

Security Policy   
Information classification

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Security Policy Information Classification | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 16.08.2022 | |
| 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 | 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 Information Classification 4](#_Toc194566092)

[2 Information classification scheme 5](#_Toc194566093)

[2.1 Classification level "Public" 5](#_Toc194566094)

[2.2 Internal" classification level 5](#_Toc194566095)

[2.3 Classification level "Restricted" 6](#_Toc194566096)

[2.4 Classification level "Confidential" 6](#_Toc194566097)

[2.5 Classification level "Strictly confidential" 7](#_Toc194566098)

[3 Labeling of information 7](#_Toc194566099)

[4 Handling instructions for classified information 8](#_Toc194566100)

[4.1 Classification level "Public" 8](#_Toc194566101)

[4.2 Internal" classification level 9](#_Toc194566102)

[4.3 Classification level "Restricted" 10](#_Toc194566103)

[4.4 Classification level "Confidential" 11](#_Toc194566104)

[4.5 Classification level "Strictly confidential" 12](#_Toc194566105)

[5 Storage of information 13](#_Toc194566106)

The SÜDVERS information classification scheme, as defined in this document, is based on the principle of "need to know" for the most sensitive information. This term means that information is not disclosed to individuals who do not have a legitimate and demonstrable business need to know. For less sensitive information, the principle of need to know applies. This concept, in conjunction with the other policies, protects SÜDVERS' information from unauthorized disclosure, use, modification and deletion.

A single lapse in information security can have significant long-term consequences. Consistent application of this Information Classification Policy is therefore essential if sensitive information is to be adequately protected. Without the consistent application of an information classification policy, SÜDVERS risks loss of customer relationships, loss of public trust, internal business disruption, excessive costs and competitive disadvantage. This policy is designed to consistently protect sensitive information, regardless of the form in which it is held, the technology used to process it, who processes it, where the information is located and at what stage of its lifecycle it is in. The scheme described in this policy must be used to classify information in all formats, including:

* physical form (e.g. contracts, minutes of management meetings, business plans, product information and employment contracts)
* in electronic form (e.g. files created with spreadsheet and database programs, word processing programs and presentation packages)
* Electronic communication (e.g. messages sent via email, MS Teams, instant messaging and online collaboration systems)
* in oral form (e.g. during meetings, telephone calls, interviews and presentations).

can be used.

# Information Classification

All information from SÜDVERS as well as information entrusted to SÜDVERS by third parties must be categorized into one of five classification levels. If no designation has been assigned, the information must be treated as "Internal" (see below).

This information classification scheme must be used at SÜDVERS to assign sensitivity classifications with separate handling requirements. This policy uses as a basis a data classification scheme that is generally considered appropriate for organizations of our size and is adapted to the specific requirements of SÜDVERS.

According to EU Regulation 2022/2554, the classification of information must be reviewed at least once a year.

# Information classification scheme

Below is a summary of the information classification levels adopted by SÜDVERS, which explicitly take into account the requirements of the Data Protection Act for personal data and sensitive personal data.

## Classification level "Public"

Information of the "Public" level may be disclosed or disseminated without restrictions in terms of content, target group or time of publication. The disclosure or dissemination of the information may not violate applicable laws or regulations, such as data protection regulations.

Changes may only be made by persons who have been expressly authorized to do so by the information owners and who have successfully authenticated themselves on the relevant computer system. Disclosure or dissemination of this information will not result in financial or reputational damage to SÜDVERS.

This category generally includes information that is classified as "negligible" according to the criticality analysis.

Examples of types of information that fall under this classification level:

* Information published on the internet by SÜDVERS (e.g. websites, publications on social media platforms)
* Brochures
* Company reports
* Seminar and presentation documents
* Materials for the exhibition

## Internal" classification level

Internal" level information is for SÜDVERS internal use only and may be disclosed or disseminated by its owner to appropriate members of SÜDVERS to the extent permitted by the owners of the information without restriction as to content or timing of disclosure.

Disclosure or dissemination of this information is not intentional and may result in some negative publicity, but is not likely to cause serious financial or reputational harm to SÜDVERS. A breach in this area could give rise to suspicion of poor management practices. A series of incidents of this level with little damage could be damaging in the long term. It could affect employee morale rather than the profitability of SÜDVERS.

This category generally includes information that falls into the "negligible" or "low" classification levels according to the criticality analysis.

Examples of types of information that fall under this classification level:

* Information published on the SÜDVERS intranet
* Internal phone book
* Internal circulars
* Internal training material
* Work instructions
* Company guidelines
* Initiation lists
* List of endangered mandates
* General information about the market and competitors
* General system or process documentation

## Classification level "Restricted"

Information at the "Restricted" level is subject to access controls and access is only permitted to a defined group of people. Information at the "Restricted" level must be stored in such a way that unauthorized persons do not have access.

Disclosure or dissemination could result in significant financial or reputational harm to SÜDVERS, such as (but not limited to) minor violations of legal, regulatory or contractual requirements, minor reputational harm, minor loss of business or delays in important projects.

This category generally includes information that is classified as "negligible" or "low" according to the criticality analysis.

Examples of types of information that fall under this classification level:

* Customer lists
* Customer meeting notes
* General e-mails to and from customers
* Information from customers or partners
* OASIS Reports
* Information that is only intended for a specific group of people
* Financial data from SÜDVERS
* Design and implementation of security systems (access control...)
* Information on business projects
* Information according to GDPR pursuant to Art. 4 para. 1
* Information on salaries and payroll accounting
* Staff appraisals

## Classification level "Confidential"

Information at the "Confidential" level is subject to access controls and data loss prevention controls, e.g. access is only permitted to a defined group of people or for a limited period of time or with limited functionality. Confidential information must be protected in such a way that unauthorized persons have no access. Information of the "Confidential" level must be secured with technical protection measures as part of "Data Loss Prevention", which also protect and ensure the confidentiality of the information outside SÜDVERS and on mobile devices (such as laptops, tablets, USB devices or smartphones).

Information in this category has at least significant value to SÜDVERS, and unauthorized disclosure or dissemination could result in significant or even catastrophic financial or reputational damage to SÜDVERS, such as (but not limited to) publicized legal action, significant loss of market position, significant or catastrophic impact on reputation for business integrity and customer service.

This category generally includes information that falls into the "medium" classification level according to the criticality analysis.

Examples of types of information that fall under this classification level:

* tactical or strategic plans
* Information on planned mergers or acquisitions
* Personal data pursuant to GDPR Art. 9 (1) (personal data requiring special protection)
* Information classified as "important" under the DORA Regulation

## Classification level "Strictly confidential"

Only those who expressly require access may have access to the data, and only to the extent that this is absolutely necessary for the performance of their work (principles: "need to know" and "least privilege"). Information of the "Strictly Confidential" level must be secured with technical protective measures within the framework of "Data Loss Prevention", which also protect and ensure the confidentiality of the information outside SÜDVERS and on mobile devices (such as laptops, tablets, USB devices or smartphones) or after transmission to third parties.

This category generally includes information that is classified as "high" according to the criticality analysis.

Examples of types of information that fall under this classification level:

* Information that has a negative impact on the European financial sector
* Information classified as "critical" under the DORA Regulation

# Labeling of information

Where technically possible, information shall marked with regard to its classification, whereby the classification scheme described above shall generally be taken into account, but may be waived in order to reduce the workload for non-confidential or not strictly confidential information.

The markings should be easy to recognize.

# Handling instructions for classified information

This section serves as a guide for handling information of a specific classification level in accordance with the previous chapter.

## Classification level "Public"

|  |  |
| --- | --- |
| **Activity** | **Requirement** |
|  |  |
| Electronic storage on non-mobile IT data carriers (network drives Microsoft Cloud Services (O365, OneDrive...)) | No restrictions |
| Electronic storage on movable IT data carriers | No restrictions |
| Electronic transmission via internal or trusted communication networks | No restrictions |
| Electronic transmission via untrusted communication networks (e.g. Internet) | No restrictions |
| Photocopying | No restrictions |
| Fax dispatch | No restrictions |
| E-mail dispatch SÜDVERS internal | No restrictions |
| Sending e-mails to external parties | No restrictions |
| Publication on online collaboration or social media platforms | No restrictions |
| Destruction | No restrictions |
| Disclosure to third parties | No restrictions |
| Hardcopy | No restrictions |
| Internal or external mailing | No restrictions |

## Internal" classification level

|  |  |
| --- | --- |
| **Activity** | **Requirement** |
|  |  |
| Electronic storage on non-mobile IT data carriers (network drives Microsoft Cloud Services (O365, OneDrive...)) | Access control,  Data carrier encryption |
| Electronic storage on movable IT data carriers | Data carrier encryption |
| Electronic transmission via internal or trusted communication networks | No restrictions |
| Electronic transmission via untrusted communication networks (e.g. Internet) | Encrypted |
| Photocopying | No restrictions |
| Fax dispatch | No restrictions |
| E-mail dispatch SÜDVERS internal | No restrictions |
| Sending e-mails to external parties | Gateway-to-gateway encrypted |
| Publication on online collaboration or social media platforms | Allowed for closed user groups |
| Destruction | See separate guideline "Destruction and disposal of data carriers" |
| Disclosure to third parties | Non-Disclosure Agreement or Disclaimer |
| Hardcopy | Optional: Information on classification level |
| Internal or external mailing | Single envelope |
| Granting of access rights by | Internal: not required  External: Information owner or line manager |

## Classification level "Restricted"

|  |  |
| --- | --- |
| **Activity** | **Requirement** |
|  |  |
| Electronic storage on non-mobile IT data carriers (network drives Microsoft Cloud Services (O365, OneDrive...)) | Access control,  Data carrier encryption,  At the request of the information owner, additional protection using tools |
| Electronic storage on movable IT data carriers | Data carrier encryption  At the request of the information owner, additional protection using tools |
| Electronic transmission via internal or trusted communication networks | No restrictions |
| Electronic transmission via untrusted communication networks (e.g. Internet) | Encrypted |
| Photocopying | No restrictions |
| Fax dispatch | No restrictions |
| E-mail dispatch SÜDVERS internal | No restrictions |
| Sending e-mails to external parties | Gateway-to-gateway encrypted |
| Publication on online collaboration or social media platforms | Allowed for closed user groups |
| Destruction | See separate guideline "Destruction and disposal of data carriers" |
| Disclosure to third parties | Non-Disclosure Agreement or Disclaimer |
| Hardcopy | Optional: Information on classification level |
| Internal or external mailing | Single envelope |
| Granting of access rights by | Information owner or line manager |

## Classification level "Confidential"

|  |  |
| --- | --- |
| **Activity** | **Requirement** |
|  |  |
| Electronic storage on non-mobile IT data carriers (network drives Microsoft Cloud Services (O365, OneDrive...)) | Data carrier encryption,  Data encryption  Logging and monitoring of access  Use of DLP tools for additional protection |
| Electronic storage on movable IT data carriers | Data carrier encryption,  Data encryption  Use of DLP tools for additional protection |
| Electronic storage, processing or transmission of information covered by the GDPR on systems that are not under the operational control of SÜDVERS | Inclusion in the procedure directory  Contract for commissioned data processing  Carrying out service provider audits (information security)  Use of DLP tools for additional protection |
| Electronic storage, processing or transmission of information covered by the GDPR on systems under the operational control of SÜDVERS | Inclusion in the procedure directory  Use of DLP tools for additional protection |
| Electronic transmission via internal or trusted communication networks | No restrictions |
| Electronic transmission via untrusted communication networks (e.g. Internet) | Encrypted |
| Photocopying | Obtaining permission from the owner of the information recommended |
| Fax dispatch | Obtaining permission from the owner of the information recommended |
| E-mail dispatch SÜDVERS internal | No restrictions |
| Sending e-mails to external parties | Gateway-to-gateway encrypted or in encrypted e-mail attachments |
| Publication on online collaboration or social media platforms | Not allowed |
| Destruction | See separate guideline "Destruction and disposal of data carriers" |
| Disclosure to third parties | authorization of the information owner is necessary and  Non-Disclosure Agreement or Disclaimer |
| Hardcopy | Information on classification level |
| Internal or external mailing | Single envelope  Addressed by name |
| Granting of access rights by | Information owner or line manager |

## Classification level "Strictly confidential"

|  |  |
| --- | --- |
| **Activity** | **Requirement** |
|  |  |
| Electronic storage on non-mobile IT data carriers (network drives Microsoft Cloud Services (O365, OneDrive...)) | Data carrier encryption,  Data encryption  Complete logging and monitoring of access  Use of DLP tools for additional protection |
| Electronic storage on movable IT data carriers | Data carrier encryption,  Data encryption  Data carriers must be stored in a safe place when not in use  Use of DLP tools for additional protection |
| Electronic storage, processing or transmission of information that falls under the GDPR (category "particularly sensitive data") on systems that are not under the operational control of SÜDVERS | Inclusion in the procedure directory  Data encryption  Use of DLP tools for additional protection Use of DLP tools for additional protection Contract for commissioned data processing  Carrying out service provider audits (information security) |
| Electronic storage, processing or transmission of information that falls under the GDPR (category "particularly sensitive data") on systems that are under the operational control of SÜDVERS | Inclusion in the procedure directory  Data encryption  Use of DLP tools for additional protection |
| Electronic transmission via internal or trusted communication networks | No restrictions |
| Electronic transmission via untrusted communication networks (e.g. Internet) | Encrypted |
| Photocopying | Authorization of the information owner required |
| Fax dispatch | Authorization of the information owner required  Sending encrypted or in consultation with the recipient |
| E-mail dispatch SÜDVERS internal | End-to-end encrypted  (encrypted e-mail attachments can be used) |
| Sending e-mails to external parties | End-to-end encrypted (encrypted e-mail attachments can be used) |
| Publication on online collaboration or social media platforms | Not allowed |
| Destruction | See separate guideline "Destruction and disposal of data carriers" |
| Disclosure to third parties | Authorization of the information owner required  Non-Disclosure Agreement |
| Hardcopy | Information on classification level |
| Internal or external mailing | Single envelope  Addressed as "Personal |
| Granting of access rights by | owner |

# Storage of information

There may be minimum or maximum periods within which information must be retained. These may be prescribed by law or contract. For more information on retention periods, please contact your line manager.