

Security Policy

destruction and disposal of storage media

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Destruction and disposal of data storage media | |  |
| 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 contents

[1 Principles 4](#_Toc188268311)

[2 Goals 4](#_Toc188268312)

[3 Controls 4](#_Toc188268313)

[3.1 Paper 4](#_Toc188268314)

[3.1.1 - Destruction of paper waste 4](#_Toc188268315)

[3.1.2 How should paper material be disposed of? 4](#_Toc188268316)

[3.2 IT equipment 5](#_Toc188268317)

[3.2.1 DVDs/CDs 5](#_Toc188268318)

[3.2.2 MAGNETIC TAPES 5](#_Toc188268319)

[3.2.3 DESKTOP PCs and LAPTOPS 5](#_Toc188268320)

[3.2.4 MEMORY STOCKS and FLASH CARDS 5](#_Toc188268321)

[3.2.5 MOBILE PHONES and SMART PHONES 5](#_Toc188268322)

[3.2.6 SIM CARDS/MEMORY STICKS 5](#_Toc188268323)

[3.2.7 SERVER, NETWORK COMPONENTS, MULTIFUNCTIONAL DEVICES, PRINTERS AND FAX DEVICES 6](#_Toc188268324)

[3.2.8 Provision of IT equipment to employees or third parties for use outside SÜDVERS 6](#_Toc188268325)

[3.3 Standards to be complied with for safe disposal and destruction 6](#_Toc188268326)

[3.3.1 Shredding of paper 6](#_Toc188268327)

[3.3.2 Secure erasure of electronic storage media 6](#_Toc188268328)

[3.3.3 Destruction of electronic storage media 6](#_Toc188268329)

# Principles

Licensed software programs, institutional/business data, personally identified or identifiable data and/or non-public data must be reliably erased and/or destroyed from paper or any electronic device before the device is transferred out of SÜDVERS' control. Failure to delete data in such a way that it cannot be recovered can pose a significant risk to SÜDVERS as the data can often be recovered by readily available means.

# Goals

Ensure that sensitive information is protected from unauthorized disclosure after it is no longer needed.

# Controls

## Paper

### - Destruction of paper waste

It is important that all business paper waste is disposed of in a secure manner to maintain confidentiality and comply with legislation. All waste/unwanted paper is disposed of in the recycling bins or locked confidential paper containers located throughout SÜDVERS. Unwanted paper may include draft documents, unwanted agendas and meeting minutes, papers in files that SÜDVERS no longer needs to keep, poor photocopies or handwritten notes, etc. Any documents that are thrown in the general wastebasket can be retrieved by anyone who wishes to view and/or use the information. Care should be taken to ensure that confidential material is labeled and removed so that only general paper is disposed of in these types of bins.

If the information requires more protection than that which falls under the "internal" classification level, it must be shredded or torn into very small pieces.

### How should paper material be disposed of?

* Up to classification level "internal": Put in the recycling garbage can. The bins are emptied by SÜDVERS as part of the normal janitor activities.
* Higher than the "internal" classification level: If sensitive information is involved, the paper must be disposed of using the secure paper disposal containers provided by SÜDVERS in our branches, which are then destroyed by certified service providers.

## IT equipment

IT equipment includes all the items listed in the following chapters. This is not an exhaustive list of all possible media, as technology evolves and new media become available over time. The following are the most common types of media in use at the time of the last update of this policy.

### DVDs/CDs

Must be physically destroyed, ideally by shredding or incineration.

### MAGNETIC TAPES

Must either be securely erased or destroyed by incineration or shredding. If you have such a device for secure deletion or destruction, please contact the IT Helpdesk for advice. This material must be physically locked away before secure deletion or destruction.

### DESKTOP PCs and LAPTOPS

Must be securely deleted or their hard disks physically destroyed, ideally by shredding. If you have such a device for secure deletion or destruction, please contact the IT Helpdesk. Before secure deletion or destruction, this material must be physically locked away.

### MEMORY STOCKS and FLASH CARDS

must either be securely deleted or physically destroyed, ideally by shredding or incineration. If you have such a device for secure deletion or destruction, please contact the IT Helpdesk for advice. This material must be physically locked away before secure deletion or destruction.

### MOBILE PHONES and SMART PHONES

Must either be securely erased or physically destroyed, ideally by shredding or incineration. If you have such a device that needs to be securely erased or destroyed, please contact the IT Helpdesk for advice. This material must be physically locked away before secure deletion or destruction.

### SIM CARDS/MEMORY STICKS

Must either be securely erased or physically destroyed, ideally by shredding or incineration. If you have such a device that needs to be securely erased or destroyed, please contact the IT Helpdesk for advice. This material must be physically locked away before secure deletion or destruction.

### SERVER, NETWORK COMPONENTS, MULTIFUNCTIONAL DEVICES, PRINTERS AND FAX DEVICES

When servers, network components, multifunction devices, printers or fax machines containing a hard disk are removed, the hard disk must either be securely erased or physically destroyed, ideally by shredding. Before secure deletion or destruction, this material must be physically locked away.

### Provision of IT equipment to employees or third parties for use outside SÜDVERS

The transfer of IT devices with storage media that have been used internally to store confidential information to employees or third parties for use outside SÜDVERS is prohibited. Exceptions apply to IT systems whose storage media have been securely deleted (see below).

Labels and markings that identify SÜDVERS or indicate the classification, owner, system or network must be removed prior to disposal, including resale or donation to a charity or similar organization.

## Standards to be complied with for safe disposal and destruction

The following standards are defined as minimum standards that must be adhered to in order to ensure the secure destruction of SÜDVERS information:

### Shredding of paper

The following minimum standards apply to the safe shredding of paper

* for information up to classification level "restricted" DIN 66389 level P-1
* for information that falls into a classification level higher than "restricted" DIN 66389 level P-2

### Secure erasure of electronic storage media

The minimum standard for the secure erasure of electronic storage media is

* DoD 5220-22.M for information up to classification level "restricted" and
* NIST 800-88 for information that falls into a classification level higher than "restricted".

### Destruction of electronic storage media

The minimum standard for the destruction of electronic storage media is NHS Digital "Destruction and Disposal of Sensitive Data v3.2": <https://www.sfh-tr.nhs.uk/media/4864/destruction-and-disposal-of-sensitive-data-version-32.pdf>