

Security Policy   
Event Logging

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Event Logging | |  |
| 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 Content

[1 Principle 4](#_Toc187920874)

[2 Objective 4](#_Toc187920875)

[3 Controls 4](#_Toc187920876)

# Principle

Important security-relevant events must be recorded in logs, stored centrally, protected against unauthorized changes and analyzed regularly.

# Objective

Detecting threats that could lead to an information security incident, maintaining the integrity of critical security-related information and supporting forensic investigations.

# Controls

The logging of security events (including the recording of user activities, exceptions, errors and information security events) must be created, stored and regularly checked on all systems in accordance with the manufacturer's recommendations.

The IT systems must be configured in such a way that:

* These enable the logging of events (using a standard format such as syslog, MITRE Common Event Expression or equivalent)
* generate suitable event types (e.g. creation of a service, system crash, deletion of an object and failed login attempt)
* include relevant event attributes in the event entries (e.g. IP address, user name, time and date, protocol used, port accessed, connection method and name of the device)

For IT systems that are directly or indirectly connected to external partners, a common and agreed time standard must be used and the integrity and availability of the time service must be guaranteed.

The security-relevant event logging must:

* be activated at all times
* be protected against unauthorized access and accidental or intentional modification/overwriting

The event log must, where technically applicable, include at least the following for each event:

* User IDs;
* System activities;
* Date, time and details of relevant events (e.g. login and logout);
* Device ID, system ID and location;
* Network addresses and protocols.

At least the following events must be taken into account for logging:

* Successful and rejected system access attempts;
* successful and rejected attempts to access data, records or other resources;
* successful and rejected attempts to access websites or other external IT systems;
* Changes to the system configuration;
* Use of privileges;
* Use of utilities and applications;
* Files or data records that have been accessed and the type of access, including the deletion of important files;
* Alarms triggered by the access control system;
* Activation and deactivation of security systems such as anti-virus systems and IDS;
* Creation, modification or deletion of identities;
* Transactions carried out by users in applications.

Mechanisms must be put in place to ensure that:

* Sufficient disk space is allocated based on the expected volume of event information
* when a maximum size of event logs is reached, the system is not stopped due to lack of memory, thus ensuring that logging continues without interruption

Security-relevant event logs must:

* be checked regularly (at least daily)
* are regularly archived and digitally signed before storage
* be stored securely and tamper-proof so that all evidence derived from it can be proven. This is particularly important in any kind of legal proceedings relating to evidence from the log data.

Security-relevant events (stored in event logs) must be stored in a central IT system.

The logging of security-relevant events must be checked to ensure that the logging functions as intended and has not been manipulated.

The ITSM process for logging security events must include at least the following

* the identification of IT systems or devices on which event logging must be activated (e.g. business-critical applications and systems where a major information security incident has occurred or systems that are subject to legal or regulatory obligations) in order to identify security-related events
* the configuration of systems or devices to generate security-related events (including event types such as user login attempts, service creation, system crashes and user account creation, modification or deletion) and event attributes associated with each event (e.g. date, time, source and destination IP addresses and user ID)
* the storage of security-relevant events in event logs (e.g. on local systems, central servers or by using the storage provided by an external service provider)
* the protection of security-relevant event logs (e.g. through encryption, access control and data backup)
* the retention of security-relevant event logs (e.g. to fulfill retention obligations and to support possible forensic investigations)
* the access rules to the generated event logs.