

Security Policy   
Business Applikation

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Security Policy Business Applications | |  |
| 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 review | 25.06.2025 | |
| 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 Register for business applications 4](#_Toc107316296)

[1.1 Principle 4](#_Toc107316297)

[1.2 Objective 4](#_Toc107316298)

[1.3 Controls 4](#_Toc107316299)

[2 Protection of business applications 6](#_Toc107316300)

[2.1 Principle 6](#_Toc107316301)

[2.2 Objective 6](#_Toc107316302)

[2.3 Controls 6](#_Toc107316303)

[3 Browser-based application protection 8](#_Toc107316304)

[3.1 Principle 8](#_Toc107316305)

[3.2 Objective 8](#_Toc107316306)

[3.3 Controls 8](#_Toc107316307)

[4 Validation of information 11](#_Toc107316308)

[4.1 Principle 11](#_Toc107316309)

[4.2 Objective 11](#_Toc107316310)

[**4.3** Controls 11](#_Toc107316311)

# Register for business applications

## Principle

Business applications must be recorded in an accurate and up-to-date software register.

## Objective

To document important information about business applications

## Controls

Details of business applications must be recorded in a software register or an equivalent register.

Business application registries should cover different types of business applications, including those delivered over the Internet:

* Business applications
* commercially available software (COTS)
* Cloud-based applications
* mobile technology (sometimes also referred to as mobile apps)
* End-user developed applications (EUDA), such as those created with spreadsheet or desktop database programs.

Business application registers should contain operational details about each application, including:

* Business purpose
* Business processes supported by the application
* Degree of criticality for SÜDVERS (e.g. by classifying applications as critical, important or standard)
* Business owner.

The business application registers should contain details of the users of each application, including the:

* Number and type of users (e.g. business users or IT specialists)
* Type and scope of connections
* Methods of user authentication (e.g. password, token or biometric).

Business applications registers must contain details of the information processed by each application, including the extent to which it is processed:

* personal data, also referred to as personally identifiable data (e.g. name, telephone number, e-mail address or postal address)
* sensitive personal data, also known as special categories (such as race, ethnicity, political opinion, health, genetics or trade union membership).

Business application registers should contain technical details about each application, including:

* Application version
* Supplier and approval requirements
* Contact persons at the technical contact points (e.g. IT specialists who provide application support).

The business application registers should be used for support:

* Support for information risk assessments
* Comparison of the relative risks between different applications
* Coordination with emergency management and business continuity planning
* identify inadmissible applications.

Registers for enterprise applications must be:

* kept up to date
* are regularly checked for accuracy (e.g. to ensure that the content is complete, comprehensive, correct and timely)
* be signed off by a responsible manager.

# Protection of business applications

## Principle

Business applications must be protected by applying proven security architecture principles.

## Objective

To ensure that business applications use consistent security features, comply with SÜDVERS' technical security infrastructure and protect the information they process.

## Controls

Business applications must be protected from invalid connections by:

* the assumption is made that entries from external systems (e.g. web services) are insecure by default
* Checking the access rights for a request to an object (e.g. a database entry, a file or similar)
* Repeating any client validation when connecting to the server to protect against man-in-the-middle attacks.

Business applications must be protected against unauthorized access to information by:

* Hardening of the operating system
* The Defense in Depth concept is applied (e.g. multiple layers of different types of protection) to avoid dependence on one type or method of security control
* secure default settings (e.g. requiring authentication and recording user activity in an event log as a preselected option) are used

Business applications must protect against unauthorized disclosure of sensitive information by ensuring that they:

* run with the least possible rights
* Use separation of privileges (e.g. by splitting the application functions and cryptographic keys)
* prevent unwanted network connections to the Internet or to untrusted networks (e.g. by configuring servers, setting rules in a firewall or using proxy servers)
* prevent information about the internal functioning of applications (e.g. in application responses, error messages or developer comments (especially in HTML and JavaScript-based applications)) from being disclosed.

Business applications must contain security controls to ensure the availability of information:

* Provision of sufficient capacity to cope with the normal/peak workload
* Carrying out load balancing and load monitoring
* Reduction or elimination of individual sources of error.

Servers that support critical business applications or services (such as DNS, file, print, database and email):

* must be separated from other productive networks (e.g. internal office network and untrusted networks) (e.g. by placing them in a special physical network or a virtual local area network (VLAN))
* run on one or more separate and dedicated physical computers or virtual servers (so that they do not provide other services such as file, print, database, email or other business applications).

If there are connections between servers (e.g. web servers) and back-office systems (e.g. application and database servers):

* these are protected by firewalls
* limits the connections to the services required for business applications
* are realized on the basis of documented, tested and approved application programming interfaces (APIs)
* encrypted (e.g. with Transport Layer Security (TLS), IPsec or equivalent).

# Browser-based application protection

## Principle

Procedural and technical controls must be applied to browser-based applications and the servers on which they run.

## Objective

To ensure that the increased risks associated with browser-based applications are minimized

## Controls

When using browser-based applications and supporting systems, additional security controls must be implemented to protect against the increased risks associated with access via unprotected networks (such as the Internet).

Information used by browser-based applications (e.g. configuration files) must be protected against damage or unauthorized disclosure.

Website content (such as web pages, articles and images) must be protected from falsification or unauthorized disclosure:

* The data must be stored separately from the operating system (e.g. on a separate partition/hard disk)
* Set strict file permissions (least privilege)
* the restriction of updates to a limited number of authorized persons (e.g. website authors or website administrators)
* Use of approved, secure methods for installing updates
* Checking the content to ensure that it is correct (e.g. that hyperlinks are valid and functional and that no vulnerabilities have been introduced by scripts or hidden form fields)
* regular checks to ensure that the content of the website is not inappropriate (e.g. defamatory, offensive or in breach of legal and regulatory requirements).

Sensitive information must be protected against unauthorized disclosure during transmission (e.g. between the web server and the user's web browser) by using protective measures:

* Encryption (e.g. with Transport Layer Security (TLS) or equivalent)
* using TLS (Transport Layer Security) certificates obtained from a reputable, approved internal or external (e.g. public) certification authority.

Unauthorized disclosure of system configuration information (which could be useful to attackers) must be prevented by applying appropriate measures that include at least the following:

* Suppression or modification of the server field in the HTTP headers that specify the brand and version of the web server
* Verification that transaction areas and directories of files on web servers are not indexable (i.e. files are not accessible to search engines, web crawlers or similar indexing systems)
* Preventing the source code of server-side executable files and scripts from being viewed by a web browser
* Ensuring that the source code of programs such as HTML, JavaScript and other client-side scripting languages does not contain any unnecessary information (e.g. comments and details of functions).

Web application sessions must be protected from being hijacked or cloned by others:

* Ensure that session IDs cannot be easily predicted (e.g. by using randomly generated session IDs)
* the encryption of network traffic between the web browser and the web server.

Web servers that go to the Internet and support business applications must be configured so that they:

* Record actions performed
* log security-related events generated by the website.

There should be a procedure to ensure this:

* important domain name registrations are regularly checked and renewed (e.g. every two years)
* Details of web servers with internet access are recorded in a register (or equivalent) containing details of the hosting location, IP address(es), domain name(s) and digital certificates used.
* SÜDVERS registers domain names that could be used to impersonate SÜDVERS (e.g. to prevent phishing attacks)
* Websites that may have been set up under domain names similar to those used by SÜDVERS are monitored (e.g. by third party monitoring services).
* illegal websites (e.g. those used for phishing attacks) are closed as quickly as possible.

Relationships with the individual Internet service providers (ISPs) or equivalent facilities should be regulated by a service level agreement (SLA).

# Validation of information

## Principle

Business applications must contain security controls that protect the confidentiality and integrity of information as it is entered into, processed by, and output from these applications.

## Objective

Protecting the integrity (validity, accuracy, completeness and timeliness) of important information stored in or processed by business applications.

## Controls

The information entered in business applications must be checked for accuracy:

* Validity
* Completeness

The integrity of information processed by business applications must be maintained by ensuring that

* information cannot be accidentally overwritten (e.g. by write-protecting key fields or files)
* Changes to important static business information such as customer master data or exchange rates are checked (e.g. by inspecting the content of data records before and after the change)
* unauthorized or incorrect changes to information are detected (e.g. by inspecting change logs, using automatic checksum tools or comparing the data with its original source).