| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P18S | | | | | Documenttitel:<br>**Beleid inzake cryptografische beheersmaatregelen** | | | | | | | |
| Versie:<br>1.0 | | Ingangsdatum:<br>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 | |
| NIST SP 800-53 Rev. 5 | SC-12 tot en met SC-17, SC-28 | |
| EU NIS2 | Artikelen 21(2)(d), 21(2)(e) | |
| EU DORA | Artikelen 6(2)(d), 9(2)(f) | |
| COBIT 2019 | DSS05.01, APO13.02 | |
| AVG | Artikelen 32(1)(a), 34 | |

**1. Doel**

1.1 Dit beleid stelt verplichte eisen aan het gebruik van encryptie en cryptografische beheersmaatregelen ter bescherming van de vertrouwelijkheid, integriteit en authenticiteit van bedrijfsgegevens en persoonsgegevens.

1.2 Het waarborgt dat cryptografische voorzieningen op passende wijze worden toegepast binnen systemen, apparaten en cloudgehoste diensten in een mkb-omgeving.

1.3 Dit beleid ondersteunt rechtstreeks certificering volgens ISO/IEC 27001:2022 en helpt de organisatie te voldoen aan de wettelijke verplichtingen uit de Algemene verordening gegevensbescherming (AVG), de NIS2-richtlijn en de Digital Operational Resilience Act (DORA).

1.4 Cryptografische beheersmaatregelen die onder dit beleid vallen, omvatten onder meer gegevensversleuteling, certificaatbeheer, veilig sleutelbeheer en versleutelde back-ups.

**2. Reikwijdte**

**2.1 Dit beleid is van toepassing op:**

2.1.1 alle medewerkers, opdrachtnemers en derden die bedrijfsgegevens verwerken;

2.1.2 alle bedrijfssystemen, eindpunten en cloudplatforms die worden gebruikt voor de opslag, overdracht of benadering van vertrouwelijke informatie;

2.1.3 alle persoonlijke, financiële, juridische of anderszins gevoelige gegevens die zijn geclassificeerd volgens het gegevensclassificatiebeleid van de organisatie;

2.1.4 alle cryptografische beheersmaatregelen, waaronder versleutelingsmethoden, sleutels, wachtwoorden, certificaten en hardwarebeveiligingsmodules.

2.2 Dit beleid heeft betrekking op gegevens in rust, gegevens tijdens transport en gegevens in gebruik. Het regelt tevens encryptie voor back-ups, e-mail, externe gegevensoverdrachten en publiek toegankelijke websites.

**3. Doelstellingen**

3.1 Waarborgen dat gevoelige en gereguleerde gegevens te allen tijde worden beschermd met passende cryptografische maatregelen

3.2 Verantwoordelijkheden vastleggen voor de selectie, configuratie en het beheer van encryptievoorzieningen en sleutels

3.3 Onbevoegde toegang, manipulatie of datalekken voorkomen door veilige beheersmaatregelen voor overdracht en opslag af te dwingen

3.4 Voldoen aan wettelijke en reglementaire vereisten die encryptie van persoonsgegevens en bedrijfsgegevens voorschrijven

3.5 Operationele beveiliging en beschikbaarheid waarborgen door certificaten en cryptografische sleutels doeltreffend te beheren

**4. Rollen en verantwoordelijkheden**

**4.1 Algemeen directeur (GM)**

4.1.1 Keurt dit beleid goed en ziet erop toe dat cryptografische vereisten worden gehandhaafd

4.1.2 Beoordeelt uitzonderingen, meldingen van inbreuken en de naleving door leveranciers van encryptievereisten

4.1.3 Verifieert dat uitbestede diensten en cloudservices voldoen aan encryptienormen

**4.2 IT-supportverlener / interne IT-beheerder**

4.2.1 Implementeert en onderhoudt encryptieoplossingen, zoals volledige-schijfversleuteling, TLS-certificaten en VPN's

4.2.2 Beheert de levenscyclus van cryptografische sleutels en voorzieningen voor veilige opslag

4.2.3 Configureert en bewaakt encryptie voor back-ups, websites en apparaatbeveiliging

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

**9. Vereisten voor beoordeling en actualisering**

**9.1 Jaarlijkse beoordeling**

9.1.1 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld door de algemeen directeur, in afstemming met de IT-supportverlener en de privacycoördinator.

**9.2 Aanleidingen voor tussentijdse beoordeling**

**9.2.1 Beoordelingen moeten ook worden uitgevoerd indien:**

9.2.1.1 cryptografische normen of protocollen wijzigen, zoals het uitfaseren van een algoritme;

9.2.1.2 nieuwe systemen of cloudservices worden ingevoerd;

9.2.1.3 een inbreuk of incident betrekking heeft op een gecompromitteerde sleutel of certificaat;

9.2.1.4 wettelijke of reglementaire wijzigingen gevolgen hebben voor encryptievereisten.

**9.3 Versiebeheer en communicatie**

9.3.1 Alle beleidswijzigingen moeten worden vastgelegd in een versiebeheerlogboek

9.3.2 Medewerkers moeten over actualisaties worden geïnformeerd en voorgaande versies moeten worden gearchiveerd

9.3.3 De meest recente goedgekeurde versie moet worden opgeslagen in de centrale beleidsrepository

**10. Gerelateerde beleidsstukken en samenhang**

**10.1 Dit beleid moet worden toegepast in samenhang met de volgende mkb-beleidsstukken:**

10.1.1 P12S – Beleid voor bedrijfsmiddelenbeheer: Waarborgt dat encryptie wordt toegepast op geclassificeerde bedrijfsmiddelen tijdens opslag, overdracht en afvoer.

10.1.2 P14S – Beleid voor bewaartermijnen en verwijdering van gegevens: Bepaalt bewaartermijnen en vereist versleutelde opslag van gegevens totdat deze veilig zijn verwijderd.

10.1.3 P17S – Beleid voor gegevensbescherming en privacy: Brengt encryptie in lijn met beginselen van gegevensbescherming en reglementaire verwachtingen onder artikel 32 AVG.

10.1.4 P22S – Beleid voor logging en toezicht: Vereist het vastleggen van sleutelgebruik, encryptiefouten en het verlopen van certificaten voor auditdoeleinden.

10.1.5 P30S – Beleid voor incidentrespons: Beschrijft escalatie-, inperkings- en meldingsprocedures wanneer encryptie faalt of sleutels zijn gecompromitteerd.

## 11. Referentienormen en raamwerken

### 11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Vereist de implementatie van operationele beheersmaatregelen, waaronder encryptie, om beveiligingsrisico's te beheersen.

### 11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.24 – Beschrijft vereisten voor het toepassen van encryptie ter bescherming van vertrouwelijkheid en integriteit.

11.2.2 Beheersmaatregel 8.25 – Beschrijft het veilig beheer van cryptografische sleutels en certificaten.

### 11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Stelt vereisten vast voor het opzetten en valideren van cryptografische sleutels.

11.3.2 SC-13 – Definieert normen voor het genereren van cryptografische sleutels.

11.3.3 SC-17 – Behandelt public key infrastructure (PKI) en het beheer van de levenscyclus van certificaten.

11.3.4 SC-28 – Vereist encryptie van gegevens in rust.

11.3.5 SC-12 tot en met SC-17 (familie) – Waarborgt dat cryptografische beschermingsmaatregelen correct binnen systemen worden geïmplementeerd.

### 11.4 AVG

11.4.1 Artikel 32(1)(a) – Vereist dat organisaties technische maatregelen zoals encryptie implementeren om de vertrouwelijkheid van gegevens te waarborgen.

11.4.2 Artikel 34 – Bepaalt dat encryptie organisaties kan vrijstellen van meldingen van inbreuken indien de gegevens onbegrijpelijk waren voor onbevoegde personen.

### 11.5 NIS2-richtlijn

11.5.1 Artikel 21(2)(d) – Vereist doeltreffende encryptie voor de beveiliging van systemen en communicatie.

11.5.2 Artikel 21(2)(e) – Benadrukt de bescherming van gegevens en het mitigeren van cyberdreigingen door middel van encryptie.

### 11.6 EU DORA

11.6.1 Artikel 6(2)(d) – Vereist dat ICT-systemen beveiligde communicatiekanalen en encryptie handhaven.

11.6.2 Artikel 9(2)(f) – Verplicht financiële entiteiten tot het gebruik van sterke encryptie ter bescherming van digitale communicatie en gegevensuitwisseling.

### 11.7 COBIT 2019

11.7.1 DSS05.01 – Schrijft bescherming van gevoelige informatie voor door middel van encryptie en cryptografische protocollen.

11.7.2 APO13.02 – Vereist doeltreffende implementatie van beveiligingsbeheersmaatregelen, waaronder cryptografische waarborgen, als onderdeel van informatiebeveiligingsplanning.