| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | [Insert Registered Legal Entity Name Here] | | | | | | | |
| Document number:<br>P29S | | | | | Document Title:<br>**Test Data and Test Environment Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>01.01.2025 | | | Document Owner:<br>IT | | | | | | | |
| 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 | Clauses 6.1, 8.1 | |
| 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 | |

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:<br>P29S</td><td colspan="9">Document Title:<br>Test Data and Test Environment Policy</td></tr>
<tr><td colspan="2">Version:<br>1.0</td><td colspan="2">Effective Date:<br>01.01.2025</td><td colspan="9">Document Owner:<br>IT</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy defines how test data and test environments must be managed to prevent accidental exposure, data breaches, or operational disruptions during testing activities.
   1.2. It ensures that real customer data is never improperly used during software or system testing and that test environments are logically and technically separated from production systems.
   1.3. The policy is designed to help SMEs comply with ISO/IEC 27001 certification requirements and relevant data protection laws, 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 systems, 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 providers
      2.1.4. Any testing that could impact 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 tests
3. **Objectives**
   3.1. Prevent the use of real, identifiable customer data in testing unless anonymized and explicitly approved.
   3.2. Maintain strict separation between test and production systems to avoid unintended data exposure or operational interference.
   3.3. Protect test systems and data from unauthorized access, accidental disclosure, or reuse across environments without appropriate controls.
   3.4. Comply with relevant data protection regulations (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 appropriate safeguards (e.g., anonymization or masking).
      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 all team members understand and follow this policy.

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

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

4.3. **Developer / IT Provider**

4.3.1. Implements and maintains isolated test environments with no access to live systems unless explicitly required.

[.....]

**Reference Standards and Frameworks**

**ISO/IEC 27001:2022**

**Clause 6.1** – Requires risk assessment and treatment actions, including testing-related risks.

**Clause 8.1** – Demands planning and control of operational processes, including test system setup.

environments.

**ISO/IEC 27002:2022**

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

**Control 8.29** – Mandates clear separation of development, test, and production

**NIST SP 800-53 Rev.5**

**SA-11** – Covers development and testing control expectations.

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

**SC-32** – Requires separation of environments and protections for test data confidentiality and integrity.

**EU General Data Protection Regulation (GDPR)**

**Article 5(1)(c)** – Calls for data minimization, including use only of necessary data for testing.

**Article 25** – Requires data protection by design, which includes test environment controls.

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

**EU NIS2 Directive (2022/2555)**

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

**EU DORA (2022/2554)**

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

**COBIT 2019**

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

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