					Insert Registered Legal Entity Name Here							
Document number: P29					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	Clause 8	Relevant to secure planning and control of test data and environments
ISO/IEC 27002:2022	Controls 8.28–8.29	Covers secure test data and protection of test environments
NIST SP 800-53 Rev. 5	SA-11, SC-28, SC-32	Addresses developer testing and evaluation, protection of data at rest, and integrity
EU GDPR	Articles 5, 25, 32	Covers data minimization, privacy by design, and security of processing in test contexts
EU NIS2	Article 21(2)(e), (h)	Relates to secure development and testing practices
EU DORA	Article 9	Pertains to ICT systems and protocols and the security of test data
COBIT 2019	DSS05, BAI07	Addresses managed security services and change acceptance and transition

1. Purpose

1.1. This policy defines the mandatory requirements for managing test environments and test data to ensure security, confidentiality, and operational integrity throughout the software development and testing lifecycle.

1.2. It is intended to prevent unauthorized access, data leakage, and contamination of production systems caused by improperly managed test environments or the use of live data in testing.

1.3. This policy mandates the secure handling of data used for testing, the hardening of test infrastructure, and role-based access controls (RBAC), while ensuring alignment with applicable regulatory and contractual obligations.

2. Scope

2.1. This policy applies to all test environments, data, tools, and processes used for software, system, application, and IT infrastructure testing across the organization.

2.2. It covers:

2.2.1. Test environments provisioned on premises, in the cloud, or through third-party platforms

2.2.2. Test data used in functional, performance, regression, and security testing

2.2.3. Manual, scripted, or automated testing (e.g., CI/CD pipelines)

2.2.4. All personnel involved in testing, including internal teams, vendors, and contractors

2.3. This policy applies regardless of system criticality, application type, or whether development is performed internally or outsourced.

3. Objectives

3.1. To prevent the use of live, sensitive, or regulated data (e.g., personally identifiable information (PII), cardholder data) in test environments unless anonymization has been applied or specific approval has been obtained.

3.2. To ensure complete network and access segregation between test and production environments to prevent unauthorized data access or contamination of production systems.

3.3. To require encryption, data masking, or synthetic data generation when representative data is needed for testing purposes.

3.4. To reduce the likelihood of compliance failures, customer data exposure, or operational disruption arising from insecure test data or test environments.

3.5. To align test data handling with industry standards (ISO, NIST, COBIT) and regulations such as GDPR, NIS2, and DORA.

4. Roles and Responsibilities

4.1. Chief Information Security Officer (CISO)

4.1.1. Owns this policy and enforces technical and administrative safeguards for test data and test environments.

4.1.2. Approves the use of real or sensitive data in testing where appropriate justification and compensating controls are in place.

4.2. QA/Test Leads

4.2.1. Coordinate test planning and ensure that all testing activities comply with the requirements of this policy.

4.2.2. Validate appropriate segregation, access controls, and data preparation for each testing phase.

[... 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 must be reviewed annually and updated as necessary to reflect:

9.1.1. Changes in regulatory requirements (e.g., GDPR, DORA, NIS2)

9.1.2. Adoption of new testing tools, platforms, or automation pipelines

9.1.3. Internal audit findings or post-incident recommendations

9.1.4. Expansion of development or QA processes that changes test data handling or environment usage

9.2. The CISO is accountable for initiating the review in collaboration with:

9.2.1. QA/Test Leads

9.2.2. DevOps and Infrastructure Managers

9.2.3. Application Development Teams

9.2.4. Data Protection Officer (DPO) and Legal Counsel

9.3. All revisions must be:

9.3.1. Version-controlled and stored in the central document repository

9.3.2. Communicated to affected personnel through formal channels (e.g., ISMS notifications, team briefings)

9.3.3. Linked to updates in associated technical standards, controls, and operating procedures

9.4. Trigger-based interim reviews must be conducted immediately following any:

9.4.1. Data leakage or breach involving test environments

9.4.2. Audit nonconformity related to test data handling

9.4.3. Significant changes in legal obligations or IT architecture

10. Related Policies and Linkages

10.1. This policy is closely integrated with the following policies to ensure the secure and compliant handling of test data and test environments:

10.1.1. P1 – Information Security Policy: Establishes the overarching security principles governing test data protection and test environment management.

10.1.2. P5 – Change Management Policy: Applies to the creation, modification, and decommissioning of test environments and deployment pipelines.

10.1.3. P13 – Data Classification and Labeling Policy: Guides test data selection and the application of sensitivity-based controls.

10.1.4. P14 – Data Retention and Disposal Policy: Defines retention periods and secure deletion requirements for test datasets.

10.1.5. P15 – Backup and Restore Policy: Mandates backup practices and recovery validation for test environments.

10.1.6. P18 – Cryptographic Controls Policy: Specifies mandatory encryption standards for data at rest and in transit within test platforms.

10.1.7. P22 – Logging and Monitoring Policy: Governs visibility and anomaly detection for activity within test environments.

10.1.8. P30 – Incident Response Policy: Defines escalation and remediation requirements for breaches or incidents involving test systems.

10.1.9. P33 – Audit and Compliance Monitoring Policy: Supports validation of policy adherence and ongoing assurance.

11. Reference Standards and Frameworks

11.1. This policy aligns with global cybersecurity standards and regulatory frameworks that require the secure handling of test data and the protection of non-production environments.

11.2. ISO/IEC 27001:

11.2.1. Clause 8.1 - Requires secure planning and control of test data and test environments.

11.3. ISO/IEC 27002:2022 – Controls 8.28–8.29:

11.3.1. Annex A Control 8.28 – Secure Test Data: Requires protection of test data used in development and testing through anonymization, data masking, or synthetic data generation.

11.3.2. Annex A Control 8.29 – Protection of Test Environments: Requires segregation from production, access controls, and environment hardening for test systems.

11.3.3. These controls define requirements for securely managing data used during testing and protecting non-production systems from misuse, compromise, or contamination.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – Developer Testing and Evaluation: Establishes expectations for secure, repeatable testing procedures with appropriate data controls.

11.4.2. SC-28 – Protection of Information at Rest: Aligns with encryption requirements for test data stored in non-production systems.

11.4.3. SC-32 – Information Integrity: Supports data validation, corruption prevention, and input/output controls during testing.

11.5. EU GDPR (2016/679):

11.5.1. Article 5 – Data Minimization: Prohibits unnecessary use of personal data in testing.

11.5.2. Article 25 – Privacy by Design: Requires data protection techniques to be applied from the outset of the development and testing lifecycle.

11.5.3. Article 32 – Security of Processing: Requires safeguards for test environments handling personal or sensitive data.

11.6. EU NIS2 Directive (2022/2555):

11.6.1. Article 21(2)(e), (h): Requires secure development and testing processes, with emphasis on protection against unauthorized access and data leakage.

11.7. EU DORA (2022/2554):

11.7.1. Article 9 – ICT Systems and Protocols: Requires testing processes to support ICT resilience and protect operational data from compromise or unauthorized disclosure.

11.8. COBIT 2019:

11.8.1. DSS05 – Manage Security Services: Supports enforcement of security policies across all environments, including non-production environments.

11.8.2. BAI07 – Manage Change Acceptance and Transition: Covers the formal transition process from testing to production, including data and environment controls.