					[Insert Registered Legal Entity Name Here]							
Document number: P16S					Document Title: **Data Masking and Pseudonymization 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 6.1.3, Clause 8.1	
ISO/IEC 27002:2022	Controls 8.11, 8.12	
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	
EU NIS2	Article 21(2)(c)	
EU DORA	Article 10(1)	
COBIT 2019	DSS05.01, DSS06.06	
EU GDPR	Articles 4(5), 5(1)(c), 32	

1. **Purpose**
   1.1. This policy defines enforceable requirements for the use of data masking and pseudonymization to protect sensitive, personal, and confidential data within small and mid-sized enterprises (SMEs).
   1.2. These techniques are mandatory when real data is not necessary, such as in development, analytics, or third-party service scenarios, helping to reduce risks of exposure, misuse, or breach.
   1.3. This policy directly supports compliance with ISO/IEC 27001:2022 certification, as well as European regulatory mandates such as the GDPR, NIS2 Directive, and DORA Regulation.
   1.4. By transforming data before using it outside its original business context, the organization limits liability and enhances its ability to demonstrate privacy and security due diligence.
2. **Scope**
   2.1. This policy applies to all structured or unstructured data classified as personal, confidential, or sensitive, whether stored or processed:
      2.1.1. In production, test, or development environments
      2.1.2. On local devices, servers, or cloud platforms
      2.1.3. By internal staff, contractors, or third-party providers
   2.2. It also covers all data transformation tools (masking, tokenization, pseudonymization), whether open-source, commercial, or developed in-house.
   2.3. Use cases under this policy include:
      2.3.1. Preparing test or development data sets
      2.3.2. Exporting data to analytics systems
      2.3.3. Vendor or consultant access to operational systems
      2.3.4. Data subject minimization to reduce processing risk
3. **Objectives**
   3.1. Ensure real personal or sensitive data is never exposed in lower-security environments where it is not essential.
   3.2. Mandate masking or pseudonymization techniques when real identifiers are not strictly needed for the task.
   3.3. Prevent unauthorized access or misuse of data by enforcing transformation controls prior to data transfer or processing.
   3.4. Guarantee all masking and pseudonymization processes are traceable, auditable, and enforced through approved tools.
   3.5. Comply with applicable legal and regulatory standards requiring data minimization, confidentiality, and transformation safeguards.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Owns and approves this policy
      4.1.2. Ensures all departments and providers comply with transformation requirements
      4.1.3. Reviews exceptions, risk assessments, and transformation logs
      4.1.4. Coordinates legal, operational, or vendor actions in case of violations

4.2. **IT Support Provider / Internal IT**

4.2.1. Selects and manages masking or pseudonymization tools

4.2.2. […….]

Reference Standards and Frameworks

This policy is aligned with the following authoritative standards and legal requirements:

ISO/IEC 27001:2022

Clause 6.1.3: Requires the treatment of information security risks, which includes mitigating exposure through data transformation techniques.

Clause 8.1: Mandates the implementation of controls necessary to meet security objectives, including pseudonymization and masking.

ISO/IEC 27002:2022

Control 8.11: Provides guidance on masking sensitive data in test and development systems.

Control 8.12: Offers strategies to prevent data leakage through controlled transformation and access practices.

NIST SP 800-53 Rev.5

SC-12: Ensures the confidentiality of information through data obfuscation.

SC-28: Protects information at rest and in use.

PT-2/PT-3: Promote the use of privacy-enhancing technologies, including pseudonymization, when processing PII.

EU GDPR

Article 4(5): Legally defines pseudonymization and mandates controls over mapping keys and identifiers.

Article 5(1)(c): Supports data minimization principles through masking.

Article 32: Recognizes pseudonymization as a technical control that reduces privacy risks.

EU NIS2 Directive

Article 21(2)(c): Requires proportionate technical measures to minimize data security risk, including pseudonymization as part of risk control.

EU DORA Regulation

Article 10(1): Mandates ICT-related risk controls that include data transformation safeguards for continuity and confidentiality during outsourcing and system development.

COBIT 2019

DSS05.01: Requires the protection of information assets, including transformation where possible.

DSS06.06: Calls for appropriate obfuscation and pseudonymization techniques to limit data exposure in lower-trust environments.