| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>P18 | | | | | Document Title:<br>**Cryptographic Controls Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>01.01.2025 | | | Document Owner: | | | | | | | |
| X | Policy | | Standard | | Procedure | | Form | | Register | | Other | |

| **Revision history** | | | | |
|---|---|---|---|---|
| **Revision number** | **Revision Date** | **Changes** | **Reviewed by** | **Process owner** |
| | | | | |
| | | | | |

| **Approvals** | | | |
|---|---|---|---|
| **Name** | **Title** | **Date** | **Signature** |
| | | | |
| | | | |

Aligned with standards and regulations

| Standard/Regulation | Clause/Article | Comment |
|---|---|---|
| ISO/IEC 27001:2022 | Clause 8 | - |
| ISO/IEC 27002:2022 | Controls 8.24, 8.25, 8 | - |
| NIST SP 800-53 Rev. 5 | SC-12 to 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, MEA03 | - |

**1. Purpose**

1.1 This policy defines mandatory requirements for the secure and compliant use of cryptographic controls across the organization to ensure the confidentiality, integrity, and availability of sensitive and regulated information.

1.2 The use of cryptography underpins trust in data security operations, supports secure communications, enforces access control, and enables regulatory compliance through effective encryption and key management practices.

1.3 This policy aligns with ISO/IEC 27001:2022 Clause 8.1 and Annex A Control 8.24 and supports legal and operational obligations under GDPR Article 32, DORA Article 6(2)(d), and NIS2 Article 21. It also supports COBIT 2019 objectives for security services and the protection of data assets.

**2. Scope**

2.1 This policy applies to all organizational units, business functions, personnel, contractors, and third-party service providers involved in the use, administration, or implementation of cryptographic tools and methods.

2.2 Covered environments include production, development, staging, backup, and disaster recovery systems in which sensitive data is transmitted, processed, or stored.

**2.3 The scope includes all cryptographic components and use cases, including but not limited to:**

2.3.1 Symmetric and asymmetric encryption

2.3.2 Digital signatures and certificates

2.3.3 Hashing algorithms

2.3.4 Secure key generation, distribution, and destruction

2.3.5 Transport Layer Security (TLS), Full Disk Encryption (FDE), and API-level encryption

2.3.6 Secure elements such as Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), and Key Management Systems (KMS)

**2.4 This policy governs cryptographic use in relation to:**

2.4.1 Data classified as Confidential, Highly Confidential, or Regulated

2.4.2 Authentication and digital identity verification

2.4.3 Secure communications with external parties

2.4.4 Key custodianship and dual-control mechanisms

## 3. Objectives

3.1 Ensure that cryptographic technologies are selected, approved, implemented, and maintained in accordance with business risk, international standards, and regulatory requirements.

3.2 Establish a standardized governance structure for managing cryptographic services, including clear accountability for implementation, validation, and exception handling.

3.3 Prevent the unauthorized use, misconfiguration, or obsolescence of cryptographic algorithms and controls through a formal approval workflow and review process.

3.4 Ensure that cryptographic controls are embedded during the system design phase and validated regularly to prevent data exposure, key compromise, or protocol degradation.

3.5 Enforce lifecycle management for all cryptographic keys, including generation, storage, use, rotation, revocation, and secure deletion.

3.6 Comply with international and regional regulations mandating encryption and secure data handling, including GDPR, DORA, NIS2, and COBIT 2019.

## 4. Roles and Responsibilities

### 4.1 Information Security Manager / CISO

4.1.1 Owns this policy and ensures its alignment with the Information Security Management System (ISMS) and ISO/IEC 27001 Annex A Control 8.24.

4.1.2 Approves the use of cryptographic algorithms and controls and enforces compliance across the organization.

### 4.2 Cryptographic Operations Lead / Security Architect

4.2.1 Manages the day-to-day operation and administration of cryptographic systems.

4.2.2 Maintains the Approved Cryptographic Methods List (ACML) and Key Management Register.

4.2.3 Conducts Cryptographic Design Reviews (CDRs) and evaluates new cryptographic technologies.

[ ... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ... ]

## 9. Review and Update Requirements

9.1 This policy shall be reviewed annually by the Information Security Manager and the Cryptographic Operations Lead.

### 9.2 Review Triggers Include:

9.2.1 Discovery of cryptographic vulnerabilities (e.g., algorithm downgrade, quantum attacks)

9.2.2 Regulatory changes requiring updated encryption standards

9.2.3 Operational or audit findings revealing policy gaps

9.2.4 Cryptographic tool upgrades or architectural changes

### 9.3 Updates must be version-controlled in the ISMS Document Control Register and communicated to:

9.3.1 All administrators with cryptographic access roles

9.3.2 Development teams and DevSecOps leads

9.3.3 Third-party providers subject to contractual encryption obligations

9.4 The ISMS team must ensure that superseded versions are archived and no longer referenced in operating procedures.

## 10. Related Policies and Linkages

10.1 P1 - Information Security Policy. Provides foundational governance for all security measures, including cryptographic control enforcement, asset protection, and secure communications.

10.2 P4 - Access Control Policy. Ensures logical access to cryptographic material and encryption management systems is strictly limited based on least privilege and segregation of duties.

10.3 P6 - Risk Management Policy. Supports the assessment of cryptographic control risks and documents the risk treatment strategy for exceptions, algorithm obsolescence, or key compromise scenarios.

10.4 P12 - Asset Management Policy. Mandates classification of sensitive data and hardware assets, which directly determines cryptographic requirements and key custodianship obligations.

10.5 P13 - Data Classification and Labeling Policy. Defines the classification levels (e.g., Confidential, Regulated) that trigger specific encryption requirements in transit and at rest.

10.6 P14 - Data Retention Policy and Secure Disposal Policy. Specifies procedures for the secure disposal of encrypted storage media and cryptographic key material at end of life.

10.7 P30 - Incident Response Policy. Outlines the organization's response strategy for key compromise, certificate misuse, or suspected algorithmic vulnerabilities, including rapid revocation and breach reporting.

## 11. Reference Standards and Frameworks

### 11.1 ISO/IEC 27001

11.1.1 Clause 8.1 - Operational Planning and Control: Enforces technical security controls, including cryptographic measures, as part of operational safeguards.

### 11.2 ISO/IEC 27002:2022

11.2.1 Controls 8.24, 8.25, 8: Provides implementation guidance on cryptographic control objectives, algorithm selection, protocol enforcement, and certificate lifecycle management.

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

11.3.1 SC-12 - Cryptographic Key Establishment: Ensures secure generation and exchange of encryption keys. P18 defines how symmetric and asymmetric keys must be generated and exchanged using approved algorithms and protocols.

11.3.2 SC-13 - Cryptographic Protection: Mandates the use of cryptography to protect the confidentiality and integrity of information. P18 enforces encryption at rest and in transit based on data classification, with algorithm standards aligned to NIST FIPS 140-3.

11.3.3 SC-17 - Public Key Infrastructure (PKI) Certificates: Requires implementation of PKI to support authentication and digital signatures. P18 outlines PKI use for securing communications, system identities, and administrative access.

11.3.4 SC-28, SC-28(1) - Protection of Information at Rest and in Transit: Requires data encryption when stored or transmitted over untrusted networks. P18 specifies enforcement of TLS, corporate VPN tunnels, full-disk encryption, and secure storage methods for sensitive data.

11.3.5 SC-12(3) - Symmetric Key Generation for Secure Storage and Distribution: Focuses on the secure generation and handling of symmetric keys. P18 mandates the use of strong random number generators, key rotation policies, and secure key vaults for cryptographic operations.

### 11.4 EU GDPR (2016/679)

11.4.1 Article 32 - Security of Processing: Explicitly recommends encryption as a risk-reduction measure for personal information (PII).

11.4.2 Recital 83: Emphasizes encryption as a control to prevent unauthorized data access.

11.4.3 Articles 33 and 34: Encryption may exempt organizations from mandatory data breach notifications if effective.

### 11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(d): Requires technical and organizational measures, including cryptographic protections, to maintain service availability and integrity.

**11.6 EU DORA (2022/2554)**

11.6.1 Article 6(2)(d): Financial institutions must secure data, including through strong encryption of critical information.

11.6.2 Article 11(1)(c): Mandates secure data processing controls for ICT third-party service providers.

**11.7 COBIT 2019**

11.7.1 DSS05.01 - Protect Information Assets: Requires the use of encryption and key management to safeguard data against unauthorized access.

11.7.2 DSS06.06 - Managed Security Testing: Recommends cryptographic compliance validation as part of vulnerability assessments.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: Enforces continuous assurance of cryptographic control effectiveness.