					Insert Registered Legal Entity Name Here							
Document number: P29S					Document Title: **Test Data and Test Environment 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	Clauses 6.1, 8	
ISO/IEC 27002:2022	Controls 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
EU GDPR	Articles 5(1)(c), 25, 32	
EU NIS2	Article 21(2)(e), (h)	
EU DORA	Article 9	
COBIT 2019	BAI07, DSS05	

1. Purpose

1.1 This policy defines how test data and test environments must be managed to prevent accidental exposure, data breaches, or operational disruption during testing activities.

1.2 It ensures that real customer data is never used inappropriately during software or system testing and that test environments are logically and technically segregated from production systems.

1.3 This policy is intended to support SMEs in meeting ISO/IEC 27001 certification requirements and applicable data protection obligations, while remaining practical and enforceable for organizations without a dedicated IT team.

2. Scope

2.1 This policy applies to:

2.1.1 All test environments (e.g., staging servers, sandbox environments, development testbeds)

2.1.2 All test data, whether manually created, generated, or derived from live data

2.1.3 All personnel involved in testing activities, including employees, contractors, freelancers, and IT service providers

2.1.4 Any testing that could affect customer-facing platforms, internal business systems, or third-party services

2.2 It covers both technical environments and processes used to support:

2.2.1 Website, application, and tool development

2.2.2 System upgrades, configuration testing, and integration testing

2.2.3 Automated and manual functional or security testing

3. Objectives

3.1 Prevent the use of real, identifiable customer data in testing unless it has been anonymized and explicitly approved.

3.2 Maintain strict segregation between test and production systems to prevent unintended data exposure or operational interference.

3.3 Protect test systems and test data from unauthorized access, accidental disclosure, or reuse across environments without appropriate controls.

3.4 Comply with applicable data protection requirements (e.g., GDPR, NIS2) by ensuring all test data is processed lawfully, fairly, and securely.

3.5 Support the organization's readiness for external audits and ISO/IEC 27001 certification by documenting testing practices and enforcing consistent safeguards.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Has overall accountability for test data protection and test system security.

4.1.2 Approves any use of real data in testing after confirming that appropriate safeguards (e.g., anonymization or masking) are in place.

4.1.3 Verifies that testing activities are properly documented and comply with this policy.

4.2 Project Owner

4.2.1 Coordinates the design and execution of testing processes.

4.2.2 Ensures that all team members understand and comply with this policy.

4.2.3 Confirms that test systems are securely configured before testing begins.

4.2.4 Reports any incidents involving test environments or data leakage to the GM.

[... 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 Scheduled Reviews

9.1.1 This policy must be reviewed at least annually by the General Manager (GM). The review must confirm that the policy remains current with:

9.1.1.1 Changes in software development tools, platforms, or environments

9.1.1.2 Updated legal obligations, including data protection or digital operational resilience requirements

9.1.1.3 SME certification and audit readiness under ISO/IEC 27001

9.2 Trigger Events for Interim Review

9.2.1 Additional reviews must take place following:

9.2.1.1 Any incident involving data exposure or compromise in test environments

9.2.1.2 Any use of real data in testing, even if anonymized

9.2.1.3 The introduction of new testing methods, systems, or vendors

9.2.1.4 Regulatory changes affecting how data is handled during testing

9.3 Change Management and Communication

9.3.1 The GM is responsible for:

9.3.1.1 Updating this policy and documenting all revisions in the version history

9.3.1.2 Notifying staff, developers, and relevant service providers of updates

9.3.1.3 Confirming that all personnel involved in testing understand and apply the latest requirements

9.3.1.4 Maintaining an accessible current version of the policy for review and audit purposes

9.4 Audit and Documentation

9.4.1 Records of all policy reviews, approvals for the use of real data, and any exception justifications must be:

9.4.1.1 Retained securely for audit purposes

9.4.1.2 Made available upon request during internal or third-party audits

9.4.1.3 Reviewed annually to ensure consistency with testing practices

10. Related Policies and Linkages

10.1 This policy must be applied in conjunction with the following SME policies to maintain security and compliance during testing:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Defines accountability for oversight of development, testing, and system segregation responsibilities.

10.1.2 P4S – Access Control Policy: Governs the assignment, management, and removal of access credentials for test systems.

10.1.3 P8S – Information Security Awareness and Training Policy: Ensures that staff understand test data risks, secure handling practices, and the proper segregation of environments.

10.1.4 P13S – Data Classification and Labeling Policy: Supports clear classification of test data and guides anonymization or masking approaches.

10.1.5 P17S – Data Protection and Privacy Policy: Aligns with GDPR obligations, including safeguards for processing and storing personal data, including in test environments.

10.1.6 P24S – Secure Development Policy: Defines overarching security expectations for development teams, including the secure use of data during testing phases.

10.1.7 P30S – Incident Response Policy: Defines how to respond to any breach or issue identified in a test environment or caused by improper handling of test data.

10.2 These policies form a unified security framework to support test integrity, data minimization, and full alignment with ISO/IEC 27001 across development and QA activities.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Requires risk assessment and risk treatment actions, including those relating to testing risks.

11.1.2 Clause 8.1 – Requires the planning and control of operational processes, including the setup of test environments.

11.2 ISO/IEC 27002

11.2.1 Control 8.28 – Requires organizations to protect test data and ensure that it does not contain sensitive data or live production data.

11.2.2 Control 8.29 – Requires clear segregation of development, test, and production environments.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Covers control requirements for development and testing.

11.3.2 SA-12 – Addresses supply chain testing risks and security evaluations.

11.3.3 SC-32 – Requires environment segregation and controls to protect the confidentiality and integrity of test data.

11.4 EU General Data Protection Regulation (GDPR)

11.4.1 Article 5(1)(c) – Requires data minimization, including the use only of data necessary for testing.

11.4.2 Article 25 – Requires data protection by design, including controls for test environments.

11.4.3 Article 32 – Requires secure processing of personal data in all systems, including non-production environments.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(e), (h) – Requires secure development and system testing, particularly where digital services are exposed to cyber risk.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – Emphasizes the importance of digital operational resilience, including secure testing of ICT systems by SMEs in the financial sector.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: Includes testing controls to validate new systems and data handling practices.

11.7.2 DSS05 – Manage Security Services: Requires test and development practices that prevent misuse or exposure of business data.