					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P17					Dokumenttitel: **Policy för dataskydd och integritet**							
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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausulerna 5.1, 6.1.3, 8.1, 10	Relevanta övergripande, tekniska och kontinuerliga förbättrings- och dataskyddskontroller
ISO/IEC 27002:2022	Kontrollerna 5.34, 8.10, 8.11, 8.12	Kontroller för hantering av PII, bevarande, radering, anonymisering och den registrerades rättigheter
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Krav avseende styrning, riskhantering, åtkomststyrning, loggning, hantering av personuppgiftsincidenter och integritetsprogram
EU:s GDPR	Artiklarna 5, 6, 12–23, 25, 28, 30, 32–34; skäl 78	Samtliga centrala krav avseende integritet, ansvarsskyldighet, den registrerades rättigheter, registrerades begäranden, personuppgiftsincidenter samt principerna om inbyggt dataskydd och dataskydd som standard
EU:s NIS2-direktiv	Artikel 21.2 e och f	Riskbaserade säkerhetskontroller för väsentliga och viktiga entiteter
EU:s DORA-förordning	Artiklarna 6.2 d, 11.1 c, 15.1, 17	Styrning, tredjepartsrisker och tidskrav för säker behandling
COBIT 2019	APO12, DSS01, DSS05, MEA	Riskhantering, säker drift och övervakning av regelefterlevnad

1. Syfte

1.1 Denna policy fastställer obligatoriska organisatoriska principer och tekniska krav för skydd av personuppgifter samt införande av inbyggt dataskydd i samtliga miljöer.

1.2 Den formaliserar organisationens ansvar enligt internationella standarder och regulatoriska ramverk samt säkerställer att personuppgifter samlas in, behandlas, bevaras, delas och avvecklas lagenligt, säkert och transparent.

1.3 Denna policy stärker även efterlevnaden av tillämplig dataskyddslagstiftning och relevanta ramverk, inklusive EU:s allmänna dataskyddsförordning (GDPR), EU:s NIS2-direktiv, EU:s DORA-förordning, ISO/IEC 27001:2022 och COBIT 2019.

2. Omfattning

2.1 Denna policy gäller för samtliga organisatoriska enheter, all personal och alla system som deltar i behandling av personuppgifter, inklusive:

2.1.1 anställda, uppdragstagare, konsulter och tredjepartsleverantörer.

2.1.2 data som samlas in från interna och externa källor inom samtliga verksamhetsfunktioner.

2.1.3 fysiska och digitala medier, inklusive molntjänster, SaaS-plattformar, mobila enheter och pappersbaserade uppgifter.

2.1.4 samtliga miljöer, inklusive produktion, utveckling, test och säkerhetskopieringssystem där personuppgifter kan förekomma.

2.2 Policyn omfattar samtliga behandlingsaktiviteter som regleras enligt tillämplig dataskyddslagstiftning och relevanta standarder, inklusive men inte begränsat till:

2.2.1 insamling, lagring, användning, överföring och avveckling av personuppgifter.

2.2.2 tillämpning av den registrerades rättigheter, dokumentation av rättslig grund och hantering av samtycke.

2.2.3 gränsöverskridande överföringar, anmälan av personuppgiftsincidenter och delning av data med tredje part.

2.2.4 säker utformning och tillämpning av dataskydd som standard i system och processer.

3. Mål

3.1 Säkerställa lagenlig, transparent och ansvarsskyldig behandling av personuppgifter i linje med ISO/IEC 27001:2022 och tillhörande rättsliga krav.

3.2 Integrera principerna om inbyggt dataskydd och dataskydd som standard i samtliga informationssystem, tjänster och verksamhetsprocesser.

3.3 Tillämpa tekniska och organisatoriska åtgärder (TOM) som skyddar personuppgifters konfidentialitet, riktighet och tillgänglighet under hela deras livscykel.

3.4 Definiera styrningsroller och ansvarstrukturer för dataskydd, inklusive ansvar för dataskyddsombud (DPO), informationssäkerhet, juridik och dataägare.

3.5 Möjliggöra full efterlevnad av artiklarna 5, 6, 25, 30 och 32 i GDPR samt krav på riskreducering och motståndskraft enligt NIS2 och DORA.

3.6 Upprätthålla den registrerades rättigheter, inklusive tillgång, rättelse, radering, begränsning, dataportabilitet, invändning och skydd mot automatiserat beslutsfattande.

3.7 Minska regulatoriska, anseendemässiga, rättsliga och operativa risker som uppstår till följd av obehörig åtkomst, felaktig användning eller förlust av personuppgifter.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Tillhandahåller strategisk styrning och avsätter tillräckliga resurser för att stödja organisationens integritetsprogram.

4.1.2 Godkänner denna policy och säkerställer att den tillämpas i hela organisationen.

4.2 Dataskyddsombud (DPO)

4.2.1 Agerar självständigt för att övervaka efterlevnaden av dataskyddsregler.

4.2.2 Upprätthåller registret över behandlingsaktiviteter (RoPA) enligt artikel 30 i GDPR.

4.2.3 Leder kontakten med tillsynsmyndigheter, genomför konsekvensbedömningar avseende dataskydd (DPIA) och hanterar processer för anmälan av personuppgiftsincidenter.

4.2.4 Granskar undantag inom dataskydd och upprätthåller registret över integritetsundantag.

[... 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 Denna policy ska granskas minst årligen eller tidigare vid följande förutsättningar:

9.1.1 väsentliga rättsliga eller regulatoriska uppdateringar (t.ex. ändringar i GDPR eller tidsfrister enligt DORA)

9.1.2 nya system eller behandlingsaktiviteter som omfattar personuppgifter

9.1.3 revisionsiakttagelser från internrevision som visar på brister i policyn

9.1.4 väsentliga personuppgiftsincidenter eller återkoppling från tillsynsmyndighet

9.2 Ansvar för granskning

9.2.1 DPO ska initiera policygranskningen och samordna med juridik, risk, informationssäkerhet och verkställande ledning.

9.2.2 Alla uppdateringar ska registreras i ISMS-registret för dokumentstyrning och distribueras till berörda intressenter.

9.3 Ändringsstyrning

9.3.1 Varje revidering av denna policy ska godkännas formellt av verkställande ledning.

9.3.2 Inaktuella versioner ska arkiveras säkert och den uppdaterade versionen ska innehålla dokumenterad ändringshistorik.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer de övergripande principerna för säkerhetsstyrning som ligger till grund för denna integritetspolicy. P1 stödjer konfidentialitet, riktighet och tillgänglighet för personuppgifter i samtliga system och tjänster.

10.2 P6 – Riskhanteringspolicy. Definierar organisationens metodik för riskbehandling, vilket är avgörande för bedömning av dataskyddsrisker, DPIA-processer och utvärdering av kvarstående risk enligt GDPR och ISO/IEC 27001 klausul 6.1.3.

10.3 P13 – Policy för informationsklassificering och märkning. Ger vägledning för kategorisering av personuppgifter och känsliga data och utgör grund för tillämpning av lämpliga dataskyddskontroller, inklusive bevarande, åtkomstbegränsning och säker avveckling.

10.4 P14 – Policy för bevarande och avveckling av data. Stödjer direkt dataskyddskraven enligt artiklarna 5.1 e och 17 i GDPR och säkerställer att personuppgifter endast bevaras så länge som nödvändigt och avvecklas säkert i enlighet med rättsliga krav.

10.5 P16 – Policy för datamaskering och pseudonymisering. Fastställer kontroller för att minska identifierbarheten i personuppgifter genom tekniska åtgärder såsom tokenisering, dynamisk maskering och pseudonymisering och tillämpar därigenom artikel 32 i GDPR samt kontroll 5.34 i ISO/IEC 27002.

10.6 P30 – Policy för incidenthantering (P30). Beskriver de obligatoriska protokollen för hantering av personuppgiftsincidenter som integreras med de tidsfrister för hantering och anmälan som krävs enligt artiklarna 33 och 34 i GDPR.

10.7 P33 – Policy för revisions- och efterlevnadsövervakning. Tillämpas för schemalagda bedömningar av integritetsprogrammets effektivitet, tillämpningen av policyn och uppföljningen av korrigerande åtgärder i organisatoriska enheter och hos personuppgiftsbiträden.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.1 – ledarskap och åtagande: fastställer ansvar på ledningsnivå för att skydda personuppgifter och tillämpa dataskyddsprinciper.

11.1.2 Klausul 6.1.3 – informationssäkerhetsriskhantering: stödjer identifiering, bedömning och behandling av dataskyddsrisker genom DPIA och undantag.

11.1.3 Klausul 8.1 – operativ planering och styrning: kräver tekniska och processmässiga skyddsåtgärder för att säkerställa att personuppgifter behandlas säkert.

11.1.4 Klausul 10.1 – kontinuerlig förbättring: kräver periodisk utvärdering och anpassning av integritetsprogrammet.

11.2 ISO/IEC 27002:2022 kontrollerna 5.34, 8.10, 8.11, 8.12: ger vägledning om hantering av PII, tillämpning av bevarande, radering, anonymisering och transparens avseende den registrerades rättigheter.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definierar styrning, roller, ansvarsskyldighet och ansvar för integritetsutbildning.

11.3.2 PL-2, PL-8: kräver integration av dataskyddskontroller i systemlivscykeln och företagsarkitekturen.

11.3.3 AC-2, AC-6: tillämpar principen om minsta privilegium och kontohantering för skydd av personuppgifter.

11.3.4 AU-2, AU-6, AU-9: kräver loggning, spårbarhet och revisionsintegritet för åtkomst till personuppgifter.

11.3.5 IR-4, IR-5, IR-6: definierar strukturerade processer för detektering, analys och rapportering av personuppgiftsincidenter.

11.3.6 PM-1, PM-21, PM-23: etablerar ett heltäckande integritetsprogram i linje med strategiska mål för riskhantering och datastyrning.

11.4 EU:s GDPR (2016/679)

11.4.1 Artiklarna 5, 6, 12–23, 25, 28, 30, 32–34: reglerar lagenlig behandling, ändamålsbegränsning, den registrerades rättigheter, ansvarsskyldighet, inbyggt dataskydd och dataskydd som standard, skyldigheter för tredje part samt hantering av personuppgiftsincidenter.

11.4.2 Skäl 78: förstärker principerna om inbyggt dataskydd.

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

11.5.1 Artikel 21.2 e och f: kräver införande av riskbaserade säkerhetskontroller och skydd av personuppgifter för väsentliga och viktiga entiteter.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 6.2 d: kräver intern styrning av IKT-risker relaterade till datahantering.

11.6.2 Artikel 11.1 c: kräver tillsyn av tredjepartsrisker för datarelaterade tjänster.

11.6.3 Artiklarna 15.1 och 17: kräver säker databehandling hos tjänsteleverantörer och skyndsam rapportering till tillsynsmyndigheter efter IKT-relaterade incidenter.

11.7 COBIT 2019

11.7.1 APO12 – riskhantering: integrerar dataskyddsrisker i organisationens övergripande riskstyrning.

11.7.2 DSS01 – hanterad drift och DSS05 – säkerhetstjänster: säkerställer säker drift inklusive åtkomstkontroll, bevarande och systemens riktighet.

11.7.3 MEA03 – övervakning av efterlevnad: kräver löpande granskning av efterlevnadsstatus mot regulatoriska och policybaserade dataskyddskrav.