					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
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, APO13.02	
EU GDPR	Articles 32(1)(a), 34	

					[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		

1. **Purpose**
   1.1. This policy defines mandatory requirements for the use of encryption and cryptographic controls to protect the confidentiality, integrity, and authenticity 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 the legal obligations of the EU General Data Protection Regulation (GDPR), the EU NIS2 Directive, and the Digital Operational Resilience Act (DORA).
   1.4. Cryptographic controls covered include data encryption, certificate management, secure key handling, and encrypted backups.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, contractors, and third parties 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 policy
      2.1.4. Any cryptographic control, including encryption methods, keys, passwords, certificates, and security modules
   2.2. The 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 sensitive and regulated data is protected using appropriate cryptographic measures at all times
   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 that mandate encryption of personal and business data
   3.5. Maintain operational security and availability by managing certificates and cryptographic keys effectively
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves this policy and ensures cryptographic requirements are enforced
      4.1.2. Reviews exceptions, breach notifications, and vendor compliance with encryption clauses
      4.1.3. Verifies that outsourced or 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 certificates, VPNs)
      4.2.2. Manages cryptographic key lifecycles and secure storage tools
      4.2.3. Configures and monitors encryption for backup, website, and device protection
   4.3. **Privacy or Security Coordinator**

4.3.1. Ensures encryption controls align with data protection obligations under Article 32 of the GDPR
4.3.2. Supports risk assessments and breach response involving encrypted systems
4.3.3. Verifies legal defensibility of encryption choices

4.4. **All Staff and Contractors**

4.4.1. Must follow encryption instructions and only use approved systems and applications
4.4.2. Are prohibited from disabling or bypassing encryption features

[…….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

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

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

NIST SP 800-53 Rev.5

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

SC-13 – Defines standards for cryptographic key generation.

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

SC-28 – Requires encryption of data at rest.

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

EU GDPR

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

Article 34 – States encryption can exempt organizations from breach notifications if data was unintelligible to unauthorized persons.

EU NIS2 Directive

Article 21(2)(d) – Requires effective encryption for securing systems and communications.

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

EU DORA

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

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

COBIT 2019

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

APO13.02 – Requires effective security control implementations, including cryptographic safeguards, as part of information security planning.