					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P18					Dokumenttitel: **Policy för kryptografiska kontroller**							
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	Clause 8	-
ISO/IEC 27002:2022	Controls 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 to SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR	Article 32, Articles 33–34, Recital 83	-
EU:s NIS2-direktiv	Article 21(2)(d)	-
EU:s DORA-förordning	Articles 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Syfte

1.1 Denna policy fastställer obligatoriska krav för säker och korrekt användning av kryptografiska kontroller i hela organisationen för att säkerställa konfidentialitet, riktighet och autenticitet för känslig och reglerad information.

1.2 Användningen av kryptografi utgör en grund för tillit i informationssäkerhetsarbetet, stöder säker kommunikation, upprätthåller åtkomstkontroll och möjliggör regelefterlevnad genom effektiv kryptering och säker nyckelhantering.

1.3 Denna policy är anpassad till ISO/IEC 27001:2022 klausul 8.1 och bilaga A, kontroll 8.24 samt stöder rättsliga och operativa skyldigheter enligt artikel 32 i GDPR, artikel 6(2)(d) i DORA och artikel 21 i NIS2. Den stöder även COBIT 2019-mål för säkerhetstjänster och skydd av informationstillgångar.

2. Omfattning

2.1 Denna policy gäller för samtliga organisatoriska enheter, verksamhetsfunktioner, all personal och tredjepartstjänsteleverantörer som använder, administrerar eller inför kryptografiska verktyg och metoder.

2.2 Omfattade miljöer inkluderar produktions-, utvecklings-, test-, säkerhetskopierings- och katastrofåterställningssystem där känsliga data överförs, behandlas eller lagras.

2.3 Omfattningen inkluderar alla kryptografiska komponenter och användningsfall, inklusive men inte begränsat till:

2.3.1 Symmetrisk och asymmetrisk kryptering

2.3.2 Digitala signaturer och certifikat

2.3.3 Hashalgoritmer

2.3.4 Säker generering, distribution och destruktion av nycklar

2.3.5 Transport Layer Security (TLS), heldiskkryptering och kryptering på API-nivå

2.3.6 Säkra komponenter såsom Hardware Security Modules (HSM), Trusted Platform Modules (TPM) och Key Management Systems (KMS)

2.4 Denna policy reglerar användning av kryptografi i relation till:

2.4.1 Data som klassificeras som Konfidentiell, Högkonfidentiell eller Reglerad

2.4.2 Autentisering och verifiering av digital identitet

2.4.3 Säker kommunikation med externa parter

2.4.4 Nyckelförvaltarskap och mekanismer för dubbel kontroll

3. Mål

3.1 Säkerställa att kryptografiska tekniker väljs, godkänns, införs och upprätthålls i enlighet med verksamhetsrisk, internationella standarder och regulatoriska krav.

3.2 Etablera en standardiserad styrningsstruktur för hantering av kryptografiska tjänster, inklusive tydligt ansvar för införande, validering och undantagshantering.

3.3 Förhindra obehörig användning, felkonfiguration eller utfasningsefterlevnad av kryptografiska algoritmer och kontroller genom en formell process för godkännande och granskning.

3.4 Säkerställa att kryptografiska kontroller byggs in i systemens designfas och valideras regelbundet för att förhindra dataexponering, kompromettering av nycklar eller protokollförsvagning.

3.5 Upprätthålla livscykelhantering för policyer och rutiner för samtliga kryptografiska nycklar, inklusive generering, lagring, användning, rotation, återkallelse och säker destruktion.

3.6 Uppfylla internationella och regionala regelverk som kräver kryptering och säker datahantering, inklusive GDPR, DORA, NIS2 och COBIT 2019.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare för denna policy och säkerställer att den är förenlig med ISMS och ISO/IEC 27001 bilaga A, kontroll 8.24.

4.1.2 Godkänner användning av kryptografiska algoritmer och kontroller samt säkerställer efterlevnad i hela organisationen.

4.2 Ansvarig för kryptografiska operationer / säkerhetsarkitekt

4.2.1 Ansvarar för den dagliga driften och administrationen av kryptografiska system.

4.2.2 Underhåller listan över godkända kryptografiska metoder (ACML) och registret för nyckelhantering.

4.2.3 Genomför granskningar av kryptografisk design (CDR) och utvärderar nya kryptografiska tekniker.

[... 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 årligen av informationssäkerhetschef och ansvarig för kryptografiska operationer.

9.2 Granskningsutlösare inkluderar:

9.2.1 Upptäckt av kryptografiska sårbarheter (t.ex. algoritmnedgradering, kvantattacker)

9.2.2 Regulatoriska ändringar som kräver uppdaterade krypteringsstandarder

9.2.3 Operativa iakttagelser eller revisionsiakttagelser som visar på brister i policyn

9.2.4 Uppgraderingar av kryptografiska verktyg eller arkitektoniska förändringar

9.3 Uppdateringar ska versionshanteras i ISMS-dokumentregistret och kommuniceras till:

9.3.1 Samtliga administratörer med åtkomstroller för kryptografi

9.3.2 Utvecklingsteam och DevSecOps-ansvariga

9.3.3 Tredjepartsleverantörer med avtalsenliga skyldigheter avseende kryptering

9.4 ISMS-teamet ska säkerställa att ersatta versioner arkiveras och inte längre refereras i operativa rutiner.

10. Relaterade policyer och kopplingar

10.1 P1 - Informationssäkerhetspolicy. Tillhandahåller grundläggande styrning för alla säkerhetsåtgärder, inklusive tillämpning av kryptografiska kontroller, skydd av tillgångar och säker kommunikation.

10.2 P4 - Åtkomstkontrollpolicy. Säkerställer att logisk åtkomst till kryptografiskt material och system för krypteringshantering är strikt begränsad enligt principen om minsta privilegium och funktionsseparering.

10.3 P6 - Riskhanteringspolicy. Stödjer bedömningen av risker i kryptografiska kontroller och dokumenterar strategin för riskbehandling av undantag, föråldrade algoritmer eller scenarier med komprometterade nycklar.

10.4 P12 - Policy för tillgångshantering. Kräver klassificering av känsliga data och hårdvarutillgångar, vilket direkt avgör kryptografiska krav och skyldigheter för nyckelförvaltning.

10.5 P13 - Policy för informationsklassificering och märkning. Definierar klassificeringsnivåer (t.ex. Konfidentiell, Reglerad) som utlöser specifika krypteringskrav under överföring och i vila.

10.6 P14 - Policy för bevarande och bortskaffande av dokument. Specificerar rutiner för säker avveckling av krypterade lagringsmedier och kryptografiskt nyckelmaterial vid livscykelns slut.

10.7 P30 - Policy för incidenthantering. Beskriver organisationens strategi för hantering av komprometterade nycklar, felaktig certifikatanvändning eller misstänkta algoritmiska sårbarheter, inklusive snabb återkallelse och rapportering av överträdelser.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 - Operativ planering och styrning: Kräver tekniska säkerhetskontroller, inklusive kryptografiska åtgärder, som en del av operativa skyddsåtgärder.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroller 8.24, 8.25, 8: Ger vägledning för införande av kryptografiska kontroller, val av algoritmer, tillämpning av protokoll och livscykelhantering av certifikat.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Etablering av kryptografiska nycklar: Säkerställer säker generering och utväxling av krypteringsnycklar. P18 definierar hur symmetriska/asymmetriska nycklar ska genereras och utväxlas med godkända algoritmer och protokoll.

11.3.2 SC-13 - Kryptografiskt skydd: Kräver användning av kryptografi för att skydda konfidentialitet och riktighet för information. P18 kräver kryptering av data i vila och under överföring baserat på dataklassificering, med algoritmstandarder anpassade till NIST FIPS 140-3.

11.3.3 SC-17 - Certifikat för Public Key Infrastructure (PKI): Kräver införande av PKI för att stödja autentisering och digitala signaturer. P18 beskriver användning av PKI för att skydda kommunikation, systemidentiteter och administrativ åtkomst.

11.3.4 SC-28, SC-28(1) - Skydd av information i vila och under överföring: Kräver datakryptering när information lagras eller överförs över icke betrodda nätverk. P18 specificerar tillämpning av TLS, VPN-tunnlar, heldiskkryptering och säkra lagringsmetoder för känsliga data.

11.3.5 SC-12(3) - Generering av symmetriska nycklar för säker lagring och distribution: Fokuserar på säker generering och hantering av symmetriska nycklar. P18 kräver användning av starka slumptalsgeneratorer, policyer för nyckelrotation och säkra nyckelvalv för kryptografiska operationer.

11.4 GDPR (2016/679)

11.4.1 Artikel 32 - Säkerhet i samband med behandling: Rekommenderar uttryckligen kryptering som en riskreducerande åtgärd för personuppgifter.

11.4.2 Skäl 83: Betonar kryptering som kontroll för att förhindra obehörig åtkomst till data.

11.4.3 Artiklarna 33 och 34: Kryptering kan undanta organisationer från obligatoriska anmälningar av personuppgiftsincidenter om den är effektiv.

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

11.5.1 Artikel 21(2)(d): Kräver tekniska och organisatoriska åtgärder, inklusive kryptografiska skydd, för att upprätthålla tjänsternas tillgänglighet och riktighet.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 6(2)(d): Finansiella entiteter ska skydda data, inklusive genom stark kryptering av kritisk information.

11.6.2 Artikel 11(1)(c): Kräver säkra kontroller för databehandling för IKT-tredjepartstjänsteleverantörer.

11.7 COBIT 2019

11.7.1 DSS05.01 - Skydda informationstillgångar: Kräver användning av kryptering och nyckelhantering för att skydda data mot obehörig åtkomst.

11.7.2 DSS06.06 - Hanterad säkerhetstestning: Rekommenderar validering av efterlevnad för kryptografi som en del av sårbarhetsbedömningar.

11.7.3 MEA03 - Övervaka, utvärdera och bedöma efterlevnad: Kräver kontinuerlig säkerställning av effektiviteten i kryptografiska kontroller.