

Security Policy   
E-mail

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| E-mail 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 contents

[1 Principle 4](#_Toc149120079)

[2 Objective 4](#_Toc149120080)

[3 Controls 4](#_Toc149120081)

[3.1 Use of e-mail by SÜDVERS employees 6](#_Toc149120082)

[3.1.1 Access rights for e-mailing and other electronic communication systems 7](#_Toc149120083)

# Principle

Email systems must be protected by a combination of policy, awareness, procedural and technical security controls.

# Objective

Ensure that email services are available when needed, the confidentiality and integrity of messages is protected during transmission and the risk of misuse is minimized.

# Controls

The use of e-mail services must be approved by the responsible IT manager.

There must be documented standards/procedures for the provision and use of email that include the following

* Specifications for the configuration of email servers (e.g. to limit the size of messages or user mailboxes)
* Scanning email messages (e.g. for malware, phishing, chain letters or offensive content)
* Improving the security of email messages (e.g. through the use of disclaimers, hashing, encryption and non-repudiation techniques)
* Guidelines for business and private use
* the permitted types of e-mail services
* User guidelines for permitted use
* Details of any monitoring measures (e.g. scanning the content of messages and attachments) to detect malicious activity and inadvertent leaks of business information.

Email servers must be configured to prevent overloading of the messaging system by limiting the size of messages/user mailboxes and automatically recognizing and aborting email loops.

Email servers must be configured to prevent the inadvertent disclosure of emails and attachments to unauthorized persons by

* Encryption between email servers (e.g. with Transport Layer Security (TLS) or equivalent method)
* Prevent users from configuring the automatic forwarding function to external recipients and from using autocomplete in email address fields
* Users are warned before they can use the "Reply to all" function for a large number of recipients.

Email systems need to be reviewed to ensure that uptime and future availability requirements can be met.

E-mail systems must be configured in such a way that they support and actively use at least the following security functions:

* DKIM (parameters to be included in the header: From, Sender, Reply-To, Subject, Date, Message-ID, To, Cc, MIME-Version, Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description, Resent-Date, Resent-From, Resent-Sender, Resent-To, Resent-Cc, Resent-Message-ID, In-Reply-To, References, List-Id, List-Help, List-Unsubscribe, ListSubscribe, List-Post, List-Owner, List-Archive. Headers not to be included are: Return-Path, Comments, Keywords, Bcc, Resent-Bcc, DKIM-Signature, Authentication-Results) and
* DMARC (with the parameter p=quarantine)

E-mail systems must be configured in such a way that at least the following anti-phishing mechanisms are actively used:

* Examining incoming emails for phishing features (checking links, etc.)
* Blocking of external incoming emails whose sender pretends to be an internal sender (this affects both the contents of the message header fields "From" and "Sender"). Explicitly enabled sender domains can be excluded from this.

E-mail messages must be scanned for:

* Attachments that may contain malicious code (e.g. malicious code hidden in self-extracting zip files, Adobe PDF documents or embedded macros)
* Text passages that are associated with malware (e.g. those commonly used in phishing, hoax viruses or chain letters)
* other active content.

Email systems must protect messages by:

* Blocking messages that are considered unwanted (e.g. by using a blacklist of known unwanted websites or email list servers)
* Use of digital signatures to determine whether email messages have been altered in transit and encryption of sensitive email messages
* Ensuring the non-repudiation of the origin of important e-mail messages (e.g. by using digital signatures)
* Checking the IP source address of sender emails (e.g. using an email validation system such as the Sender Policy Framework (SPF)) to restrict spoofing.

The business integrity of e-mail messages must be protected by:

* Adding legally required information and details of the return address (in the case of incorrectly delivered emails) to business emails (e.g. in the form of a disclaimer)
* Warning users that the content of e-mail messages can be legally and contractually binding and that the use of e-mail can be monitored.

SÜDVERS should:

* the automatic forwarding of e-mails to external e-mail addresses
* unauthorized private encryption of emails or attachments
* opening attachments from unknown or untrusted sources

prohibit

Users must be trained in how to protect the confidentiality and integrity of email messages (e.g. by using encryption, digital certificates and digital signatures).

## Use of e-mail by SÜDVERS employees

The private use of business emails should be clearly marked as private. Sent and received private e-mails etc. should be moved to a "Private" folder or deleted.

In the event of an employee's planned absence, the employee must set up an automated notification of the employee's absence and - if set up - of their replacement. If this is necessary for operational purposes, a substitute assistant can be set up at (access by a colleague) or incoming e-mails etc. can be automatically forwarded to a substitute.

If an out-of-office message has not been set up or was not possible due to an unplanned absence, this can be done by the employer. Automated forwarding is only set up in urgent cases, in particular if an absence message or a substitute assistant alone does not meet the operational requirements. Automated forwarding to an external recipient is not permitted.

Before leaving the company, employees must remove their private e-mails or the "Private" folder from the company e-mail inbox or personal areas of other electronic communication systems. The employee must be given a reasonable period of time to do so. If the normal notice periods are observed without a leave of absence, a reasonable period of time is generally given. In the case of leave of absence or resignation without notice, the period will be discussed with the employee. It will generally be 14 days. The employer has the right to supervise the use of the SÜDVERS systems during this period, taking into account the interests of both parties.

The incoming and outgoing emails in the company email inbox are backed up daily to ensure the functionality of the system and stored for a maximum of 10 years. If private use of the company e-mail inbox is permitted, this may also affect private e-mails, provided they have not been deleted or filed in a folder marked as "personal" before being saved. Such emails are not stored for the stated purpose.

In order to comply with statutory retention obligations (e.g. in accordance with Section 257 HGB, Section 147 AO), incoming and outgoing emails from the company email inbox and other electronic communication systems are regularly archived and stored for a maximum permitted period. If private use of the company e-mail inbox is permitted, this may also affect private e-mails or personal areas of other electronic communication systems, provided they have not been deleted or stored in a folder marked as "personal" before archiving.

### Access rights for e-mailing and other electronic communication systems

* If this is necessary for operational purposes, a substitute assistant can be set up (access by a colleague) or incoming e-mails etc. can be automatically forwarded to a substitute.
* If an absence message was not set up or was not possible due to an unplanned absence, this can be done by the employer.
* Automated forwarding is only set up in urgent cases, in particular if an out-of-office message or a substitute assistant alone does not meet the operational requirements. Automated forwarding to an external recipient is not permitted.
* Access to the company email inbox or personal areas of other electronic communication systems of the employee concerned for company purposes - for example, if the contents of the inbox are required for further processing - may only take place if this is necessary for company purposes.

Such access can be granted either after approval by the e-mail box user (by telephone to the IT helpdesk or by e-mail to the IT helpdesk or the person to whom access is to be denied) or, in the case of temporary absences of the e-mail box user (and their unavailability), temporarily at the written (e-mail) request of the manager (HR and data protection officer must be informed) or with the involvement of trusted persons (data protection officers or their deputies) in accordance with the dual control principle. The employee must be informed immediately of the access. Recognizably private emails, emails marked as "personal", folders with recognizably private content (e.g. "private"), recognizable emails to or from employees of the HR department, with the company doctor, the social counseling service, the data protection officer or the compliance office may not be acknowledged in terms of content.