

Security Policy

System development

Information Security

|  |  |
| --- | --- |
|  |  |
| System development |  |
| Number | [Number] |
| Issued on | 04.07.2022 |
| Through | Chief Information Security Officer |
| Entry into force | 04.07.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Compliance |
| Responsible function | Information security |
| Responsible person | Dirk Franken |
| Overriding regulation | Information security policy |
| Replaces | n/a |
| Applicable documents |  |
| Validity | Until further notice |
| Last | 14.07.2025 |
| Next review | 07.01.2026 |
| Publication | SÜDVERS Intranet |
| Classification | Internal |
| Archive | Document management system |
| Organizational system | [Organizational system] |
| Languages |  |
| Formats |  |
| Remarks |  |

Table of contents

[1 Principle 4](#_Toc188346241)

[2 Objective 4](#_Toc188346242)

[3 Controls 4](#_Toc188346243)

[3.1 System development environment 4](#_Toc188346244)

[3.2 Acquisition of software 4](#_Toc188346245)

[3.3 Outsourced system development 6](#_Toc188346246)

[3.4 System test 7](#_Toc188346247)

[3.5 Security check 7](#_Toc188346248)

[3.6 Requirements for transfer to the production environment 7](#_Toc188346249)

[3.7 Requirements for the installation 8](#_Toc188346250)

[3.8 Decommissioning 9](#_Toc188346251)

# Principle

System development activities must be carried out in development environments that are separate from the live and test environments and protected from unauthorized access.

Systems under development (including application software packages, system software, hardware, communications and services) should be tested in a dedicated test area that simulates the live environment before the system is moved to the live environment.

# Objective

Providing a secure environment for system development activities and avoiding interruptions to business activities.

Ensure that systems function as intended, meet predefined security requirements and do not compromise information security

# Controls

## System development environment

Two or more system development environments (e.g. a dedicated network or a dedicated group of information systems) must be set up in which development and testing activities can be carried out.

Development and test environments must be isolated from live environments and from each other. The following points must be taken into account as a minimum:

* an appropriate separation of development and production systems and their operation in different domains (e.g. in separate virtual or physical environments); the following is considered "appropriate" for the respective criticality levels (according to BIA):
  + up to level "low": logical separation of systems and data, use of the same AD domain
  + up to level "medium": requirements of level "low" plus separation of the AD domains and logical separation of the network segments used
  + Level "high": Requirements of level "medium" and plus separation of physical environments (end user, server and network)
* Definition, documentation and implementation of rules and approvals for the use of software from development to production status;
* Testing of changes to IT systems and applications in a test or staging environment before they are applied to production systems;
* no tests in production environments;
* the display of suitable environment labels in the menus to reduce the risk of errors;
* No copying of sensitive information into the development and test system environment.

## Acquisition of software

There must be documented standards/procedures for the procurement of software (or systems) that specify the following:

* Guidelines for the selection of software (e.g. lists of approved providers, security considerations and contractual conditions)
* Methods for detecting and eliminating security vulnerabilities in software
* a procedure for the review and approval of software prior to purchase
* Documentation of the software in a software
* the need to meet software licensing requirements.

The standards/procedures must apply to all software purchased from SÜDVERS, including

* Operating systems and virtualization software
* software
* services
* commercially available software
* software

Software is a must:

* Acquired from approved suppliers (e.g. purchased or leased)
* be tested before use to identify and security vulnerabilities
* are covered by appropriate support and maintenance contracts.

When purchasing software:

* the safety requirements should be determined
* Suppliers should ensure that they can meet the safety requirements.
* Reliability should be given high priority in the selection process.
* The contractual conditions must be agreed with the suppliers.

The software licensing requirements must be met by acquiring appropriate licenses for the planned use and by providing proof of ownership of the software.

The acquisition of software must:

* checked by persons who have the necessary knowledge and skills to determine the extent to which the software meets the safety requirements
* be approved by the heads of the relevant specialist department (functional and budget)
* be approved by the Head of IT (compatibility and interoperability with existing environment)
* be documented in one or more registers.

The registers must contain important details about the purchased software, including

* a clear description of the software used (e.g. using serial numbers, network address(es) or product numbers)
* Versions of the hardware and software used (including patch levels)
* the location where the software is installed (e.g. on mobile devices and servers)
* Licensing information (such as license key and proof of ownership).

Registers containing details of software must be regularly reviewed by relevant IT staff to identify any discrepancies with software licenses. Any unlicensed or unauthorized software identified must be investigated and remedied (e.g. by purchasing new licenses, removing unlicensed software or renegotiating contracts).

The accuracy of the details recorded in the register via the software should be supported by the use of automatic detection/mapping tools used for this purpose:

* To detect discrepancies in the register
* detect the introduction of unauthorized software
* detect the illegal use of software (e.g. no license).

## Outsourced system development

Where system development is outsourced, SÜDVERS shall communicate and agree requirements and expectations and continuously monitor and verify that the delivery of the outsourced work meets these expectations. The following points should be considered throughout the external supply chain:

* Licensing agreements, ownership of code and intellectual property rights in relation to the outsourced content;
* contractual requirements regarding safe design, programming and verification practices;
* Provision of the threat model for consideration by external developers;
* Acceptance test regarding the quality and accuracy of the services provided;
* Proof that an acceptable minimum level of security and data protection is provided (e.g. trustworthiness reports);
* Proof that sufficient checks have been carried out to exclude the presence of malicious content (both intentional and unintentional) at the time of delivery;
* Submission of evidence that sufficient checks have been carried out to rule out the existence of known vulnerabilities;
* Escrow agreements for the software source code (e.g. if the supplier ceases to do business);
* contractual right to review the development processes and measures;
* Security requirements for the development environment;
* Compliance with the applicable legal provisions (e.g. on the protection of personal data).

## System test

Sensitive business information (such as customer data, medical data, product prices ...) used for testing purposes must be protected by:

* the prohibition of the use of personal data (i.e. information that can be used to identify an individual person) as part of the review process. Exceptions must be requested from the data protection officer and, if approved, documented accordingly.
* Data masking to hide real information (e.g. through pseudonymization, data obfuscation, data de-identification or data encryption)
* Require separate authorization for each copying of business information from the live environment to the test environment
* Restricting access to business information in the test environment
* Logging the use of business information
* the secure destruction of copies of business information once testing has been completed.

## Security check

The systems must be tested to determine the effectiveness of the security controls, including:

* Vulnerability assessments (to identify vulnerabilities in software and security controls)
* Penetration tests (e.g. black box, white box or grey box tests to simulate attacks that show how vulnerabilities can be exploited)

A procedure must be in place to ensure that any errors or vulnerabilities identified during the testing process are fixed in a consistent manner, including

* Recording details of any safety deficiencies found (e.g. in a test report or on a test results sheet)
* the assessment of the associated risks
* Implementation of measures to manage these risks
* Repeat the tests of the systems after the remedial measures.

## Requirements for transfer to the production environment

Strict and documented acceptance criteria should be met before new systems go live.

Before new systems go live, implementation specialists and business managers must carry out checks to ensure that:

* security and information risk assessments have been carried out.
* residual risks are documented.
* the approval of a responsible head of department has been obtained
* Service Level Agreements (SLAs) were defined to support the systems in the live environment.

Checks must be carried out to ensure that:

* performance and capacity requirements can be met
* all necessary patches and updates have been tested and successfully applied
* all remaining technical safety gaps do not exceed the approved threshold values
* that there are no adverse effects on existing systems
* the security of the new systems can be continuously supported
* precautions have been taken in the event that the new systems do not function as intended.

Before new systems have to be transferred to the live environment:

* Procedures for troubleshooting and restarting are defined
* contingency plans and arrangements (e.g. as part of business continuity or disaster recovery) are developed or updated
* Operating procedures are documented and tested
* users are trained and educated to use the systems correctly and safely
* IT specialists (e.g. helpdesk staff/system administrators) are trained in how to operate systems correctly and apply the necessary security controls effectively.

Precautions must be taken to ensure that only tested and approved versions of hardware and software are introduced into the live environment.

## Requirements for the installation

The installation of new systems must be planned in advance and approved by a responsible department head and the CAB (or equivalent) to avoid disruption to the running environment.

The systems may only be installed in live environments, provided that these:

* be supported by a robust and reliable technical infrastructure that uses standard security management procedures (such as system hardening, patch management, malware protection and access control)
* are protected by a minimum level of standardized security management practices (e.g. access control, malware protection, patch management, security event analysis and incident management)
* are subject to a change management process.

The installation of new systems in live environments must:

* be regulated by a documented installation process (or deployment plan)
* restricted to a limited number of authorized persons
* be carried out from approved locations.

The installation process must include the necessary technical activities, including

* integration into the technical security infrastructure of

Sufficient tests must be carried out during installation in order to:

* check the functionality of the system (e.g. whether users can log in and all menus work as expected)
* confirm that the system works as expected in the live environment
* check whether the security controls are functioning as intended
* ensure that the fallback arrangements work if necessary.

The installation process should cover the required user-related activities, which include the following:

* Provision of new or revised documents
* Informing the persons involved about their tasks and responsibilities
* Raising users' awareness of their responsibility when using new systems safely
* constant technical support (e.g. via electronic help screens, a telephone helpdesk or a hotline)
* Implementation of new or revised standards/procedures
* Transfer of responsibility to people who operate the live environment.

The installation process should include other necessary activities, such as

* the elimination of old software, procedures and documentation
* Precautions in the event of a system failure
* Record installation activity, highlighting details of unexpected conditions, ad hoc changes to the system and security issues
* the archiving of previous software versions together with the corresponding information (including configuration settings, operating procedures and supporting software).

## Decommissioning

Systems that are no longer required (sometimes referred to as redundant or obsolete systems) that may need to be decommissioned should be identified.

Where a decision has been made to decommission a system, it should be subject to a documented, approved decommissioning process that includes the following:

* Identification of the type, classification and location of all information, software, services, devices and equipment associated with the system
* Carrying out a risk assessment
* Migration, archiving or destruction of information
* Uninstalling or removing certain software and services
* the safe disposal of appliances and systems.

A review should be carried out to ensure that all aspects of the decommissioning process have been satisfactorily completed.