					Insert Registered Legal Entity Name Here							
Document number: P16					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 6.1	General requirements for risk management and operational controls for masking and pseudonymization
ISO/IEC 27002:2022	Controls 8.11, 8	Implementation guidance for masking and pseudonymization controls
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Privacy and confidentiality controls for data minimization, transformation, and access restriction
EU GDPR	Articles 4(5), 5(1)(c,f), 32	Legal basis and requirements for pseudonymization and data protection measures
EU NIS2	Article 21(2)(c)	Requirement for technical and organizational measures, including privacy-enhancing technologies (PETs)
EU DORA	Articles 10(1), 10(2)(e)	ICT risk management and confidentiality controls for data masking and pseudonymization
COBIT 2019	DSS05.01, DSS06.06, MEA	Governance controls for data protection through masking and compliance assessment

1. Purpose

1.1 This policy defines the organization's approach to implementing data masking and pseudonymization as privacy-enhancing technologies (PETs) to reduce the identifiability and exposure of personal or sensitive data.

1.2 It supports the secure use of information in testing, analytics, and operations while ensuring compliance with legal and regulatory requirements, reducing the impact of breaches, and enforcing the principles of data minimization and confidentiality.

1.3 This policy aligns with ISO/IEC 27001:2022, supports GDPR Article 4(5) on pseudonymization, and incorporates risk-based implementation consistent with NIST, NIS2, DORA, and COBIT 2019.

2. Scope

2.1 This policy applies to:

2.1.1 All employees, contractors, third parties, and vendors with access to systems that process personal, confidential, or sensitive information.

2.1.2 All data environments, including production, development, test, and staging environments.

2.1.3 All forms of data masking (e.g., static, dynamic, deterministic, tokenization) and pseudonymization techniques used to reduce privacy risk.

2.1.4 All data types (structured and unstructured), systems (on premises or cloud-hosted), and applications involving personal data or data subject to regulation.

2.2 This scope includes use within:

2.2.1 Application development and QA/testing environments

2.2.2 Analytics and reporting platforms

2.2.3 Data exchange with third parties or service providers

2.2.4 Backup, archival, and recovery systems

3. Objectives

3.1 Ensure the consistent and effective application of masking and pseudonymization to reduce the risk of data exposure or misuse.

3.2 Ensure that live data is never used in non-production environments unless it has been transformed using approved PET techniques.

3.3 Maintain referential integrity, usability, and format-preserving transformation where required for operational consistency.

3.4 Enforce strict access controls for original data, masked data, and re-identification keys.

3.5 Treat masked and pseudonymized datasets as sensitive data, subject to access logging, retention controls, and incident response procedures.

3.6 Validate the effectiveness of these controls through ongoing testing, monitoring, and audit activities.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves this policy and ensures its enforcement as part of broader IT governance and data protection initiatives.

4.2 Chief Information Security Officer (CISO) / ISMS Manager

4.2.1 Oversees implementation and ongoing compliance.

4.2.2 Ensures alignment with ISO/IEC 27001 Clause 6.1.3 (risk treatment) and Clause 8.1 (operational control).

4.2.3 Reviews audit logs and validates control effectiveness.

[... 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 at least annually, or earlier in the event of:

9.1.1 Regulatory changes affecting masking or pseudonymization

9.1.2 Adoption of new IT systems that process sensitive data

9.1.3 Material changes to the organization’s data classification scheme

9.1.4 Audit findings indicating control deficiencies

9.1.5 Emergence of new threats or masking technologies

9.2 The ISMS Manager shall lead the review in consultation with the DPO, Data Owners, IT Security, and Legal and Compliance. Updates must be version controlled, approved by Top Management, and communicated to all affected stakeholders.

10. Related Policies and Linkages

10.1 P13 - Data Classification and Labeling Policy. Masking and pseudonymization decisions depend directly on the classification of data fields and sensitivity levels defined in P13.

10.2 P14 - Data Retention and Disposal Policy. Transformed datasets must be retained and disposed of in accordance with the lifecycle rules set out in P14, ensuring that masked and pseudonymized data is treated as sensitive data.

10.3 P17 - Data Protection and Privacy Policy. Provides the privacy principles and regulatory basis for applying pseudonymization as a compliant processing activity under GDPR and similar legislation.

10.4 P22 - Logging and Monitoring Policy. Enables centralized audit logging and alerting for masking and pseudonymization events in accordance with structured security monitoring requirements.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1.3 - Risk Treatment Plan: Establishes masking and pseudonymization as risk treatment measures for reducing the identifiability of sensitive data in non-essential processing environments.

11.1.2 Clause 8.1 - Operational Planning and Control: Requires technical and procedural controls for secure data transformation during processing, storage, or transfer.

11.2 ISO/IEC 27002:2022

11.2.1 Controls 8.11, 8: Guidance on data masking and pseudonymization to minimize re-identification and data leakage risks.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protection of PII: Implementation of privacy-enhancing technologies such as masking and pseudonymization.

11.3.2 PT-2, PT-3: Minimization and Security of PII Processing - Transformation to reduce identifiability and enforce access control.

11.3.3 SC-12, SC-28, SC-30: Data Confidentiality and Integrity - Confidentiality and obfuscation controls for storage, transmission, and use.

11.4 EU GDPR (2016/679)

11.4.1 Article 4(5): Formal definition of pseudonymization.

11.4.2 Article 32: Security of Processing - Organizational and technical measures for pseudonymization.

11.4.3 Article 5(1)(c,f): Data minimization and confidentiality through pseudonymization and masking.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(c): Requires PETs such as masking and pseudonymization as security measures.

11.6 EU DORA (2022/2554)

11.6.1 Article 10(1): The ICT risk management framework includes masking and pseudonymization controls.

11.6.2 Article 10(2)(e): Requires the use of transformation technologies to protect personal and financial data.

11.7 COBIT 2019

11.7.1 DSS05.01: Protect Information Assets - Requirements for masking and pseudonymization.

11.7.2 DSS06.06: Secure Testing and Analytics - Masking in environments outside production.

11.7.3 MEA03: Compliance monitoring for the effectiveness of masking and pseudonymization.