					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**

Legal Notice (Copyright & Usage Restrictions)

(C) 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.
Unauthorized use is strictly prohibited and may lead to legal action.
For licensing, contact: info@clarysec.com

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 6.1.3, Clause 8	Information security risks and required controls, including masking and pseudonymization
ISO/IEC 27002:2022	Controls 8.11, 8.12	Guidance on masking and prevention of data leakage
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Data obfuscation and privacy-enhancing technologies
EU NIS2	Article 21(2)(c)	Proportionate technical measures, including pseudonymization as a control
EU DORA	Article 10(1)	ICT risk controls, including data transformation safeguards
COBIT 2019	DSS05.01, DSS06	Data protection and obfuscation/pseudonymization techniques
EU GDPR	Articles 4(5), 5(1)(c), 32	Data minimization and pseudonymization as a technical control

1. Purpose

1.1. This policy establishes mandatory requirements for the use of data masking and pseudonymization to protect sensitive, personal, and confidential data within small and medium-sized enterprises (SMEs).

1.2. These techniques are mandatory where live data is not required, including in development, analytics, and third-party service scenarios, in order to reduce the risk of exposure, misuse, or breach.

1.3. This policy directly supports compliance with ISO/IEC 27001:2022 certification requirements and applicable European regulatory obligations, including the GDPR, the NIS2 Directive, and the DORA Regulation.

1.4. By transforming data before it is used outside its original business context, the organization reduces exposure and strengthens its ability to demonstrate due diligence in privacy and information security.

2. Scope

2.1. This policy applies to all structured and 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 personnel, contractors, or third-party providers

2.2. This policy also applies to all data transformation tools, including masking, tokenization, and pseudonymization tools, whether open-source, commercial, or developed in-house.

2.3. Use cases covered by this policy include:

2.3.1. Preparation of test or development datasets

2.3.2. Export of data to analytics systems

2.3.3. Supplier or consultant access to operational systems

2.3.4. Data minimization measures to reduce processing risk

3. Objectives

3.1. Ensure that live personal or sensitive data is not exposed in lower-security environments where it is not essential.

3.2. Require masking or pseudonymization where real identifiers are not strictly necessary for the task.

3.3. Prevent unauthorized access to, or misuse of, data by enforcing transformation controls before data transfer or processing.

3.4. Ensure that all masking and pseudonymization processes are traceable, auditable, and implemented using approved tools.

3.5. Comply with applicable legal and regulatory requirements relating to data minimization, confidentiality, and data transformation safeguards.

4. Roles and Responsibilities

4.1. General Manager (GM)

4.1.1. Owns and approves this policy.

4.1.2. Ensures that all departments and providers comply with data transformation requirements.

4.1.3. Reviews exceptions, risk assessments, and transformation logs.

4.1.4. Coordinates legal, operational, or supplier-related actions in the event of violations.

4.2. IT Support Provider / Internal IT

4.2.1. Selects and manages masking and pseudonymization tools.

4.2.2. Ensures that appropriate transformation methods are applied based on data type.

4.2.3. Maintains logs of transformed datasets and key management procedures.

4.2.4. Ensures that masking is applied before use for testing, supplier access, or analytics.

[... 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 to ensure that it reflects:

9.1.1.1. Updates to applicable regulations, such as the GDPR and DORA.

9.1.1.2. New business systems or third-party data exchanges.

9.1.1.3. Feedback from audits or incidents involving the use of unmasked data.

9.2. Interim Reviews

9.2.1. Reviews must also be carried out when:

9.2.1.1. New applications or platforms that process sensitive data are introduced.

9.2.1.2. A major incident identifies gaps in current transformation controls.

9.2.1.3. Changes to classification levels affect data handling procedures.

9.3. Version Control and Change Management

9.3.1. All policy changes must be:

9.3.1.1. Approved by the GM and documented in a change log.

9.3.1.2. Clearly communicated to affected employees and service providers.

9.3.1.3. Archived securely, with access to obsolete versions restricted.

10. Related Policies and Linkages

10.1. This policy must be applied together with the following SME policies to ensure consistent and enforceable protection of sensitive data:

10.1.1. P13S – Data Classification and Labeling Policy: Defines the classification levels, such as "Confidential – Personal", that determine when masking or pseudonymization must be applied. This policy enforces transformation requirements based on data sensitivity levels.

10.1.2. P14S – Data Retention and Disposal Policy: Ensures that transformed datasets, including backups containing masked or pseudonymized data, are retained and disposed of in accordance with applicable requirements, including deletion of mapping keys when no longer required.

10.1.3. P17S – Data Protection and Privacy Policy: Aligns transformation practices with broader privacy obligations, including GDPR requirements for data minimization and the use of pseudonymization as a safeguard for personal data processing.

10.1.4. P30S – Incident Response Policy: Covers reporting and escalation procedures in the event of unauthorized data disclosure, including improper use of, or reversal of, masked or pseudonymized data.

10.1.5. P2S – Governance Roles & Responsibilities Policy: Assigns overall accountability for policy implementation, risk acceptance, and approval of exceptions, primarily to the General Manager.

10.2. These policies form an integrated data protection framework to ensure that masking and pseudonymization support ISO 27001 certification and cross-regulatory compliance.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 6.1.3: Requires treatment of information security risks, including reduction of exposure through data transformation techniques.

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

11.2. ISO/IEC 27002

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

11.2.2. Control 8.12: Provides measures to prevent data leakage through controlled transformation and access practices.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Helps ensure the confidentiality of information through data obfuscation.

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

11.3.3. PT-2/PT-3: Promote the use of privacy-enhancing technologies, including pseudonymization, when processing personally identifiable information.

11.4. EU GDPR

11.4.1. Article 4(5): Defines pseudonymization and requires controls over mapping keys and identifiers.

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

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

11.5. EU NIS2 Directive

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

11.6. EU DORA Regulation

11.6.1. Article 10(1): Requires ICT risk controls that include data transformation safeguards to maintain continuity and confidentiality during outsourcing and system development.

11.7. COBIT 2019

11.7.1. DSS05.01: Requires protection of information assets, including transformation where appropriate.

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