					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P18					Documenttitel: **Beleid inzake cryptografische beheersmaatregelen**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	-
ISO/IEC 27002:2022	Beheersmaatregelen 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 t/m SC-17, SC-28, SC-28(1), SC-12(3)	-
AVG	Artikel 32, artikelen 33–34, overweging 83	-
EU NIS2	Artikel 21(2)(d)	-
EU DORA	Artikelen 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Doel

1.1 Dit beleid stelt bindende eisen vast voor het veilige en conforme gebruik van cryptografische beheersmaatregelen binnen de gehele organisatie, teneinde de vertrouwelijkheid, integriteit en authenticiteit van gevoelige en gereguleerde informatie te waarborgen.

1.2 Het gebruik van cryptografie vormt de basis voor vertrouwen in gegevensbeveiligingsprocessen, ondersteunt veilige communicatie, dwingt toegangsbeheersing af en faciliteert naleving van wet- en regelgeving door middel van doeltreffende encryptie- en sleutelbeheerpraktijken.

1.3 Dit beleid is afgestemd op ISO/IEC 27001:2022, clausule 8.1 en Annex A-beheersmaatregel 8.24, en ondersteunt juridische en operationele verplichtingen uit hoofde van artikel 32 AVG, artikel 6(2)(d) DORA en artikel 21 NIS2. Daarnaast ondersteunt dit beleid COBIT 2019-doelstellingen voor beveiligingsdiensten en de bescherming van informatieactiva.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle organisatieonderdelen, bedrijfsfuncties, medewerkers en externe dienstverleners die betrokken zijn bij het gebruik, beheer of de implementatie van cryptografische middelen en methoden.

2.2 De onder dit beleid vallende omgevingen omvatten productie-, ontwikkel-, test-, back-up- en herstelomgevingen waarin gevoelige gegevens worden verzonden, verwerkt of opgeslagen.

2.3 De reikwijdte omvat alle cryptografische componenten en gebruiksscenario's, waaronder in ieder geval:

2.3.1 Symmetrische en asymmetrische encryptie

2.3.2 Digitale handtekeningen en certificaten

2.3.3 Hashalgoritmen

2.3.4 Veilige generatie, distributie en vernietiging van sleutels

2.3.5 Transport Layer Security (TLS), volledige schijfversleuteling (FDE) en encryptie op API-niveau

2.3.6 Veilige componenten zoals Hardware Security Modules (HSM's), Trusted Platform Modules (TPM's) en Key Management Systems (KMS)

2.4 Dit beleid reguleert het gebruik van cryptografie in relatie tot:

2.4.1 Gegevens die zijn geclassificeerd als Vertrouwelijk, Zeer Vertrouwelijk of Gereguleerd

2.4.2 Authenticatie en verificatie van digitale identiteiten

2.4.3 Veilige communicatie met externe partijen

2.4.4 Sleutelbeheer en mechanismen voor duale controle

3. Doelstellingen

3.1 Waarborgen dat cryptografische technologieën worden geselecteerd, goedgekeurd, geïmplementeerd en onderhouden in overeenstemming met bedrijfsrisico's, internationale normen en verplichtingen uit wet- en regelgeving.

3.2 Een gestandaardiseerde governancestructuur vaststellen voor het beheer van cryptografische diensten, met duidelijke verantwoordelijkheid voor implementatie, validatie en uitzonderingsbeheer.

3.3 Ongeautoriseerd gebruik, onjuiste configuratie of veroudering van cryptografische algoritmen en beheersmaatregelen voorkomen via een formeel goedkeurings- en beoordelingsproces.

3.4 Waarborgen dat cryptografische beheersmaatregelen in de ontwerpfase van systemen worden ingebed en periodiek worden gevalideerd om gegevensblootstelling, compromittering van sleutels of verzwakking van protocollen te voorkomen.

3.5 Levenscyclusbeheer afdwingen voor alle cryptografische sleutels, met inbegrip van generatie, opslag, gebruik, rotatie, intrekking en veilige vernietiging.

3.6 Voldoen aan internationale en regionale regelgeving die encryptie en veilige gegevensverwerking voorschrijft, waaronder AVG, DORA, NIS2 en COBIT 2019.

4. Rollen en verantwoordelijkheden

4.1 Informatiebeveiligingsmanager / CISO

4.1.1 Is eigenaar van dit beleid en ziet toe op de afstemming met het ISMS en ISO/IEC 27001 Annex A-beheersmaatregel 8.24.

4.1.2 Keurt het gebruik van cryptografische algoritmen en beheersmaatregelen goed en handhaaft naleving binnen de organisatie.

4.2 Verantwoordelijke voor cryptografische operaties / beveiligingsarchitect

4.2.1 Beheert de dagelijkse uitvoering en administratie van cryptografische systemen.

4.2.2 Beheert de lijst met goedgekeurde cryptografische methoden (ACML) en het sleutelbeheerregister.

4.2.3 Voert cryptografische ontwerpbeoordelingen (CDR's) uit en evalueert nieuwe cryptografische technologieën.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisatie

9.1 Dit beleid moet jaarlijks worden beoordeeld door de Informatiebeveiligingsmanager en de verantwoordelijke voor cryptografische operaties.

9.2 Aanleidingen voor herziening omvatten:

9.2.1 Ontdekking van cryptografische kwetsbaarheden (bijvoorbeeld algorithm downgrade, quantum attacks)

9.2.2 Wijzigingen in wet- en regelgeving die geactualiseerde encryptiestandaarden vereisen

9.2.3 Operationele bevindingen of auditbevindingen die lacunes in het beleid aan het licht brengen

9.2.4 Upgrades van cryptografische middelen of architectuurwijzigingen

9.3 Actualisaties moeten onder versiebeheer worden opgenomen in het ISMS-register voor documentbeheer en worden gecommuniceerd aan:

9.3.1 Alle beheerders met cryptografische toegangsrollen

9.3.2 Ontwikkelteams en DevSecOps-verantwoordelijken

9.3.3 Externe dienstverleners met contractuele verplichtingen inzake encryptie

9.4 Het ISMS-team moet erop toezien dat vervallen versies worden gearchiveerd en niet langer in operationele procedures worden gebruikt.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P1 - Informatiebeveiligingsbeleid. Biedt de fundamentele governance voor alle beveiligingsmaatregelen, met inbegrip van de afdwinging van cryptografische beheersmaatregelen, bescherming van activa en veilige communicatie.

10.2 P4 - Beleid inzake toegangsbeheersing. Waarborgt dat logische toegang tot cryptografisch materiaal en encryptiebeheersystemen strikt wordt beperkt op basis van het beginsel van minimale bevoegdheden en functiescheiding (SoD).

10.3 P6 - Beleid inzake risicobeheer. Ondersteunt de beoordeling van risico's van cryptografische beheersmaatregelen en documenteert de strategie voor risicobehandeling voor uitzonderingen, veroudering van algoritmen of compromittering van sleutels.

10.4 P12 - Beleid inzake beheer van bedrijfsmiddelen. Verplicht classificatie van gevoelige gegevens en hardwareactiva, wat rechtstreeks bepalend is voor cryptografische vereisten en verplichtingen rond sleutelbeheer.

10.5 P13 - Beleid inzake gegevensclassificatie en etikettering. Definieert de classificatieniveaus (bijvoorbeeld Vertrouwelijk, Gereguleerd) die specifieke encryptie-eisen tijdens transport en in rust activeren.

10.6 P14 - Beleid inzake gegevensbewaring en afvoer. Specificeert procedures voor de veilige afvoer van versleutelde opslagmedia en cryptografisch sleutelmateriaal aan het einde van de levensduur.

10.7 P30 - Incidentresponsbeleid. Beschrijft de responsstrategie van de organisatie voor compromittering van sleutels, misbruik van certificaten of vermoedelijke algoritmische kwetsbaarheden, met inbegrip van snelle intrekking en incidentmelding.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 - Operationele planning en beheersing: verplicht technische beveiligingsmaatregelen, waaronder cryptografische maatregelen, als onderdeel van operationele beheersing.

11.2 ISO/IEC 27002:2022

11.2.1 Beheersmaatregelen 8.24, 8.25, 8: biedt implementatierichtlijnen voor cryptografische beheersdoelstellingen, selectie van algoritmen, protocolafdwinging en levenscyclusbeheer van certificaten.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Vaststelling van cryptografische sleutels: waarborgt veilige generatie en uitwisseling van encryptiesleutels. P18 bepaalt hoe symmetrische en asymmetrische sleutels met goedgekeurde algoritmen en protocollen moeten worden gegenereerd en uitgewisseld.

11.3.2 SC-13 - Cryptografische bescherming: verplicht het gebruik van cryptografie om de vertrouwelijkheid en integriteit van informatie te beschermen. P18 dwingt encryptie in rust en tijdens transport af op basis van gegevensclassificatie, met algoritmestandaarden afgestemd op NIST FIPS 140-3.

11.3.3 SC-17 - Public Key Infrastructure (PKI)-certificaten: vereist implementatie van PKI ter ondersteuning van authenticatie en digitale handtekeningen. P18 beschrijft het gebruik van PKI voor het beveiligen van communicatie, systeemidentiteiten en administratieve toegang.

11.3.4 SC-28, SC-28(1) - Bescherming van informatie in rust en tijdens transport: vereist gegevensencryptie wanneer informatie wordt opgeslagen of verzonden over niet-vertrouwde netwerken. P18 specificeert de afdwinging van TLS, VPN-tunnels, volledige schijfversleuteling en beveiligde opslagmethoden voor gevoelige gegevens.

11.3.5 SC-12(3) - Symmetrische sleutelgeneratie voor veilige opslag en distributie: richt zich op het veilig genereren en verwerken van symmetrische sleutels. P18 verplicht het gebruik van sterke willekeurige getallengeneratoren, beleid voor sleutelrotatie en beveiligde sleutelkluizen voor cryptografische operaties.

11.4 AVG (2016/679)

11.4.1 Artikel 32 - Beveiliging van de verwerking: beveelt encryptie uitdrukkelijk aan als maatregel voor risicoreductie voor persoonsgegevens.

11.4.2 Overweging 83: benadrukt encryptie als beheersmaatregel om ongeautoriseerde toegang tot gegevens te voorkomen.

11.4.3 Artikelen 33 en 34: effectieve encryptie kan organisaties vrijstellen van bepaalde meldverplichtingen bij inbreuken.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(d): vereist technische en organisatorische maatregelen, waaronder cryptografische bescherming, om de beschikbaarheid en integriteit van diensten te waarborgen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(2)(d): financiële instellingen moeten gegevens beveiligen, onder meer door middel van sterke encryptie van kritieke informatie.

11.6.2 Artikel 11(1)(c): verplicht veilige beheersmaatregelen voor gegevensverwerking voor ICT-dienstverleners van derde partijen.

11.7 COBIT 2019

11.7.1 DSS05.01 - Bescherm informatieactiva: vereist het gebruik van encryptie en sleutelbeheer om gegevens te beschermen tegen ongeautoriseerde toegang.

11.7.2 DSS06.06 - Beheerde beveiligingstesten: beveelt validatie van naleving van cryptografische eisen aan als onderdeel van kwetsbaarheidsbeoordelingen.

11.7.3 MEA03 - Monitoren, evalueren en beoordelen van naleving: verplicht continue assurance over de doeltreffendheid van cryptografische beheersmaatregelen.