					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P18S					Dokumenttitel: **Politik for kryptografiske kontroller**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	
ISO/IEC 27002:2022	Kontrol 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 til SC-17	
EU NIS2	Artikel 21(2)(d), 21(2)(e)	
EU DORA	Artikel 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
EU GDPR	Artikel 32(1)(a), 34	

1. Formål

1.1 Denne politik fastsætter obligatoriske krav til anvendelse af kryptering og kryptografiske kontroller for at beskytte fortrolighed, integritet og autenticitet af forretningsdata og personoplysninger.

1.2 Den sikrer, at kryptografiske værktøjer anvendes hensigtsmæssigt på tværs af systemer, enheder og cloudtjenester i virksomheden.

1.3 Denne politik understøtter direkte certificering efter ISO/IEC 27001:2022 og hjælper organisationen med at opfylde retlige forpligtelser i henhold til databeskyttelsesforordningen (GDPR), NIS2-direktivet og Digital Operational Resilience Act (DORA).

1.4 De kryptografiske kontroller, der er omfattet, omfatter datakryptering, certifikatstyring, sikker nøglehåndtering og krypterede sikkerhedskopier.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, kontrahenter og tredjeparter, der håndterer virksomhedens data

2.1.2 Alle forretningssystemer, slutpunkter og cloudplatforme, der anvendes til at lagre, overføre eller tilgå fortrolige oplysninger

2.1.3 Alle personoplysninger samt finansielle, juridiske eller følsomme registreringer, der er klassificeret i henhold til organisationens Politik for dataklassificering og mærkning

2.1.4 Enhver kryptografisk kontrol, herunder krypteringsmetoder, nøgler, adgangskoder, certifikater og sikkerhedsmoduler

2.2 Politikken omfatter data i hvile, data under overførsel og data i brug. Den regulerer også kryptering anvendt til sikkerhedskopier, e-mail, eksterne dataoverførsler og offentligt tilgængelige websites.

3. Mål

3.1 Sikre, at følsomme og regulerede data til enhver tid er beskyttet med passende kryptografiske foranstaltninger

3.2 Fastlægge ansvar for valg af krypteringsværktøjer, konfiguration og nøglestyring

3.3 Forebygge uautoriseret adgang, manipulation eller datalækage ved at håndhæve sikre kontroller for overførsel og lagring

3.4 Overholde retlige og regulatoriske krav, der kræver kryptering af personoplysninger og forretningsdata

3.5 Opretholde driftssikkerhed og tilgængelighed gennem effektiv styring af certifikater og kryptografiske nøgler

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender denne politik og sikrer, at kryptografiske krav håndhæves

4.1.2 Gennemgår undtagelser, underretninger om brud og leverandørers efterlevelse af krypteringskrav

4.1.3 Verificerer, at outsourcede tjenester og cloudtjenester opfylder gældende krypteringsstandarder

4.2 IT-support/IT-administrator

4.2.1 Implementerer og vedligeholder krypteringsløsninger, herunder fuld diskkryptering, TLS-certifikater og VPN-forbindelser

4.2.2 Styrer livscyklussen for kryptografiske nøgler og værktøjer til sikker opbevaring

4.2.3 Konfigurerer og overvåger kryptering til beskyttelse af sikkerhedskopier, websites og enheder

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Årlig gennemgang

9.1.1 Denne politik skal gennemgås mindst én gang årligt af direktøren i koordinering med IT-support og databeskyttelseskoordinatoren.

9.2 Udløsende forhold for ekstraordinær gennemgang

9.2.1 Gennemgang skal også gennemføres, hvis:

9.2.1.1 Kryptografiske standarder eller protokoller ændres, herunder udfasning af en algoritme

9.2.1.2 Nye systemer eller cloudtjenester indføres

9.2.1.3 Et brud eller en hændelse involverer en kompromitteret nøgle eller et kompromitteret certifikat

9.2.1.4 Retlige eller regulatoriske opdateringer påvirker krav til kryptering

9.3 Versionsstyring og kommunikation

9.3.1 Alle ændringer i politikken skal dokumenteres i en ændringslog

9.3.2 Medarbejdere skal underrettes om opdateringer, og tidligere versioner skal arkiveres

9.3.3 Den seneste godkendte version skal opbevares i det centrale dokumentarkiv

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal anvendes sammen med følgende SME-politikker:

10.1.1 P12S – Politik for aktiver: Sikrer, at kryptering anvendes på klassificerede aktiver under lagring, overførsel og bortskaffelse.

10.1.2 P14S – Politik for opbevaring og sikker bortskaffelse af data: Fastlægger opbevaringsperioder og kræver krypteret lagring af data, indtil de slettes sikkert.

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Afstemmer kryptering med databeskyttelsesprincipper og regulatoriske forventninger efter GDPR artikel 32.

10.1.4 P22S – Politik for logning og overvågning: Kræver logning af nøgleanvendelse, krypteringssvigt og certifikatudløb til revisionsformål.

10.1.5 P30S – Politik for hændelseshåndtering: Beskriver eskalering, inddæmning og underretningsprocedurer, når kryptering svigter, eller nøgler kompromitteres.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kræver implementering af operationelle kontroller, herunder kryptering, til styring af sikkerhedsrisici.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.24 – Beskriver krav til anvendelse af kryptering til sikring af fortrolighed og integritet.

11.2.2 Kontrol 8.25 – Beskriver sikker styring af kryptografiske nøgler og certifikater.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Fastsætter krav til etablering og validering af kryptografiske nøgler.

11.3.2 SC-13 – Definerer standarder for generering af kryptografiske nøgler.

11.3.3 SC-17 – Omfatter offentlig nøgleinfrastruktur (PKI) og styring af certifikaters livscyklus.

11.3.4 SC-28 – Kræver kryptering af data i hvile.

11.3.5 SC-12 til SC-17 (familie) – Sikrer, at kryptografiske beskyttelsesforanstaltninger implementeres korrekt på tværs af systemer.

11.4 EU GDPR

11.4.1 Artikel 32(1)(a) – Kræver, at organisationer implementerer tekniske foranstaltninger såsom kryptering for at sikre datafortrolighed.

11.4.2 Artikel 34 – Fastslår, at kryptering kan fritage organisationer fra underretning om brud, hvis data var uforståelige for uautoriserede personer.

11.5 EU NIS2-direktivet

11.5.1 Artikel 21(2)(d) – Kræver effektiv kryptering til sikring af systemer og kommunikation.

11.5.2 Artikel 21(2)(e) – Fremhæver databeskyttelse og afbødning af cybertrusler gennem kryptering.

11.6 EU DORA

11.6.1 Artikel 6(2)(d) – Kræver, at IKT-systemer opretholder sikre kommunikationskanaler og kryptering.

11.6.2 Artikel 9(2)(f) – Forpligter finansielle enheder til at anvende stærk kryptering for at beskytte digital kommunikation og dataudveksling.

11.7 COBIT 2019

11.7.1 DSS05.01 – Kræver beskyttelse af følsomme oplysninger gennem kryptering og kryptografiske protokoller.

11.7.2 APO13.02 – Kræver effektiv implementering af sikkerhedskontroller, herunder kryptografiske sikkerhedsforanstaltninger, som led i planlægning af informationssikkerhed.