

Security Policy   
Voice over IP

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| VoIP policy | |  |
| 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, its majority-owned subsidiaries, and 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 | 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 Principles 4](#_Toc108428417)

[2 Goals 4](#_Toc108428418)

[3 Controls 4](#_Toc108428419)

# Principles

Networks used for IP-based telephony systems[[1]](#footnote-1) (VoIP) must be authorized and protected by a combination of general network and VoIP-specific controls, regularly monitored and supported by access restrictions.

# Goals

Ensuring the availability of IP-based telephony networks and protecting the confidentiality and integrity of sensitive information (such as the content of calls) during transmission.

# Controls

The use of IP-based telephony services must be approved by the IT department.

There must be documented standards/procedures for VoIP services and the underlying technical infrastructure that include the following

* General network controls for VoIP such as
  + Bandwidth monitoring using tools that are able to detect VoIP traffic
  + Use of network components to ensure reliability and redundancy
  + Restrict access to VoIP networks to authorized devices (such as VoIP adapters or VoIP telephones).
* VoIP-specific controls such as
  + Ensuring that the LAN infrastructure cannot be accessed when monitoring the VoIP system via non-LAN infrastructures (such as management ports, telephone lines, etc.)
  + Where technically possible, the separation of voice traffic through virtual local area networks (VLANs)
  + Hardening of VoIP devices
  + Scanning VoIP networks for vulnerabilities in accordance with the vulnerability management policy and remediating these vulnerabilities as required
  + the analysis of VoIP-related event logs

1. For the purposes of this policy, smartphones or collaboration platforms (such as MS Teams, ...) are not considered VOIP systems. [↑](#footnote-ref-1)