordning (GDPR) (2016/679)	Artikel 5.2, artikel 32	Ansvarsskyldighetsprincipen och säkerhetsåtgärder för behandling, särskilt avseende dokumenterade roller
NIS2-direktivet (EU 2022/2555)	Artikel 21.2 a	Kräver riskhanteringsåtgärder samt roller och ansvar för cyberrisker
DORA-förordningen (EU 2022/2554)	Artikel 9, artikel 10	Kräver tilldelning av roller för IKT-riskhantering och verksamhetskontinuitet
COBIT 2019	EDM03, APO13, DSS05	Säkerställer riskoptimering, säkerhetsstyrning och hantering av säkerhetstjänster genom tydlig rolltilldelning

1. Syfte

1.1 Denna policy fastställer organisationens åtagande att skydda kund- och verksamhetsinformation genom att tydligt definiera ansvar och praktiska säkerhetsåtgärder, anpassade för organisationer utan dedikerade IT-team.

1.2 Den säkerställer att alla anställda, entreprenörer och tjänsteleverantörer följer bindande krav, vilket möjliggör full efterlevnad av kraven för ISO/IEC 27001-certifiering.

1.3 Denna policy gör det möjligt för organisationen att bygga kundförtroende genom att tydligt visa hur information skyddas genom definierat ansvar, strukturerade processer och tydlig ansvarsskyldighet.

2. Omfattning

2.1 Denna policy gäller för alla personer som har åtkomst till eller hanterar organisationens information och system, inklusive:

2.1.1 verksamhetsägare och verkställande chef

2.1.2 anställda, entreprenörer och praktikanter

2.1.3 externa IT-tjänsteleverantörer eller konsulter

2.2 Den omfattar alla typer av information, system och tjänster, inklusive:

2.2.1 verksamhetsdokumentation, kunduppgifter, lösenord och e-post

2.2.2 IT-utrustning såsom bärbara datorer och telefoner

2.2.3 molntjänster som används för fillagring, kommunikation eller ekonomi

2.2.4 fysiska dokument som förvaras i kontorslokaler

2.3 Policyn gäller i alla arbetsmiljöer – på kontoret, på distans och i molnmiljöer – och omfattar alla enheter och all programvara som används för att behandla eller lagra verksamhetsinformation.

3. Mål

3.1 Tydlig ansvarstilldelning: Säkerställa att det alltid finns en utsedd ansvarig för informationssäkerheten. Vanligtvis är detta den verkställande chefen eller den person som denne formellt utser.

3.2 Skydd av kund- och verksamhetsinformation: Tillhandahålla tillförlitliga och konsekventa skyddsåtgärder för att förhindra missbruk, förlust eller stöld av känsliga uppgifter, inklusive kunduppgifter och finansiella register.

3.3 Stöd för ISO/IEC 27001-certifiering: Göra det möjligt för organisationen att visa full efterlevnad av kraven i ISO/IEC 27001, med revisionsberedskap och möjlighet till certifiering utan att komplex infrastruktur krävs.

3.4 Integrera säkerhet i verksamheten: Integrera informationssäkerhet i dagliga arbetsuppgifter och beslut i hela organisationen.

3.5 Stärka säkerhetsmedvetande och säkerhetskultur: Säkerställa att varje anställd förstår och upprätthåller säkra arbetssätt, såsom att använda starka lösenord och rapportera misstänkt aktivitet.

4. Roller och ansvar

4.1 Verkställande chef eller verksamhetsägare

4.1.1 Har det övergripande ansvaret för informationssäkerheten.

4.1.2 Godkänner och förvaltar denna policy.

4.1.3 Säkerställer att alla centrala säkerhetsuppgifter antingen hanteras direkt eller delegeras skriftligen.

4.1.4 Verifierar att delegerade säkerhetsuppgifter, såsom åtkomsthantering eller incidenthantering, utförs effektivt.

4.1.5 Är primär kontaktpunkt för alla interna och externa säkerhetsfrågor, inklusive revisioner och kundförfrågningar.

4.1.6 Följer upp framstegen mot dessa mål inom ramen för den årliga granskningen. Mål ska vara mätbara där det är möjligt, till exempel andel utbildad personal och antal rapporterade incidenter, och ska revideras utifrån säkerhetsrelaterade iakttagelser och förändringar i riskbilden.

4.2 Utsedd medarbetare (om tillämpligt)

4.2.1 Får bistå den verkställande chefen genom att hantera löpande uppgifter, såsom att skapa användarkonton, ta bort åtkomst för personer som lämnar organisationen eller samordna med IT-leverantören.

4.2.2 Ska vara formellt utsedd och ha tillräckliga befogenheter och verktyg för att utföra uppgifterna.

4.2.3 Rapporterar eventuella frågor eller problem till den verkställande chefen.

[... 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 Årlig granskning

9.1.1 Denna policy ska granskas av den verkställande chefen (GM) minst en gång per år för att säkerställa fortsatt efterlevnad av kraven för ISO/IEC 27001-certifiering, förändringar i regulatoriska krav, såsom EU:s dataskyddsförordning (GDPR), NIS2-direktivet och DORA-förordningen, samt förändrade verksamhetsbehov.

9.2 Löpande granskningar

9.2.1 Ytterligare granskningar ska genomföras när betydande förändringar inträffar, såsom:

9.2.1.1 större säkerhetsincidenter eller överträdelser

9.2.1.2 införande av nya verksamhetsprocesser eller tekniker, till exempel ny programvara, plattformar för distansarbete eller molntjänster

9.2.1.3 ändringar i rättsliga eller regulatoriska krav som påverkar informationshanteringen

9.3 Dokumentation av ändringar

9.3.1 Alla policygranskningar och ändringar ska dokumenteras formellt med tydlig angivelse av datum, typ av revidering och GM:s godkännande.

9.3.2 Ett historiskt register över policyversioner ska bevaras säkert för att visa policyutveckling och efterlevnad vid revisioner.

9.4 Kommunikation av uppdateringar

9.4.1 Alla ändringar i denna policy ska skyndsamt kommuniceras till alla anställda, entreprenörer och relevanta tredje parter.

9.4.2 Uppdaterade versioner av policyn ska vara lätt tillgängliga för all berörd personal, till exempel genom elektronisk delning eller fysisk anslagning på arbetsplatsen.

10. Relaterade policyer och kopplingar

10.1 Denna policy samverkar nära med andra policyer i organisationens SME-policyramverk, särskilt:

10.1.1 P2S – Policy för styrningsroller och ansvar: Förtydligar tilldelning av säkerhetsuppgifter och ansvar.

10.1.2 P4S – Policy för åtkomstkontroll: Definierar säker hantering av åtkomst till organisationens information.

10.1.3 P8S – Policy för informationssäkerhetsmedvetande och utbildning: Ger grundläggande vägledning för personalens utbildning och medvetande.

10.1.4 P17S – Policy för dataskydd och integritet: Säkerställer efterlevnad av GDPR och andra dataskyddslagar.

10.1.5 P30S – Policy för incidenthantering: Beskriver detaljerade åtgärder som krävs vid säkerhetsincidenter.

10.2 Dessa relaterade policyer ger tydlig operativ vägledning och ska implementeras samordnat för att uppnå full efterlevnad av kraven för ISO/IEC 27001-certifiering.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.1 – Ledarskap och åtagande: Kräver att högsta ledningen visar åtagande och ansvar för informationssäkerhetens effektivitet inom organisationen.

11.1.2 Klausul 5.2 – Informationssäkerhetspolicy: Kräver tydliga, dokumenterade policyer i linje med organisationens strategi och efterlevnadskrav.

11.1.3 Klausul 5.3 – Roller, ansvar och befogenheter i organisationen: Definierar tydlig tilldelning av ansvar för informationssäkerhet i hela organisationen, vilket är grundläggande för effektiv styrning och efterlevnad vid revision.

11.1.4 Klausul 6.1 – Åtgärder för att hantera risker och möjligheter: Säkerställer att informationssäkerhetsrisker identifieras, bedöms och behandlas systematiskt.

11.1.5 Klausul 8.1 – Operativ planering och styrning: Kräver att organisationen planerar och genomför de processer som behövs för att uppnå informationssäkerhetsmålen och effektivt hantera tillhörande risker.

11.2 ISO/IEC 27002:2022 kontroller 5.1–5.5

11.2.1 Bilaga A kontroll 5.1 – Policyer för informationssäkerhet: Anger upprättande och kommunikation av dokumenterade informationssäkerhetspolicyer.

11.2.2 Bilaga A kontroll 5.2 – Roller och ansvar inom informationssäkerhet: Förtydligar och tilldelar formellt roller och ansvar inom informationssäkerhet till relevanta parter.

11.2.3 Bilaga A kontroll 5.3 – Funktionsuppdelning: Kräver tydlig uppdelning av arbetsuppgifter för att minska intressekonflikter och bedrägeririsker vid hantering av känslig information.

11.2.4 Bilaga A kontroll 5.4 – Ledningens ansvar: Kräver att ledningen visar åtagande för informationssäkerhet genom aktiv uppföljning och resursallokering.

11.2.5 Bilaga A kontroll 5.5 – Kontakt med myndigheter: Förstärker behovet av tydliga styrningsstrukturer och definierade kontaktvägar inom informationssäkerhetsarbetet.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan för informationssäkerhetsprogram: Kräver dokumenterade strategier och policyer för informationssäkerhetsstyrning och ger ett ramverk för konsekvent genomförande och hantering.

11.3.2 PL-1 – Policy för säkerhetsplanering: Kräver en organisationsövergripande policy för säkerhetsplanering för att styra säker drift och strategisk anpassning av informationssäkerhetsaktiviteter.

11.3.3 CA-1 – Policy för säkerhetsbedömning och auktorisering: Kräver tydligt definierade roller för bedömning och auktorisering för att säkerställa fortlöpande effektivitet och efterlevnad av informationssäkerhetskrav.

11.3.4 AC-1 – Policy för åtkomstkontroll: Kräver att organisationer tydligt definierar, dokumenterar och tillämpar arbetssätt och ansvar för åtkomsthantering.

11.4 EU:s dataskyddsförordning (GDPR) (2016/679)

11.4.1 Artikel 5.2 – Ansvarsskyldighetsprincipen: Kräver att organisationer kan visa efterlevnad av dataskyddsprinciperna, inklusive dokumenterade roller och policyer för dataskyddsansvar.

11.4.2 Artikel 32 – Säkerhet i behandlingen: Kräver genomförande av lämpliga tekniska och organisatoriska åtgärder, inklusive tydliga säkerhetsansvar, för att skydda personuppgifter mot incidenter och obehörig åtkomst.

11.5 NIS2-direktivet (EU 2022/2555)

11.5.1 Artikel 21.2 a – Riskhanteringsåtgärder: Kräver tydliga styrningsarrangemang, inklusive definierade roller och ansvar för informationssäkerhet, vilket är nödvändigt för att effektivt hantera cyberrisker.

11.6 DORA-förordningen (EU 2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Kräver att organisationer tydligt tilldelar roller och ansvar kopplade till IKT-riskhantering, vilket stärker motståndskraft och beredskap för verksamhetskontinuitet.

11.6.2 Artikel 10 – IKT-verksamhetskontinuitet: Kräver tydlig ansvarstilldelning och strukturerade roller för att upprätthålla IKT-motståndskraft och kontinuitet samt säkerställa att organisationer på ett tillförlitligt sätt kan hantera störningar.

11.7 COBIT 2019

11.7.1 EDM03 – Säkerställ riskoptimering: Betonar tydligt definierat ansvar och roller vid hantering av organisatoriska risker, vilket ger stark styrning och effektiv uppföljning av informationssäkerhetsrisker.

11.7.2 APO13 – Hantera säkerhet: Kräver att organisationer tydligt etablerar och kommunicerar ansvar för säkerhetsstyrning samt säkerställer anpassning till verksamhetsmål och regulatoriska krav.

11.7.3 DSS05 – Hantera säkerhetstjänster: Kräver strukturerade roller och tydligt ansvar för hantering av säkerhetstjänster, vilket möjliggör konsekvent genomförande och verifiering av efterlevnad.