					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P16					Dokumenttitel: **Policy för datamaskering och pseudonymisering**							
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	Referens	Kommentar
ISO/IEC 27001:2022	Avsnitt 6.1, 8.1	Allmänna krav för riskhantering samt operativa kontroller avseende datamaskering och pseudonymisering
ISO/IEC 27002:2022	Avsnitt 8 och kontroll 8.11	Vägledning för genomförande av datamaskering och pseudonymisering
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Integritets- och konfidentialitetskontroller för uppgiftsminimering, datatransformation och åtkomstbegränsning
EU:s dataskyddsförordning (GDPR)	Artiklar 4(5), 5(1)(c) och (f), 32	Rättslig definition och krav för pseudonymisering och dataskyddsåtgärder
EU:s NIS2-direktiv	Artikel 21(2)(c)	Skyldighet att tillämpa tekniska och organisatoriska åtgärder, inklusive integritetshöjande tekniker (PET)
EU:s DORA-förordning	Artiklar 10(1), 10(2)(e)	IKT-riskhantering och konfidentialitetskontroller avseende datamaskering och pseudonymisering
COBIT 2019	DSS05.01, DSS06.06, MEA03	Kontroller för styrning av dataskydd genom datamaskering samt bedömning av efterlevnad

1. Syfte

1.1 Denna policy definierar organisationens angreppssätt för att tillämpa datamaskering och pseudonymisering som integritetshöjande tekniker (PET) i syfte att minska identifierbarheten och exponeringen av personuppgifter eller andra känsliga data.

1.2 Den stödjer säker användning av information i testning, analys och drift samtidigt som rättsliga och regulatoriska krav uppfylls, konsekvenserna av säkerhetsincidenter begränsas och principerna om uppgiftsminimering och konfidentialitet upprätthålls.

1.3 Policyn är anpassad till ISO/IEC 27001:2022, stödjer artikel 4(5) i GDPR om pseudonymisering och bygger på ett riskbaserat genomförande i linje med NIST, EU:s NIS2-direktiv, EU:s DORA-förordning och COBIT 2019.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla anställda, uppdragstagare, tredjeparter och leverantörer med åtkomst till system som hanterar personuppgifter, konfidentiell information eller känsliga data.

2.1.2 Samtliga datamiljöer, inklusive produktions-, utvecklings-, test- och stagingmiljöer.

2.1.3 Alla former av datamaskering (t.ex. statisk, dynamisk och deterministisk maskering samt tokenisering) och pseudonymiseringstekniker som används för att minska integritetsrisker.

2.1.4 Alla datatyper (strukturerade eller ostrukturerade), system (lokalt eller i molnmiljö) och applikationer som hanterar personuppgifter eller uppgifter som omfattas av regulatoriska krav.

2.2 Denna policy omfattar användning i:

2.2.1 Applikationsutveckling samt kvalitetssäkrings- och testmiljöer

2.2.2 Analys- och rapporteringsplattformar

2.2.3 Datautbyte med tredjeparter eller tjänsteleverantörer

2.2.4 Säkerhetskopierings-, arkiverings- och återställningssystem

3. Mål

3.1 Säkerställa en enhetlig och effektiv tillämpning av datamaskering och pseudonymisering för att minska risker för dataexponering eller missbruk.

3.2 Säkerställa att skarpa data aldrig används i icke-produktionsmiljöer om de inte först har transformerats med godkända integritetshöjande tekniker (PET).

3.3 Bibehålla referensintegritet, användbarhet och formatbevarande egenskaper när det krävs för operativ konsistens.

3.4 Upprätthålla strikt åtkomstkontroll för originaldata, maskerade data och återidentifieringsnycklar.

3.5 Behandla maskerade eller pseudonymiserade dataset som känsliga data, med krav på åtkomstloggning, bevarandekontroller och incidenthanteringsrutiner.

3.6 Validera effektiviteten i dessa kontroller genom kontinuerlig testning, övervakning och återkommande revision.

4. Roller och ansvar

4.1 Högsta ledningen

4.1.1 Fastställer denna policy och säkerställer att den tillämpas som en del av organisationens övergripande IT-styrning och dataskyddsarbete.

4.2 Informationssäkerhetschef (CISO) eller ISMS-ansvarig

4.2.1 Övervakar genomförandet och den löpande efterlevnaden.

4.2.2 Säkerställer överensstämmelse med ISO/IEC 27001, avsnitt 6.1.3 (riskbehandling) och avsnitt 8.1 (operativ planering och styrning).

4.2.3 Granskar revisionsloggar och validerar kontrollernas effektivitet.

[... 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:

9.1.1 Regulatoriska förändringar som påverkar datamaskering eller pseudonymisering

9.1.2 Införande av nya IT-system som hanterar känsliga data

9.1.3 Väsentliga ändringar i organisationens dataklassificeringsschema

9.1.4 Revisionsiakttagelser som indikerar kontrollbrister

9.1.5 Framväxten av nya hot eller nya tekniker för datamaskering

9.2 ISMS-ansvarig ska leda granskningen i samråd med dataskyddsombudet (DPO), dataägare, IT-säkerhetsfunktionen och juridisk funktion. Uppdateringar ska versionshanteras, godkännas av högsta ledningen och kommuniceras till alla berörda intressenter.

10. Relaterade policyer och kopplingar

10.1 P13 - Policy för dataklassificering och märkning. Beslut om datamaskering och pseudonymisering är direkt beroende av den klassificering av datafält och de känslighetsnivåer som fastställs i P13.

10.2 P14 - Policy för databevarande och bortskaffning. Transformerade dataset ska bevaras och bortskaffas enligt livscykelreglerna i P14, så att maskerade och pseudonymiserade data behandlas som känsliga data.

10.3 P17 - Policy för dataskydd och integritet. Den anger dataskyddsprinciper samt de rättsliga och regulatoriska utgångspunkterna för att tillämpa pseudonymisering som en behandlingsmetod som uppfyller kraven enligt GDPR och liknande lagstiftning.

10.4 P22 - Loggnings- och övervakningspolicy. Den möjliggör centraliserad granskning och larmning av händelser kopplade till datamaskering och pseudonymisering i enlighet med strukturerade rutiner för säkerhetsövervakning.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:2022

11.1.1 Avsnitt 6.1.3 - riskbehandling: Fastställer datamaskering och pseudonymisering som riskbehandlingsåtgärder för att minska identifierbarheten hos känsliga data i behandlingsmiljöer som inte är nödvändiga för operativ drift.

11.1.2 Avsnitt 8.1 - operativ planering och styrning: Föreskriver tekniska och processuella kontroller för säker datatransformation vid behandling, lagring eller överföring.

11.2 ISO/IEC 27002:2022

11.2.1 Avsnitt 8 och kontroll 8.11: Vägledning om datamaskering och pseudonymisering för att minimera risker för återidentifiering och dataläckage.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Skydd av personligt identifierbar information (PII): Införande av integritetshöjande tekniker såsom datamaskering och pseudonymisering.

11.3.2 PT-2, PT-3: Minimering och säker behandling av personligt identifierbar information (PII) - datatransformation för att minska identifierbarhet och tillämpa åtkomstkontroll.

11.3.3 SC-12, SC-28, SC-30: Konfidentialitet och riktighet för data - kontroller för konfidentialitet och obfuskering av data vid lagring, överföring och användning.

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

11.4.1 Artikel 4(5): Formell definition av pseudonymisering.

11.4.2 Artikel 32: Säkerhet i behandlingen - organisatoriska och tekniska åtgärder för pseudonymisering.

11.4.3 Artikel 5(1)(c) och (f): Uppgiftsminimering och konfidentialitet genom pseudonymisering och datamaskering.

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

11.5.1 Artikel 21(2)(c): Kräver integritetshöjande tekniker (PET) såsom datamaskering och pseudonymisering som säkerhetsåtgärder.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 10(1): Ramverket för IKT-riskhantering omfattar kontroller för datamaskering och pseudonymisering.

11.6.2 Artikel 10(2)(e): Kräver användning av datatransformationstekniker för att skydda personuppgifter och finansiella data.

11.7 COBIT 2019

11.7.1 DSS05.01: Skydd av informationstillgångar - krav på datamaskering och pseudonymisering.

11.7.2 DSS06.06: Säker testning och analys - datamaskering i miljöer utanför produktion.

11.7.3 MEA03: Övervakning av efterlevnad och kontrollernas effektivitet för datamaskering och pseudonymisering.