					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P18S					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/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	
ISO/IEC 27002:2022	Kontroller 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 till SC-17	
EU:s NIS2-direktiv	Artiklarna 21(2)(d), 21(2)(e)	
EU:s DORA-förordning	Artiklarna 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
EU:s GDPR	Artiklarna 32(1)(a), 34	

1. Syfte

1.1 Denna policy fastställer obligatoriska krav för användning av kryptering och kryptografiska kontroller för att skydda konfidentialitet, riktighet och autenticitet i verksamhetsdata och personuppgifter.

1.2 Den säkerställer att kryptografiska verktyg används korrekt i system, enheter och molntjänster inom en småföretagsmiljö.

1.3 Denna policy stödjer direkt certifiering enligt ISO/IEC 27001:2022 och hjälper organisationen att uppfylla rättsliga skyldigheter enligt EU:s allmänna dataskyddsförordning (GDPR), EU:s NIS2-direktiv och DORA-förordningen.

1.4 Kryptografiska kontroller som omfattas inkluderar datakryptering, certifikathantering, säker nyckelhantering och krypterade säkerhetskopior.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 alla anställda, uppdragstagare och tredje parter som hanterar företagets data

2.1.2 alla verksamhetssystem, klientenheter och molnplattformar som används för att lagra, överföra eller ge åtkomst till konfidentiell information

2.1.3 alla personrelaterade, finansiella, juridiska eller känsliga register som klassificeras enligt organisationens policy för informationsklassificering och märkning

2.1.4 varje kryptografisk kontroll, inklusive krypteringsmetoder, nycklar, lösenord, certifikat och säkerhetsmoduler

2.2 Policyn omfattar data i vila, data under överföring och data under användning. Den reglerar även kryptering som används för säkerhetskopior, e-post, externa dataöverföringar och publika webbplatser.

3. Mål

3.1 Säkerställa att känsliga och reglerade data alltid skyddas med lämpliga kryptografiska åtgärder

3.2 Fastställa ansvar för val av krypteringsverktyg, konfigurering och nyckelhantering

3.3 Förhindra obehörig åtkomst, manipulation eller dataläckage genom att tillämpa säkra kontroller för överföring och lagring

3.4 Uppfylla rättsliga och regulatoriska krav som föreskriver kryptering av personuppgifter och verksamhetsdata

3.5 Upprätthålla operativ säkerhet och tillgänglighet genom effektiv hantering av certifikat och kryptografiska nycklar

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 godkänner denna policy och säkerställer att kryptografiska krav tillämpas

4.1.2 granskar undantag, incidentrapportering och leverantörers efterlevnad av krypteringskrav

4.1.3 verifierar att outsourcade tjänster och molntjänster uppfyller gällande krypteringsstandarder

4.2 Extern IT-tjänsteleverantör / intern IT-administratör

4.2.1 implementerar och upprätthåller krypteringslösningar (t.ex. heldiskkryptering, SSL-certifikat, VPN)

4.2.2 hanterar livscykeln för kryptografiska nycklar och verktyg för säker lagring

4.2.3 konfigurerar och övervakar kryptering för säkerhetskopior, webbplatser och enhetsskydd

[... 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 minst en gång per år av verkställande direktören i samordning med IT-tjänsteleverantören och dataskyddssamordnaren.

9.2 Utlösande faktorer för mellanliggande granskning

9.2.1 Granskningar ska även genomföras om:

9.2.1.1 kryptografiska standarder eller protokoll ändras (t.ex. utfasning av en algoritm)

9.2.1.2 nya system eller molntjänster införs

9.2.1.3 en överträdelse eller incident rör en komprometterad nyckel eller ett komprometterat certifikat

9.2.1.4 rättsliga eller regulatoriska uppdateringar påverkar krypteringskraven

9.3 Versionshantering och kommunikation

9.3.1 Alla policyändringar ska dokumenteras i en versionslogg

9.3.2 Personal ska informeras om uppdateringar och tidigare versioner ska arkiveras

9.3.3 Den senast godkända versionen ska lagras i det centrala policyarkivet

10. Relaterade policyer och kopplingar

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

10.1.1 P12S – Policy för tillgångshantering: Säkerställer att kryptering tillämpas på klassificerade tillgångar vid lagring, överföring och avveckling.

10.1.2 P14S – Policy för dokumentbevarande och säker avveckling: Fastställer bevarandeperioder och kräver krypterad lagring av data till dess att de raderas på ett säkert sätt.

10.1.3 P17S – Policy för dataskydd och integritet: Anpassar kryptering till dataskyddsprinciper och regulatoriska förväntningar enligt artikel 32 i GDPR.

10.1.4 P22S – Policy för loggning och övervakning: Kräver loggning av nyckelanvändning, krypteringsfel och certifikats utgångsdatum för revisionsändamål.

10.1.5 P30S – Policy för incidenthantering: Beskriver eskalerings-, begränsnings- och aviseringsrutiner när kryptering brister eller nycklar komprometteras.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver implementering av operativa kontroller, inklusive kryptering, för att hantera säkerhetsrisker.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.24 – Beskriver krav för tillämpning av kryptering för konfidentialitet och riktighet.

11.2.2 Kontroll 8.25 – Beskriver säker hantering av kryptografiska nycklar och certifikat.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Fastställer krav för etablering och validering av kryptografiska nycklar.

11.3.2 SC-13 – Definierar standarder för generering av kryptografiska nycklar.

11.3.3 SC-17 – Omfattar infrastruktur för publika nycklar (PKI) och livscykelhantering för certifikat.

11.3.4 SC-28 – Kräver kryptering av data i vila.

11.3.5 SC-12 till SC-17 (familj) – Säkerställer att kryptografiska skydd implementeras korrekt i olika system.

11.4 EU:s GDPR

11.4.1 Artikel 32(1)(a) – Kräver att organisationer implementerar tekniska åtgärder såsom kryptering för att säkerställa datakonfidentialitet.

11.4.2 Artikel 34 – Anger att kryptering kan undanta organisationer från anmälan om personuppgiftsincident om data var obegripliga för obehöriga personer.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(d) – Kräver effektiv kryptering för att skydda system och kommunikation.

11.5.2 Artikel 21(2)(e) – Betonar skydd av data och begränsning av cyberhot genom kryptering.

11.6 EU:s DORA-förordning

11.6.1 Artikel 6(2)(d) – Kräver att IKT-system upprätthåller säkra kommunikationskanaler och kryptering.

11.6.2 Artikel 9(2)(f) – Ålägger finansiella entiteter att använda stark kryptering för att skydda digital kommunikation och datautbyte.

11.7 COBIT 2019

11.7.1 DSS05.01 – Kräver skydd av känslig information genom kryptering och kryptografiska protokoll.

11.7.2 APO13.02 – Kräver effektiva säkerhetskontroller, inklusive kryptografiska skyddsåtgärder, som en del av planeringen av informationssäkerhet.