

Security Policy   
Collaboration Platforms

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Directive Collaboration platforms | |  |
| 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 Principle 4](#_Toc108432485)

[2 Objective 4](#_Toc108432486)

[3 Controls 4](#_Toc108432487)

Collaboration platforms are a category of business software that extends work processes with comprehensive social networking functions. Types of collaboration platforms include online communication (e.g. instant messaging and conferencing services), online office, social networks, project management and file sharing software.

# Principle

Collaboration platforms need to be protected by establishing management policies, using application controls, configuring the security settings of each platform and improving the security of the supporting technical infrastructure.

# Objective

Ensure that collaboration platforms are available when needed, that the confidentiality and integrity of information is protected during transmission and that the risk of misuse is minimized.

# Controls

The use of collaboration platforms and their provision within the framework of ITSM Service Configuration Management as approved IT services for SÜDVERS requires the approval of the Head of IT for each platform in order to ensure compliance with legal and contractual requirements, technical feasibility and conformity with the company's IT strategy.

IT must have documented standards/procedures for collaboration platforms that include the following

* the configuration of the security settings
* Ensuring the security of content processed by collaboration platforms
* Improving the security of the technical infrastructure to support collaboration platforms
* Protection of conference services against unauthorized access.

The security of collaboration platforms must be improved by:

* Purchase and use only of approved platforms
* Assessment of the information risks of each platform that is acquired or used
* Processes for adding, updating and deleting user profiles (e.g. when hiring new employees or changing their tasks)
* Raising user awareness of the safe use of these platforms (e.g. through an acceptable use policy for employees or a code of conduct for external users).

Collaboration platforms must be configured in such a way that they function securely by:

* These require authentication before users are granted access to the platforms
* unauthorized functions (e.g. message transcripts, outward-facing APIs or user self-registration) are deactivated
* the integrity of messages is protected (e.g. through the use of digital signatures)
* certain security-related events (e.g. to check for unauthorized activities, to investigate possible breaches and to keep records for regulatory purposes).

The security of the infrastructure of cooperation platforms must be improved by:

* the use of a standard configuration for each platform
* Hardening of servers for collaboration platforms
* Configuration of firewalls to block the use of unauthorized collaboration platforms (e.g. by blocking known ports).

Conference services (such as teleconferences, video conferences and web-based online conferences) must be protected against unauthorized access by:

* authentication is required before users are granted access to a conference
* keep a record of who joins and leaves a conference session and ensure that network connections are disabled or closed at the end of a conference session.