					Insert Registered Legal Entity Name Here							
Document number: P18S					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	
ISO/IEC 27002:2022	Controls 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 to SC-17	
EU NIS2	Articles 21(2)(d), 21(2)(e)	
EU DORA	Articles 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
EU GDPR	Articles 32(1)(a), 34	

1. Purpose

1.1 This policy establishes mandatory requirements for the use of encryption and cryptographic controls to protect the confidentiality, integrity, and availability of business and personal data.

1.2 It ensures that cryptographic tools are used appropriately across systems, devices, and cloud services in a small business environment.

1.3 This policy directly supports ISO/IEC 27001:2022 certification and helps the organization meet its legal obligations under the EU General Data Protection Regulation (GDPR), the EU NIS2 Directive, and the Digital Operational Resilience Act (DORA).

1.4 Cryptographic controls covered by this policy include data encryption, certificate management, secure key handling, and encrypted backups.

2. Scope

2.1 This policy applies to:

2.1.1 All Personnel, Contractors, and Third-Party Service Providers handling company data

2.1.2 All business systems, endpoints, and cloud platforms used to store, transmit, or access confidential information

2.1.3 All personal, financial, legal, or sensitive records classified under the organization's Data Classification and Labeling Policy

2.1.4 Any cryptographic control, including encryption methods, keys, passwords, certificates, and security modules

2.2 This policy covers data at rest, data in transit, and data in use. It also governs encryption used for backups, email, external data transfers, and public-facing websites.

3. Objectives

3.1 Ensure that sensitive and regulated data is protected at all times using appropriate cryptographic measures

3.2 Define responsibility for encryption tool selection, configuration, and key management

3.3 Prevent unauthorized access, tampering, or data leakage by enforcing secure transmission and storage controls

3.4 Comply with legal and regulatory requirements mandating the encryption of personal and business data

3.5 Maintain operational security and availability through effective management of certificates and cryptographic keys

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Approves this policy and ensures that cryptographic requirements are enforced

4.1.2 Reviews exceptions, data breach notifications, and vendor compliance with encryption requirements

4.1.3 Verifies that outsourced and cloud services meet encryption standards

4.2 IT Support Provider / Internal IT Administrator

4.2.1 Implements and maintains encryption solutions (e.g., full-disk encryption, SSL/TLS certificates, corporate VPNs)

4.2.2 Manages cryptographic key lifecycles and secure storage solutions

4.2.3 Configures and monitors encryption for backups, websites, and device protection

[... 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 Annual Review

9.1.1 This policy must be reviewed at least annually by the General Manager in coordination with the IT Support Provider and Privacy Coordinator.

9.2 Triggers for Interim Review

9.2.1 Reviews must also be conducted if:

9.2.1.1 Cryptographic standards or protocols change (e.g., deprecation of an algorithm)

9.2.1.2 New systems or cloud services are introduced

9.2.1.3 A breach or incident involves a compromised key or certificate

9.2.1.4 Legal or regulatory updates affect encryption requirements

9.3 Version Control and Communication

9.3.1 All policy changes must be documented in a version control log

9.3.2 Staff must be notified of updates, and previous versions must be archived

9.3.3 The latest approved version must be stored in the central policy repository

10. Related Policies and Linkages

10.1 This policy must be applied in conjunction with the following SME policies:

10.1.1 P12S – Asset Management Policy: Ensures that encryption is applied to classified assets during storage, transfer, and disposal.

10.1.2 P14S – Data Retention Policy and Secure Disposal Policy: Defines retention periods and requires encrypted storage of data until securely deleted.

10.1.3 P17S – Data Protection and Privacy Policy: Aligns encryption with data protection principles and regulatory expectations under GDPR Article 32.

10.1.4 P22S – Logging and Monitoring Policy: Requires logging of key usage, encryption failures, and certificate expirations for audit purposes.

10.1.5 P30S – Incident Response Policy: Details escalation, containment, and notification procedures when encryption fails or keys are compromised.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Requires the implementation of operational controls, including encryption, to manage security risks.

11.2 ISO/IEC 27002

11.2.1 Control 8.24 – Describes requirements for applying encryption to protect confidentiality and integrity.

11.2.2 Control 8.25 – Outlines the secure management of cryptographic keys and certificates.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Establishes requirements for cryptographic key establishment and validation.

11.3.2 SC-13 – Defines standards for cryptographic key generation.

11.3.3 SC-17 – Covers public key infrastructure (PKI) and certificate lifecycle management.

11.3.4 SC-28 – Requires encryption of data at rest.

11.3.5 SC-12 to SC-17 (family) – Ensures that cryptographic protections are properly implemented across systems.

11.4 EU GDPR

11.4.1 Article 32(1)(a) – Requires organizations to implement technical measures such as encryption to ensure data confidentiality.

11.4.2 Article 34 – States that encryption may exempt organizations from breach notification if the data was unintelligible to unauthorized persons.

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(d) – Requires effective encryption to secure systems and communications.

11.5.2 Article 21(2)(e) – Emphasizes data protection and mitigation of cyber threats through encryption.

11.6 EU DORA

11.6.1 Article 6(2)(d) – Requires ICT systems to maintain secure communication channels and encryption.

11.6.2 Article 9(2)(f) – Requires financial entities to use strong encryption to safeguard digital communications and data exchanges.

11.7 COBIT 2019

11.7.1 DSS05.01 – Requires protection of sensitive information through encryption and cryptographic protocols.

11.7.2 APO13.02 – Requires effective implementation of security controls, including cryptographic safeguards, as part of information security planning.