					[Insert Registered Legal Entity Name Here]								
Document number: P18					Document Title: **Cryptographic Controls Policy**								
Version: 1.0		Effective Date: 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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 8.24, 8.25, 8.27	
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	

					[Insert Registered Legal Entity Name Here]							
Document number: P18					Document Title: **Cryptographic Controls Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

1. Purpose

1.1 This policy defines mandatory requirements for the secure and compliant use of cryptographic controls throughout the organization to ensure the confidentiality, integrity, and authenticity 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 protection of data assets.

2. Scope

2.1 This policy applies to all organizational units, business functions, personnel, 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 where 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 mandates.

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 and review process.

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

3.5 Enforce lifecycle management of all cryptographic keys, including generation, storage, usage, rotation, revocation, and secure destruction.

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 ISMS and ISO/IEC 27001 Annex A Control 8.24.

[.....]

11. Reference Standards and Frameworks

This policy aligns with global standards and regulatory frameworks to ensure cryptographic controls meet legal, operational, and security obligations.

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022 - Controls 8.24, 8.25, 8.27

Provides implementation guidance on cryptographic control objectives, algorithm selection, protocol enforcement, and certificate lifecycle management.

NIST SP 800-53 Rev.5

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

SC-13 - Cryptographic Protection. Mandates 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.

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

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, VPN tunnels, full-disk encryption, and secure storage methods for sensitive data.

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

EU GDPR (2016/679)

Article 32 - Security of Processing: Explicitly recommends encryption as a risk-reduction measure for personal data.

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

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

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