					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P18					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	Clause 8	-
ISO/IEC 27002:2022	Controls 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 til SC-17, SC-28, SC-28(1), SC-12(3)	-
EU GDPR	Article 32, Articles 33–34, Recital 83	-
EU NIS2	Article 21(2)(d)	-
EU DORA	Articles 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Formål

1.1 Denne politik fastsætter obligatoriske krav til sikker og regelkonform anvendelse af kryptografiske kontroller i hele organisationen med henblik på at sikre fortrolighed, integritet og autenticitet for følsomme og regulerede oplysninger.

1.2 Anvendelsen af kryptografi skal understøtte tillid til informationssikkerhedsdriften, sikker kommunikation, håndhævelse af adgangskontrol samt overholdelse af regulatoriske krav gennem effektiv kryptering og forsvarlig nøglestyring.

1.3 Denne politik er tilpasset ISO/IEC 27001:2022 Clause 8.1 og Annex A Control 8.24 og understøtter juridiske og operationelle forpligtelser efter GDPR Article 32, DORA Article 6(2)(d) og NIS2 Article 21. Den understøtter desuden COBIT 2019-mål vedrørende sikkerhedstjenester og beskyttelse af dataaktiver.

2. Omfang

2.1 Denne politik gælder for alle organisatoriske enheder, forretningsfunktioner, medarbejdere og tredjepartsleverandører, der er involveret i anvendelse, administration eller implementering af kryptografiske værktøjer og metoder.

2.2 Omfattede miljøer omfatter produktions-, udviklings-, test-, backup- og katastrofeberedskabssystemer, hvor følsomme data overføres, behandles eller opbevares.

2.3 Omfanget omfatter alle kryptografiske komponenter og anvendelsestilfælde, herunder, men ikke begrænset til:

2.3.1 Symmetrisk og asymmetrisk kryptering

2.3.2 Digitale signaturer og certifikater

2.3.3 Hashalgoritmer

2.3.4 Sikker nøglegenerering, distribution og destruktion

2.3.5 Transport Layer Security (TLS), fuld diskkryptering (FDE) og kryptering på API-niveau

2.3.6 Sikre elementer såsom Hardware Security Modules (HSM'er), Trusted Platform Modules (TPM'er) og Key Management Systems (KMS)

2.4 Denne politik regulerer kryptografisk anvendelse i relation til:

2.4.1 Data klassificeret som Fortrolig, Strengt fortrolig eller Reguleret

2.4.2 Autentifikation og verifikation af digitale identiteter

2.4.3 Sikker kommunikation med eksterne parter

2.4.4 Nøgleforvaltning og mekanismer til dobbeltkontrol

3. Mål

3.1 Sikre, at kryptografiske teknologier udvælges, godkendes, implementeres og vedligeholdes i overensstemmelse med forretningsrisici, internationale standarder og regulatoriske krav.

3.2 Etablere en standardiseret styringsstruktur for forvaltning af kryptografiske tjenester, herunder entydig ansvarstildeling for implementering, validering og håndtering af undtagelser.

3.3 Forebygge uautoriseret brug, fejlkonfiguration eller forældelse af kryptografiske algoritmer og kontroller gennem en formel proces for godkendelse og gennemgang.

3.4 Sikre, at kryptografiske kontroller indarbejdes i systemdesignfasen og valideres regelmæssigt for at forhindre dataeksponering, nøglekompromittering eller svækkelse af protokoller.

3.5 Håndhæve livscyklusstyring af alle kryptografiske nøgler, herunder generering, opbevaring, anvendelse, rotation, tilbagekaldelse og sikker destruktion.

3.6 Efterleve internationale og regionale regler, der kræver kryptering og sikker håndtering af data, herunder GDPR, DORA, NIS2 og COBIT 2019.

4. Roller og ansvar

4.1 Informationssikkerhedschef / CISO

4.1.1 Har ejerskab for denne politik og sikrer, at den er tilpasset ISMS'et og ISO/IEC 27001 Annex A Control 8.24.

4.1.2 Godkender anvendelsen af kryptografiske algoritmer og kontroller og håndhæver efterlevelse i hele organisationen.

4.2 Ansvarlig for kryptografiske operationer / sikkerhedsarkitekt

4.2.1 Har ansvar for den daglige drift og administration af kryptografiske systemer.

4.2.2 Vedligeholder listen over godkendte kryptografiske metoder (ACML) og registret for nøglestyring.

4.2.3 Gennemfører kryptografiske designgennemgange (CDR) og vurderer nye kryptografiske teknologier.

[... 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 Denne politik skal gennemgås årligt af informationssikkerhedschefen og den ansvarlige for kryptografiske operationer.

9.2 Udløsende forhold for gennemgang omfatter:

9.2.1 Identifikation af kryptografiske sårbarheder (f.eks. algoritmenedgradering, kvanteangreb)

9.2.2 Regulatoriske ændringer, der kræver opdaterede krypteringsstandarder

9.2.3 Driftsmæssige forhold eller revisionskonstateringer, der afdækker mangler i politikken

9.2.4 Opgraderinger af kryptografiske værktøjer eller arkitekturændringer

9.3 Opdateringer skal være versionsstyrede i ISMS'ets dokumentstyringsregister og kommunikeres til:

9.3.1 Alle administratorer med adgangsroller til kryptografi

9.3.2 Udviklingsteams og DevSecOps-ansvarlige

9.3.3 Tredjepartsleverandører med kontraktuelle krypteringsforpligtelser

9.4 ISMS-teamet skal sikre, at erstattede versioner arkiveres og ikke længere refereres i driftsprocedurer.

10. Relaterede politikker og sammenhænge

10.1 P1 - Informationssikkerhedspolitik. Angiver det grundlæggende styringsgrundlag for alle sikkerhedsforanstaltninger, herunder håndhævelse af kryptografiske kontroller, beskyttelse af aktiver og sikker kommunikation.

10.2 P4 - Politik for adgangskontrol. Sikrer, at logisk adgang til kryptografisk materiale og systemer til styring af kryptering er strengt begrænset efter princippet om mindst privilegium og funktionsadskillelse.

10.3 P6 - Politik for risikostyring. Understøtter vurdering af risici ved kryptografiske kontroller og dokumenterer strategien for risikobehandling ved undtagelser, algoritmers forældelse eller scenarier med nøglekompromittering.

10.4 P12 - Politik for styring af aktiver. Kræver klassificering af følsomme data og hardwareaktiver, hvilket direkte fastlægger kryptografiske krav og forpligtelser vedrørende nøgleforvaltning.

10.5 P13 - Politik for dataklassificering og mærkning. Definerer de klassificeringsniveauer (f.eks. Fortrolig, Reguleret), der udløser specifikke krypteringskrav under overførsel og i hvile.

10.6 P14 - Politik for opbevaring og sikker bortskaffelse af data. Angiver procedurer for sikker bortskaffelse af krypterede lagringsmedier og kryptografisk nøglemateriale ved endt livscyklus.

10.7 P30 - Politik for hændelseshåndtering. Beskriver organisationens strategi for håndtering af nøglekompromittering, misbrug af certifikater eller mistænkte algoritmiske sårbarheder, herunder hurtig tilbagekaldelse og rapportering af brud.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 - operationel planlægning og styring: Håndhæver tekniske sikkerhedskontroller, herunder kryptografiske foranstaltninger, som en del af de operationelle sikkerhedsforanstaltninger.

11.2 ISO/IEC 27002:2022

11.2.1 Controls 8.24, 8.25, 8: Indeholder implementeringsvejledning om formål med kryptografiske kontroller, valg af algoritmer, håndhævelse af protokoller og livscyklusstyring af certifikater.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Etablering af kryptografiske nøgler: Sikrer sikker generering og udveksling af krypteringsnøgler. P18 fastsætter, hvordan symmetriske og asymmetriske nøgler skal genereres og udveksles ved brug af godkendte algoritmer og protokoller.

11.3.2 SC-13 - Kryptografisk beskyttelse: Kræver anvendelse af kryptografi til at beskytte oplysningers fortrolighed og integritet. P18 håndhæver kryptering i hvile og under overførsel baseret på dataklassificering med algoritmestandarder tilpasset NIST FIPS 140-3.

11.3.3 SC-17 - Public Key Infrastructure (PKI)-certifikater: Kræver implementering af PKI til understøttelse af autentifikation og digitale signaturer. P18 beskriver anvendelsen af PKI til at sikre kommunikation, systemidentiteter og administrativ adgang.

11.3.4 SC-28, SC-28(1) - Beskyttelse af oplysninger i hvile og under overførsel: Kræver datakryptering ved opbevaring eller transmission over ikke-betroede netværk. P18 specificerer håndhævelse af TLS, VPN-tunneller, fuld diskkryptering og sikre opbevaringsmetoder for følsomme data.

11.3.5 SC-12(3) - Symmetrisk nøglegenerering til sikker opbevaring og distribution: Har fokus på sikker generering og håndtering af symmetriske nøgler. P18 kræver anvendelse af stærke tilfældighedsgeneratorer, politikker for nøglerotation og sikre nøglelagre til kryptografiske operationer.

11.4 EU GDPR (2016/679)

11.4.1 Article 32 - behandlingssikkerhed: Anbefaler udtrykkeligt kryptering som en risikoreducerende foranstaltning for personoplysninger.

11.4.2 Recital 83: Fremhæver kryptering som en kontrol til forebyggelse af uautoriseret adgang til data.

11.4.3 Articles 33 and 34: Kryptering kan fritage organisationer for obligatorisk anmeldelse af brud, hvis den er effektiv.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(d): Kræver tekniske og organisatoriske foranstaltninger, herunder kryptografisk beskyttelse, for at opretholde tjenesters tilgængelighed og integritet.

11.6 EU DORA (2022/2554)

11.6.1 Article 6(2)(d): Finansielle institutioner skal beskytte data, herunder gennem stærk kryptering af kritiske oplysninger.

11.6.2 Article 11(1)(c): Kræver sikre kontroller for databehandling hos IKT-tredjepartsleverandører.

11.7 COBIT 2019

11.7.1 DSS05.01 - Beskyt informationsaktiver: Kræver anvendelse af kryptering og nøglestyring til at beskytte data mod uautoriseret adgang.

11.7.2 DSS06.06 - Styret sikkerhedstestning: Anbefaler validering af kryptografisk efterlevelse som en del af sårbarhedsvurderinger.

11.7.3 MEA03 - Overvåg, evaluer og vurder efterlevelse: Understøtter løbende overvågning og vurdering af effektiviteten af kryptografiske kontroller.