KISTERS Information Security Guideline

v.5.6, 2025-07-21

Owner:
KISTERS ISMT

Table of contents

1 Introduction

Information and processing thereof play a key role for the KISTERS Group to fulfil its tasks. All data and information accessed by KISTERS staff in connection with their work activities shall always be treated as internal or confidential. For this reason, protecting this information from unauthorized access, non-authorized changes or dissemination as well as unacceptable non-availability is of existential importance. The "KISTERS Information Security Policy" outlines security objectives pertaining to information and IT systems as well as strategic requirements and boundary conditions for these objectives to be met.
The aim of this guideline is to provide KISTERS Group staff concrete measures and instructions to meet the security objectives. In addition to general measures, these also include measures pertaining to handling IT systems which are to be taken to achieve and maintain information security.

1.1 Scope

This Information Security Guideline applies to all members of staff, business units, sites and the entire IT infrastructure of the KISTERS Group and IT systems operated as part of it. The KISTERS Group includes the KISTERS AG as well as all of its national and international subsidiaries. The staff includes the employees of the KISTERS Group, including interns and temporary employees, as well as all employees of third parties and individuals who work for or at the KISTERS Group.
Security regulations contained in this Guideline are binding for the mentioned groups of persons. Gross negligent or intentional violations of the information security guidelines are prosecuted and penalized by both disciplinary and (criminal) law to the extent permitted by law.

1.2 Terminology

To be able to clearly distinguish normative and informative contents, the following key terms according to RFC 2119 will be used:

- "MUST" / "SHALL ONLY" or "REQUIRED" indicate normative requirements. Any exceptions must be authorized in writing by the KISTERS Board or one of its representatives.
- "MUST NOT" / "SHALL NOT" or "FORBIDDEN" indicate the normative exclusion of a feature. Any exceptions must be authorized in writing by the KISTERS Board or one of its representatives.
- "SHOULD" or "RECOMMENDED" indicate a strong recommendation. Deviations from these recommendations must be justified on a case-by-case basis and approved by the supervisors and/or those responsible for the respective subject.
- "SHOULD NOT" or "NOT RECOMMENDED" indicate a strong recommendation to exclude a feature or behaviour. Deviations from these recommendations must be justified on a case-by-case basis and approved by the supervisors and/or those responsible for the respective subject.
- "MAY" or "OPTIONAL" indicate that this feature or behaviour is truly optional.

All sections of this Information Security Guideline shall generally be considered normative. Informative sections are labelled clearly with the keyword [INFO].

1.3 Contact persons

The information security management team is available at all times regarding matters pertaining to information security, data protection and business continuity:

Name	Role	Phone	Email
Bernd Kisters	CIO (Head IT)	+49 2408 9385 105 +49 172 7181704	bernd.kisters@kisters.de
Dr. Heinz-Josef Schlebusch	CISO (Chief Information Security Officer) & DPO (Data Protection Officer)	+49 2408 9385 226 +49 172 7181829	schlebusch@kisters.de
Jens Weber	BCMO (Business Continuity Management Officer)	+49 2408 9385 126 +49 170 3755187	jens.weber@kisters.de
Jasmina Rade	IS Expert	+49 2408 9385 433 +49 171 1042409	jasmina.rade@kisters.de
Mailbox IT security			itsecurity@kisters.de
Mailbox data protection			datenschutz@kisters.de
Mailbox mail security			mailsecurity@kisters.de
Mailbox System Administration			sysadmin@kisters.de
Jira Service Desk information security	https://conflks.atlassian.net/servicedesk/customer/portal/11		
Jira Service Desk System-Administration	https://conflks.atlassian.net/servicedesk/customer/portal/5		
Jira Service Desk Whistleblowing	https://conflks.atlassian.net/servicedesk/customer/portal/14		

The contact for technical questions is KISTERS IT Administration (hereinafter referred to as "IT Administration" or "IT Administrators").

1.4 Further information

Further information and guidelines pertaining to information security and data protection is available on the KISTERS Confluence Compliance Center Space (https://conflks.atlassian.net/wiki/spaces/CC/pages/30049401/Information+Security+and+Data+Protection+Informationssicherheit+und+Datenschutz).
Information on available software tools are made available by the IT administrators on the KISTERS Confluence General Information Space under “Systemadministration -> Tools & Software“ (https://conflks.atlassian.net/wiki/spaces/GEN/pages/44500611/Tools+Software).

2 Information security in business operations

2.1 Obligation to comply

The regulations on information security, data protection and business continuity are binding and MUST be taken into account in all business activities.
For internal and external projects, regardless of the size and type of project, the requirements for and effects on information security and data protection MUST be identified and evaluated.
To this end,

- the objectives of information security,data protection and business continuity management SHOULD be included in the project objectives, where applicable;
- A risk assessment of information security, data protection and business continuity management SHOULD be conducted at an early stage of the project to identify necessary security measures;
- information security, data protection and business continuity management SHOULD be considered at all stages of project implementation.

For projects and operational activities that may have a significant impact on information security, privacy or business continuity, the CISO, DPO and BCMO MUST be informed and involved at the earliest possible stage to identify necessary security, privacy or BCM measures and avoid possible risks.

2.2 Deviations and exceptions

Deviations and exceptions from the information security requirements MAY be approved for a limited period of time. For this purpose, the risks arising from the deviations MUST be assessed by the respective risk owner and handled in accordance with the risk management requirements. The approved deviations, their time limitation as well as the risk assessment and treatment MUST be suitably documented, for example by corresponding tickets in the KISTERS ticket system.

3 Acceptable use of company assets

Company assets used by KISTERS employees in the course of their employment with the KISTERS Group MUST ONLY be used for business purposes. This includes, but is not limited to, buildings, premises, workplaces, equipment, vehicles, IT systems, communication systems, applications, documents, information in analogue or electronic form.
By way of exception, company assets MAY be used for non-business purposes if there is a general exemption or a specific exemption agreement.

[INFO] To achieve and maintain information security, unauthorized or improper use of company values must be prevented. To this end, measures to control physical, logical and data access are being taken.

- Physical access control refers to physical access to buildings, rooms and IT systems,
- Logical access control refers to the use of IT systems,
- Data access control refers to access to any information, data and documents.

The extent to which buildings, IT systems and information require protection depends on their purpose and criticality. For this reason, these company values are classified and measures to meet security objectives will be defined according to a multi-level system.
Classification and the respective measures are defined in the guideline "KISTERS Classification of Assets - Physical, Logical and Data Access Control" and are a compulsory component of the "KISTERS Information Security Guideline". The following is a simplified summary of the measures outlined therein.

3.1 Physical access control

Each KISTERS facility (company building, parts of buildings or rooms on rented premises) MUST always be secured against unauthorized access. The facility MUST remain locked outside of business hours that are defined for each site. Site-specific regulations pertaining to access and securing of the business premises MUST be followed.
Access for third parties MUST be registered using the visitors' list at reception or the secretary's office. Third parties SHALL ONLY access the internal areas of KISTERS business premises in the company of KISTERS staff.
Rooms requiring a high level of protection MUST remain locked at all times. Access to these rooms SHALL ONLY be granted to authorized staff or in the company of authorized staff. Rooms requiring a high level of protection include server rooms, installations rooms, archives and file storages.

3.1.1 Use of recording devices

Within KISTERS premises, photo, video, audio and other recordings by employees SHALL ONLY be made for official business purposes. These recordings SHOULD ONLY be made using KISTERS equipment. Recordings MUST be deleted from other recording devices as soon as the purpose of the recordings no longer holds or the recordings have been transferred to KISTERS systems.
Photo, video, audio, and other recordings by external third parties SHALL ONLY be made with the permission of the responsible KISTERS employee.
Recordings MUST be classified and handled according to the classification of the information recorded. All recordings MUST comply with applicable privacy regulations.

3.2 Logical access control

Adequate measures for the control and monitoring of logical access to prevent unauthorized use and abuse MUST be defined for each IT system and each application.
For each information, IT system or application, one or more persons MUST be designated as responsible for granting access authorization and the assignment of user rights within the system.
All rights MUST be assigned according to the "principle of least privilege" and the "minimum need-to-know principle". Those responsible MUST review granted rights on a regular basis.
In the event that a member of staff leaves the company or that their role changes, their supervisor MUST notify those responsible for the information and systems used by the member of staff immediately and require a review and, if necessary, a change of the access and user rights and passwords.

3.2.1 Passwords

[INFO] Passwords and PINs ("Personal Identification Number") are confidential information, and compromising them can have far-reaching consequences.
Use of passwords and PINs is regulated in "KISTERS Password Guideline", which is also a compulsory component of this guideline.

3.3 Data access control

3.3.1 Internal and confidential information

The classification of data and information MUST be performed by those responsible for such data and information.

All data and information accessed by KISTERS staff in connection with their work activities MUST be treated as internal information unless specified otherwise. All data which can be linked to a natural person directly or indirectly are subject to particular protection as defined by the European General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) and any other applicable data privacy regulations MUST be treated as confidential.

In handling any internal and confidential information of any type and form, the following rules have to be observed:

- The information SHALL ONLY be used for operating purposes.
- The information SHALL ONLY be transmitted to authorised recipients (internal/external).
    - Transmission of the information MUST be authorized by those responsible.
    - Authorisation of the recipient MUST be checked/verified by the person transmitting the information.
- The information MUST be protected from unauthorized access.

3.3.2 Third-party business data

Business data of third parties MUST always be treated as "confidential" unless otherwise classified by the transferring third parties.

In general, all data provided to us by customers or partners MUST be managed by the respective project managers. These MUST also comply to the customer's terms of use.

Project managers MUST monitor the correct use of these data in order to make sure that persons handling them comply with the respective privacy policies.

It SHOULD be clearly traceable who is dealing with which data.

[INFO] If no privacy policy is provided by the clients or partners, the KISTERS Information Security Guidelines and the Commitment to Confidentiality and Data Protection will apply in any case.

3.4 Clean desk - clear screen

The principle of “clean desk - clear screen” MUST be applied by each employee in order to reduce the risk of unauthorized access, the loss or damage of documents, information storage devices and information processing facilities.

3.4.1 Clean desk

All confidential documentation and media carrying confidential data SHALL ONLY be stored at the work place as long as they are absolutely required to carry out the business tasks related to them. Apart from that, this documentation MUST be stored securely in locked rooms or cabinets at all times. Particularly sensitive or critical documents (e.g., staff records) MUST be stored at all times in locked rooms or cabinets with restricted access permission provided for this purpose.

3.4.2 Clear screen

Each computer system MUST have an enabled lock screen with password protection to avoid unauthorized use. Whenever the workplace is left – even if only for a short period of time – the password protected lock screen MUST be activated. If a longer interruption of work for more than one day is expected or planned, users SHOULD log off from single-user systems (workstations, laptops, etc.). Users MUST log off from single-user systems if the work is interrupted for more than one week. Users of multi-user systems MUST always log off after completion of the tasks to be performed there.

3.5 Measures in case of suspected unauthorized use

In the event that a computer or application is suspected to have been used in an unauthorised manner, or if information is suspected to have been accessed without appropriate authorisation, the following steps SHOULD be taken:

1. Stay calm! Never follow messages that appear on the screen. Oftentimes, traces of unauthorized use may be deleted by hasty actions, making tracking impossible.
2. If traces of unauthorized use or access can be found on-screen, capture them by taking a picture or a screenshot.
3. If files or file contents point to unauthorized use, do not modify or delete them but, if possible, make a note of their relevant meta information (folder path, size, date, etc.).
4. Inform your IT administrators by phone(!). Have the following information ready:
   4.1. What device are we talking about, where is it and how is it currently linked to the corporate network?
   4.2. How did you detect unauthorized use (application messages, unusual processes, unusual files or file changes, etc.)?
   4.3. What applications were in use and may be affected?
   4.4. What data may be affected?
   4.5. Wait for further instructions of your IT administrator.
5. Hand over your computer to the IT administration for securing of evidence and potentially further forensic investigation by external specialists.

4 Data protection

[INFO] Data protection refers to the protection of personal data. Personal data is any information relating to an identified or identifiable natural person. This includes, for example, name, address and date of birth, but also location data or IP addresses, insofar as these can be assigned to a person (by adding further information).

[INFO] At the KISTERS Group, data protection is regulated by the "Declaration of commitment to information security, confidentiality and data protection". This commitment is signed by all KISTERS staff and is part of the employment contract of all employees of the KISTERS Group. Any violation of the regulations in the area of information security, confidentiality and data protection is subject to disciplinary and (criminal) legal actions to the extent permitted by law.

External co-workers working with the KISTERS Group or for the KISTERS Group as part of a project or service contract MUST also sign the "Declaration of commitment to information security, confidentiality and data protection" .The project manager is responsible to ensure the agreements have been signed.

5 Data backup and archiving

5.1 Data backup

[INFO] Data backup is used to avoid possible data loss by regularly copying data to other storage devices (backup). These backups can be used to recover original data in the event of loss or destruction (restore). Data on file servers, Exchange servers and Notes servers is centrally backed up daily by the IT administration.
Each employee is responsible for backing up locally stored data. This data SHOULD be regularly backed up by the employees. The IT administration provides suitable tools (hardware/software) for this purpose.
Further regulations for data backup are laid down in the "KISTERS IS Guideline for Administrators".

5.2 Data archiving

[INFO] All business documents and data are subject to longer-term archiving obligations and deletion periods due to legal requirements. The data on file servers, Exchange servers and Notes servers is archived centrally by the IT Administration. The data archives are deleted after the retention periods have expired. Therefore, all employees MUST store all business-relevant data, such as project data, contract data, etc., on the corresponding file servers, Exchange servers and Notes servers.

6 Encryption

Sensitive and critical data are subject to special protection requirements with regard to their confidentiality and SHALL ONLY be stored or transmitted in encrypted form under certain circumstances. Those responsible for the information MUST determine if encryption is required. In case of personal information, the DPO SHOULD be consulted.
Requirements pertaining to data encryption are defined in detail within the "KISTERS IS Policy and Guideline on Cryptographic Controls" and are a compulsory component of this guideline.
The following is a simplified summary of the measures outlined therein.

6.1 Internal email

Internal email cannot be encrypted in Outlook. Instead, all internal emails containing confidential data and information (e.g. details of personnel data) MUST be sent with the sensitivity "**Private**".

6.2 External email

Confidential information that is exchanged by email with external parties (clients or partners) SHOULD be encrypted. The process MUST be coordinated with the external sender/recipient and IT administration in each individual case. The standard procedure SHALL be an exchange via S/MIME encryption.

6.3 Mobile data storage devices

[INFO] Mobile data storage devices include

- all USB flash drives (USB memory sticks), SIM cards or external hard drives that can be connected to computer systems via USB or other external ports,
- hard drives of all mobile workstations such as notebooks, netbooks and PDAs, and

- tapes, CDs and DVDs that are used for data backup and archiving.

Confidential data MUST be stored in encrypted form on these mobile data storage devices.
[INFO] The storage device will either be encrypted completely (e.g., using BitLocker), or an encrypted section will be created on the storage device for the storage of confidential information instead (e.g., using VeraCrypt). The software necessary for the encryption, which performs the encryption according to the state-of -the-art (currently: AES-XTS-265), is provided by the IT administration.
As an alternative, the encryption MAY be limited to individual files or file archives containing confidential data. This MAY be done for example using the free encryption tool PDFEncrypt for PDF-files or the file archiving tool 7-zip. When using encryption, the AES-256 method MUST be used if the tool supports it. in any case a strong password MUST be chosen.
The central IT administration in Aachen, Germany, MUST be immediately informed of a loss or theft of a storage device!

7 Procurement and Disposal of Data Storage Devices

IT systems (workstations, laptops, tablets, mobile phones) and mobile data storage devices (hard disks, USB flash drives, tapes, CDs, DVDs, etc.) that are used for business purposes or on which business data (KISTERS data, customer data) is stored MUST be procured by the KISTERS IT administration. The business use of devices procured elsewhere is FORBIDDEN.
IT systems and mobile data storage devices that are damaged or no longer needed MUST be submitted to the IT Administration to prepare for reuse or disposal.
Data stored on these devices that is no longer needed SHOULD be deleted before the devices are handed over to the IT administration, if this is technically possible.
[INFO] The IT administration ensures that sensitive data and licensed software are deleted or securely overwritten. Any other reuse or disposal is strictly prohibited. Further guidelines on the disposal of data storage devices are set forth in the “KISTERS Information Security Guideline for Administrators”.
Non-electronic data storages containing internal or confidential information (e.g., handwritten notes, prints etc.) MUST be destroyed using data shredders provided at each site. To destroy larger amounts of files containing confidential data, these SHOULD be collected in locked containers and handed to specialist service providers for destruction.

8 Company assets outside of KISTERS premises

8.1 General provisions

[INFO] Company assets are IT systems, general operating resources, information, documents, software, etc., which are used to perform operational tasks and carry out business processes. The following rules must always be observed for company assets:

- Enterprise assets SHALL ONLY be used by qualified and authorized users.
- The taking and use of company assets outside the KISTERS premises MUST be authorized by the person responsible for these assets or a representative.
- The taking of company assets SHOULD be documented, especially if the assets are expected to be removed from the KISTERS premises for an extended period of time.

- All company assets MUST be secured by appropriate measures against unauthorized use, damage, theft and loss, especially outside the KISTERS premises.
- The regulations on physical access, logical access and data access control MUST be observed at all times.
- When transporting classified KISTERS documents, IT systems and other assets between KISTERS locations or between a KISTERS location and customers, partners or service providers, the completeness and integrity of the transported assets MUST be verified upon delivery. This MAY be done, for example, by creating and verifying a parts list or a bill of materials.
- Theft, loss or unauthorised usage of company assets are security incidents and MUST immediately be reported to the person responsible for the assets and the CISO.
- Company assets that are no longer required MUST be returned to the responsible persons.
- All internal and confidential data SHOULD be deleted before IT systems and data carriers that are no longer required are returned to the IT administration.

8.2 Mobile use of IT systems, teleworking sites

[INFO] Mobile devices and telecommuting devices are regularly transported, stored and used outside the physically secured premises of the KISTERS Group. These devices are frequently used to access other KISTERS IT systems and information. Mobile use also includes the use of IT systems as presentation or demo systems at trade fairs, exhibitions or similar events or as test systems at customers' or partners' premises. Special measures against unauthorized use, theft and loss must be taken for these devices:

- Mobile devices and teleworking stations MUST be clearly assigned to an employee at all times.
- Mobile devices and teleworking stations MUST be protected from unauthorized access by means of passwords and/or PINs (“Personal Identification Number”). Use of passwords and PINs is defined in the “KISTERS Password Guideline”, which is a compulsory component of this guideline.
- Central IT administration in Aachen and the CISO MUST be notified immediately of a loss, theft or suspected unauthorized use of mobile or teleworking devices.
- All mobile and teleworking devices no longer required MUST be handed back to central IT Administration in Aachen for further use or disposal.
- Measures for mobile data storage devices, measures for the protection from malware, data backup measures and measures for remote access in particular MUST be observed for mobile devices and teleworking stations.

8.2.1 Mobile devices

[INFO] Mobile devices include laptops, notebooks, netbooks, tablet computers, PDAs, smartphones, cameras etc.

- Mobile devices used for operational purposes MUST be procured and approved for use by IT administration (“company devices”).
- The devices MUST be physically protected against unauthorised access, loss or theft, e.g., by means of
    - personal supervision and access protection (e.g., in the car, on the train or plane)
    - storage in locked rooms or closets
    - chaining (“Kensington lock”)
- A “boot password” SHOULD be set for these devices.

- Users MUST ensure that mobile devices are updated to the most recent IT security level. This includes among others security patches of the installed software as well as updates of virus signatures. This MUST be done, depending on the device, by connecting the device to the KISTERS network or by handing it to IT administration.
- Confidential data MUST be stored encrypted on the data storage of the mobile device. ONLY the confidential data necessary for the intended purpose SHOULD be stored on these data media. [INFO] The software necessary for the encryption is provided by the IT administration (see section "Mobile data storage devices").
- Using mobile devices in private or public networks, users MUST choose the relevant security settings when connecting to the network. These include:
    - usage of "guest WLAN" in case of wireless connection
    - network option "public" to prevent release of data
    - encrypted data transmission by using VPN, https, sftp etc.
- Communication interfaces of mobile devices like Wi-Fi, Bluetooth or NFC MUST be deactivated when no network connection is required. Data connections between mobile devices (e.g., via Bluetooth-Pairing) SHOULD be used as infrequently as possible and ideally only in physically secure environments, in which eavesdropping of the communication by unauthorised third parties is not possible.
- Voice assistants SHOULD be deactivated unless they are absolutely necessary. In general, it SHOULD not be possible to use a voice assistant if the device is locked.
- When working with mobile devices, care SHOULD be taken to ensure that no sensitive information can be spied on. To this end, an appropriate privacy screen SHOULD be used that covers the entire screen of the respective device and makes it difficult to spy out information.

8.2.2 Smartphones

The following additional measures apply to smartphones:

- Confidential data SHALL NOT be stored on smartphones, with the exception of encrypted copies of the personal Outlook database.
- Screens and interfaces of a smartphone not in use MUST be locked when the device is being put down.
- Unlocking a smartphone
    - MUST be done by use of a PIN or a biometric factor (fingerprint, face recognition);
    - using unlock patterns MUST be deactivated as these patterns are readily identifiable.
- On smartphones for business purposes ONLY known and widely used apps from the official stores MAY be installed. In case of doubt, approval SHOULD be obtained from the CISO team or the system administration.
- For Android smartphones, the use of antivirus protection is recommended, but not mandatory.

[INFO] Accessing business emails and the calendar on the KISTERS Exchange Online Server (M365) from a mobile device via Outlook App or web access is permitted and does not require explicit authorisation of this device by the system administration. The data exchange between the Smartphone and the Exchange Server is carried out via an encrypted Internet connection. All local Outlook data MUST BE stored encrypted on the smartphone.

8.2.3 Teleworking sites

[INFO] Teleworking sites are workplaces that are regularly used by KISTERS employees outside the KISTERS Group's premises (e.g., home office, temporary workplace at customer's premises, work on the road, ...). KISTERS provides employees with mobile or stationary company equipment for teleworking, for which the following regulations apply:

- The work equipment provided by KISTERS MUST NOT be used for private purposes.
- Work equipment MUST NOT be made available to third parties.
- Employees MUST ensure that the work equipment is physically protected at all times against unauthorised access, loss and theft by third parties.
- The operational and legal regulations of data protection and data security MUST be observed and applied.
- In particular, the requirements for a clean desk and clear screen MUST be observed.
- Internal and confidential information MUST be protected by the employees in such a way that third parties - especially persons living in the employees' household - cannot view and/or access it.
- Documents or data carriers MUST ONLY be brought to the teleworking site with the consent of the supervisor and MUST be encrypted or transported in sealed containers.
- For home offices: The internet access of the business IT systems SHOULD be separated from the home network, e.g., using a separate guest access. If this is not possible, the access to the home network MUST be configured as an access to a “public network”.
- For access to the KISTERS network the VPN software and credentials provided by the IT administration MUST be used.

Further specific regulations for the establishment and use of teleworking sites are defined in the "KISTERS Agreement on Teleworking".

9 Private devices and media – “Restricted BYOD” guideline

Devices and media (stationary or mobile IT systems, data storage devices, peripherals, etc.) owned privately by KISTERS staff MAY be used for business in exceptional cases for tasks of limited duration or limited function (“Restricted Bring Your Own Device”).

- The use MUST be approved in advance by the employee's supervisor; in exceptional cases (e.g., emergency situations) the use MAY also be approved retroactively.
- Approval SHALL ONLY be granted if the equipment and media are sufficiently secure for the intended use (e.g., current anti-virus program on IT systems, secure physical access protection and virus check for data carriers).
- Confidential data MUST NOT be stored on private mobile devices. If in exceptional cases confidential information has been stored on private devices (e.g., notes, pictures of whiteboards or screens), this MUST be deleted from the device as swiftly as possible.
- If the need to transmit data from a private device to a KISTERS IT system arises from this, the same security precautions MUST be taken which apply when transmitting data from the internet or other unsecured sources.

9.1 Business Cloud services on private devices

[INFO] It is not technically possible to prevent the use of business cloud services such as Outlook, Teams or Confluence and Jira from private IT systems (smartphones, tablets, laptops, etc.). These services require 2-factor authentication, making unauthorised use more difficult. However, depending on the user interface used (web, app), data may be deliberately or automatically stored locally on private IT systems during use. Therefore, the following rules for the use of these services on private IT systems must be observed:

- The use of business cloud services MUST ONLY be carried out from private IT systems if there is a business necessity for this.
- Private IT systems that are used to access company cloud services MUST be treated like company IT systems with regard to their IT security (access protection, virus protection, patch management, etc.). The responsibility for this lies with the users.
- If the use is no longer required, e.g., when leaving the company, all business data (e.g., email) stored on the private IT systems due to the use of the business cloud services MUST be completely deleted.
- If security risks arise due to the use of business cloud services on private IT systems, this use MAY be prohibited individually by management directive. Violations shall be penalised accordingly.

10 Network access

[INFO] The KISTERS network is logically divided into separate segments used to different ends and requiring different levels of protection:

- General KISTERS Data Network (KISTERS LAN, “wlanac22“)
- Network for internet access for mobile KISTERS devices and smartphones (“mnotes”)
- Network for internet access for external third parties (visitors, service providers, etc.) (“External-Guests”)
- Special networks with particular access rights (admin access to IT systems, data backup network, KISTERScloud network…)

10.1 Access to KISTERS data network

[INFO] Access to the company-wide data network from the internet is only realised by means of the OpenVPN Client or Cisco VPN (for older systems). Access codes are, after prior verification, only assigned on a personal basis and only by the central IT administration in Aachen.

The data network SHALL ONLY be accessed using devices approved for this purpose by the central IT administration in Aachen and solely used for business purposes. These are usually corporate computers; private IT systems (computers, mobile devices) are excluded from access to the corporate network. Smartphones cannot be used to access the data network.

In special cases the KISTERS AG Board MAY grant an exception regarding access to the company network to KISTERS staff to use private computers subject to further conditions.

10.2 Access to Internet

[INFO] Devices that are not connected to the KISTERS data network can only access the internet via the "mnotes" network. This applies in particular to all smartphones that are authorised for accessing the user's business email via Outlook, regardless of whether they are company devices or private devices of KISTERS employees. Due to network segmentation, access to the data network via smartphones is not possible. The usage of the “mnotes” network by external third parties is not allowed.

10.3 Internet access for third parties

[INFO] Using their own devices, third parties may only access the internet using WiFi (“ExternalGuests“) on KISTERS premises.
For this purpose, temporary valid passwords MUST be requested from the IT administration.

10.4 Access to external systems / remote maintenance access

[INFO] Access to external IT systems (remote maintenance access or access to IT systems of clients or partners) is centrally managed by the IT administration in Aachen. The IT administration will provide special computers (virtual machines) for this purpose, which have been configured for access to specific client systems and which are located in separate sub-networks.

- Client systems MUST NOT be accessed directly from workplace computers but ONLY through systems provided for this purpose by the IT Administration.
- In exceptional cases, workplace computers MAY be used for access through TeamViewer; the client or partner MUST explicitly agree to this.
- Remote maintenance access users MUST be identified. The remote access SHALL ONLY be used by the persons that have been identified to the client/partner.
- Clients’ security and privacy policy and guidelines MUST be observed during the remote maintenance work. If necessary, this information MUST be obtained before starting work.
- The client MUST be made aware of staff leaving the KISTERS Group that have used remote maintenance access. The client SHOULD then decide whether new access data should be created or the existing data can be used further.
- Access codes SHALL ONLY be made available to authorised persons.

In all other respects, the requirements for handling passwords and securing access to the provided systems (logout, lock screen, etc.) shall apply accordingly.

10.4.1 Prohibition of private use

All IT components that allow access to IT systems of clients or partners SHALL ONLY be used for business purposes. Private use by staff members is FORBIDDEN. Private IT components SHALL NOT be used for access to systems of clients or partners and SHALL NOT be connected to IT systems that are intended for the access to clients’ or partners' resources.

11 Email, internet, communication software and AI assistance systems

11.1 Email

Company email addresses and mailboxes are provided to employees of the KISTERS Group as a work resource and MUST ONLY be used for company purposes; private use is not permitted. The business use includes

- internal communication within the KISTERS Group,
- external communication with external third parties (customers, partners, suppliers etc.) for business purposes,
- the registration with forums, websites, service portals, suppliers, tender platforms etc. for business purposes,
- “private use caused by business” (e.g. informing family members that their return home will be delayed),
- the facilitation of private contacts with customers, insofar as this is of direct interest to the company.

The following are not permitted, among others

- private communication with external third parties,
- the registration at forums, websites, service portals, online shops, social media etc. for private purposes,
- the use of the Outlook client on KISTERS IT systems to retrieve other, non-business email accounts and calendars.

Automatic forwarding of emails to external email addresses MUST NOT be set up.
All incoming and outgoing emails MUST be classified as business/business documents regardless of their actual content and are subject to the associated classification, control and archiving processes.
Emails have the legal meaning of a written letter and MUST clearly identify the sender. All outgoing emails MUST always be signed with a valid sender’s business signature.
[INFO] Signatures are attached centrally to outgoing emails and are not visible to the user at the time of sending. Information on this is available in KISTERS Confluence under the search term "kisters mail signature".

11.2 Internet

The internet connection of the KISTERS Group is reserved for business use. Private use of the KISTERS Group internet connection is permitted, but the following rules of conduct MUST be observed:

- Private use SHALL NOT impact orderly business operations, for instance by downloading large volumes of data.
- KISTERS staff are strictly prohibited from visiting websites or exchanging contents with third parties that
    - are in clear violation of the law,
    - have or offer pornographic contents,

- are sexually explicit or offensive,
- incite racial hatred,
- glorify or play down violence,
- glorify war, or
- may endanger the moral welfare of children or young people or impair their well-being.

- Downloading games, music and videos, and other contents that may not be downloaded due to intellectual property rights or are likely to endanger the information security is strictly prohibited.
- Copying videos, games, music and other copyright-protected content is prohibited.

These rules are self-evident forms of behaviour. If these rules of conduct are not adhered to, KISTERS is forced to completely block the use of the internet on an individual basis. If these activities result in tangible or intangible damage to the KISTERS Group, additional disciplinary and (criminal) legal measures will be taken to the extent possible within the legal limits.

11.3 Internet-based applications and Cloud services

Applications that transfer or replicate internal or confidential data from the corporate network to external IT systems MUST NOT be used unless approved by the CISO. These include internet- or Cloud-based utilities and desktop applications (e.g., Google Desktop, DropBox or similar) that temporarily or permanently store documents, file indexes or catalogues or other information and data on external IT systems. This also includes online services such as file converters, translators and services based on artificial intelligence.

Applications that automatically load files or active content from the internet onto KISTERS IT systems in a manner that is uncontrolled by the user MUST NOT be installed and used.

If the use of such a system is necessary for business reasons, the use MUST be approved by the IT Administration, the CISO and those responsible for the information concerned. Specific rules and restrictions of use MUST be established. The current list of approved software applications and services is maintained in Confluence: see “Software approved for communication and remote access”.

The use of internet-based applications operated or administered by customers or partners within the framework of joint project or cooperation work (e.g., Trello, SharePoint, GitHub, etc.) MUST be approved by the IT administration, the CISO and those responsible for the information concerned.

A permission MUST be revoked if, due to security incidents or other findings, information security or data protection cannot be guaranteed when using the application.

11.4 Communication and control software

Software such as Microsoft Teams, Skype, TeamViewer, VNC and others SHALL ONLY be used for internal and external communication if approved and maintained by KISTERS IT administration. The current list of approved software applications and services is maintained in Confluence: see “Software approved for communication and remote access”. The following security measures MUST be observed:

- Password
  - If the authentication function of the software is not linked to the central KISTERS authentication server (Active Directory), then the passwords MUST be application specific and SHALL NOT be used for other applications and systems.
- Contacts

- Since in many communication tools (e.g., Skype) the identity of the caller (sender of messages) is not secured, these tools SHALL ONLY be used to communicate with known and verified communication partners.
- Communication tools SHOULD be configured to only allow calls by contacts from the list of contacts (“buddy-list”).
- Incoming calls MUST NOT be accepted automatically.

- Data Exchange
  - Confidential or sensitive information (e.g., passwords) SHALL NOT be exchanged via chat.
  - Files with confidential or sensitive content SHALL NOT be transferred.
  - Files SHALL ONLY be received from trusted communication partners and only with activated and up-to-date virus protection program.
  - If screen content is transferred, it MUST be ensured that no confidential or sensitive data is visible in the transferred portion of the screen.
  - If web cams are used in chats, it MUST also be ensured that no confidential or sensitive data is visible in the transferred video stream.
- Links
  - Before clicking on internet links in chats these MUST be checked for trustworthiness to largely exclude the access of fraudulent or dangerous web sites.
  - In particular, internet links which have been received as a chat message outside of an active chat session MUST be checked for trustworthiness by explicit asking for confirmation from the displayed sender using different communication media (email, phone).
  - If the displayed sender does not unambiguously confirm the authenticity of the chat message, then the link MUST NOT be clicked, since the account of the sender has most likely been compromised.
- Remote control
  - Remote operation of the computer SHALL ONLY be done under observation by the user or an administrator and SHALL ONLY be carried out by a trustworthy partner.
  - To prevent uncontrolled remote access to the computer, the software SHALL NOT be executed in “host mode” (unsupervised access).
- Compromised account
  - If there is the suspicion that a user account has been compromised, the IT Administration and the CISO MUST be informed. Furthermore, the user SHOULD try to inform the provider of the affected service and to delete the compromised account completely to avoid any further misuse.
- Software
  - Unapproved software for communication, file transfer, remote access or remote operation of computers (e.g., GoToMyPC, Dameware, Radmin or others) SHALL NOT be installed or used.

11.5 Use of AI assistance systems

[INFO] AI assistance systems are systems that are based on artificial intelligence and support people in completing tasks or answering questions. Well-known examples of AI assistance systems are ChatGPT from OpenAi and Copilot from Microsoft. The voice assistants Siri, Google Assistant and Alexa are also

well-known examples that use AI. AI assistance systems do not only bring some advantages, but also some risks, particularly in terms of data protection and the protection of internal information and copyrights. The following rules need to be observed:

12 Only approved AI assistance systems SHALL be used (see Confluence). In any case, the "Corporate Policy on the Use of Artificial Intelligence Tools" MUST be observed. Especially with public AI systems, NO personal or internal company data MUST be disclosed. Employees SHOULD be trained in the use of AI assistance systems so that they understand the capabilities, limitations and risks of the systems. Employees SHOULD NOT blindly rely on their results. Ownership of content created with AI assistance systems is subject to KISTERS' intellectual property policy. Correct attribution and compliance with copyright law are essential.Installation of software

The installation of software (application programs, service programs, drivers or similar) on KISTERS IT systems is an administrative task and MUST NOT be carried out without appropriate authorization, permission, knowledge and precautions.
Before installing the software, it MUST be verified and ensured that the software complies with information security and data protection requirements and that the intended operational use is permitted by the usage and license rights.
Software that is to be installed on workstations MUST first be approved for installation by the IT administration or the CISO team and MUST be included in the list of approved software tools.
Software that is not installed and maintained by the IT administration MUST always be kept up-to-date by the system administrator; in particular, security patches MUST be installed as quickly as possible when available.
Further guidelines on this topic are set forth in the "KISTERS Information Security Guideline for Administrators and System Owners".

13 Protection from malicious software

[INFO] Malicious software such as computer viruses, worms, Trojans or logic bombs can intrude into the KISTERS IT systems in a wide variety of ways. It is therefore essential that all IT users take active measures in order to prevent an infection through or spread of malicious software, and not rely solely on the automatic virus scanner.

13.1 Measures against malicious software (proactive)

The following instructions and rules apply regardless of the IT system used. Measures marked with an asterisk (*) have already been implemented on Windows systems set up and managed by IT administration by means of group guidelines and configurations and SHALL NOT be disabled by users or administrators. Users and administrators MUST implement and adhere to these measures accordingly for all other IT systems.

- An up-to-date virus scanner MUST be installed and activated on the system (*).
- Data storage devices (USB sticks, SD cards, floppy disks, CDs/DVDs, mobile hard drives, …) of unknown or questionable origin SHALL NOT be connected to KISTERS IT systems.
- Data storage devices of trusted third parties MUST be scanned for viruses using an up-to-date virus scanner prior to first access (*).
- The hard drive MUST be scanned for viruses using a virus scanner on a regular basis (*).
    - The function “Scan for viruses” of the Explorer context menu on the corresponding drive SHOULD be used for this purpose.
- The AutoRun feature MUST be disabled for all storage devices (*).
- Display of all file types in file management programs such as Windows Explorer SHOULD be enabled. This can facilitate the discovery of possible computer anomalies.
- Running macros in standard applications (e.g., documents from word processors, tables and maps from table processors, presentations from presentation processors) SHOULD be deactivated by default. This applies in particular to documents from the internet, or from emails received from third parties, or other data exchange mechanisms. Macros SHOULD only be active if the document is from a trusted source and if the automatic virus scan has not detected any threat.
- Incoming emails are initially checked by the general spam filter, and any suspected malicious content is moved to the “quarantine”. However, sometimes malicious emails cannot be automatically detected and isolated. From experience, emails can be dangerous, especially if
    - the sender cannot be verified definitely,
    - the text does not fit the sender (e.g., English text from a German friend),
    - the reference to previous correspondence is missing or wrong,
    - they have more copies to unknown addressees,
    - they contain links to unknown or dubious web sites,
    - they prompt to carry out certain actions, sometimes in connection with the requirement of strict confidentiality,
    - multiple messages with the same subject have been received,
    - they come unannounced from unknown or unsolicited senders, or
    - terms such as “money”, “sex”, “secret”, etc. appear in the subject line.

Emails that are obviously or potentially dangerous SHOULD be forwarded as attachments to the mailbox “mailsecurity@kisters.de” and then deleted immediately. If the sender of the mail is unknown, then this sender SHOULD be blocked locally.
Furthermore, the following rules apply:

- Executable files (e.g., programs, scripts, macros etc.) MUST be saved locally at first and may only then be run or opened.

- Clearly incorrect emails or “spam emails” (e.g., email advertising) SHOULD be deleted without opening.
  Before clicking on Internet links in e-mails, they MUST be checked for trustworthiness or correctness as far as possible in order to largely rule out access to fraudulent or dangerous websites ("phishing mails").
  [INFO] When positioning the mouse over the text of the link, the link address actually hidden behind the text appears at the bottom edge of the window. The email spam filters we use (Microsoft, Mimecast) offer additional protection against dangerous Internet links by replacing the original link addresses in emails from external senders with extended or automatically generated links (URL rewriting). When these replaced links are clicked on, the original link address is not called up directly, but a security check is carried out beforehand. Forwarding is only carried out if the spam filters do not detect any obvious threat.
- Likewise, before scanning QR-codes the trustworthiness and correctness of the sender MUST be verified, since the QR-codes may also point to fraudulent or dangerous websites.
- Alleged external virus reports SHOULD NOT be forwarded by email since in most cases these are hoaxes and IT administration will usually have been made aware of current viruses.

- [INFO] Internet browsers also offer some degree of protection against viruses. However, browser security settings must be adjusted on a high level of protection in order to disable active content (Java, ActiveX and JavaScript) that can contain viruses. Since this always hampers web browsing – e.g., constant prompts about whether a page should really be opened or even the refusal to open certain pages – these features are disabled by default by the manufacturer. This means that browsers can only protect against viruses if the user has previously adjusted basic settings accordingly.
- Files on the internet SHALL ONLY be downloaded from trusted websites such as the original pages of software and hardware manufacturers, public institutions, partners, etc.
- Applications, drivers or other executable files MUST ONLY be downloaded installed under observance of the “KISTERS Information Security Guideline for Administrators”.
- Applications which are not purchased and installed by the system administration MUST ONLY be downloaded and installed after check and release by the CISO.
- Applications for which KISTERS does not hold a valid commercial or “public domain” license MUST NOT be installed.
- Applications no longer required MUST be removed from the IT systems in any case.

[INFO] In most cases, a virus can be identified by its impact and damage. These include:

- Abnormal PC behaviour
- Unexpected delays when running certain programs and fetching data
- Unexplained drop in the available space in the main memory or on the hard disk
- Very long response times in the program flow
- Very high CPU, disk or network load without any user activity

- Unexplained crashes in so far perfectly running programs
- Incorrect or changing screen appearance
- Modified or missing files or programs

[INFO] To scan a suspicious file which the virus scanner has deemed no threat, the following websites may be used for instance:

- https://www.virustotal.com/gui/home/upload/
- https://internxt.com/virus-scanner/
- https://metadefender.opswat.com/
- https://www.hybrid-analysis.com/

However, privacy-relevant confidential data (files containing client data, passwords, etc.) SHALL NOT be uploaded to and scanned on the above websites!

13.2 Measures in case of suspected malware attack (reactive)

The following steps SHOULD be taken if you suspect that your computer has been infected with a virus:

1. Stay calm! Never follow messages that appear on the screen, such as prompts to format your hard disk. Oftentimes, a greater damage is done by panic reactions than by the virus itself.
2. Immediately immediately disconnect all network connections: Activate airplane mode, switch off WiFi/Bluetooth, unplug the network cable. In particular, all connections to the KISTERS network must be disconnected!
3. Do not start any further programmes and do not open any further files!
4. Your IT administrators MUST BE informed by phone(!) or via another channel that is independent of the affected device. Have the following information on hand:
   4.1. What device are we talking about, where is it and how was it and/or is it currently incorporated into the corporate network?
   4.2. How was the virus detected (virus scanner, messages/comments in documents, crashes, error messages, etc.)?
   4.3. If detected by virus scanners: What kind of virus has been detected?
   4.4. What was the possible virus source (email, website, download, network, USB stick, CD, etc.)?
   4.5. Could it be that the virus has been transferred to others (via email, USB stick, network, CD, etc.)?
   4.6. Wait for further instructions of your IT administrator.
5. If you have an internet connection, you can have your computer tested using an scanner available online after consultation and on the instructions of the IT administrators:
   5.1. https://www.trendmicro.com/de_de/forHome/products/housecall.html/
   5.2. https://www.eset.com/de/home/online-scanner/
   If available, a log file shall be saved and forwarded to the central IT Administration in Aachen in order to identify other vulnerable systems and eliminate the virus as soon as possible.
6. Hand over your computer to the IT administration for securing of evidence and potentially further forensic investigation by external specialists.

14 Notifications of security events and incidents

[INFO] Despite using one's best efforts, adverse conditions can lead to security measures not to be observed at all or in part or to implemented measures not being sufficiently effective ("security events").

One individual or a series of security events can lead to a "security incident", in the case of which information, IT systems or processes are likely to be compromised and information security is under threat. Each individual employee MUST promptly report observations or discoveries that may be or are actually related to security events and incidents to the responsible staff members. These are:

- The CISO or Data Protection Officer or the BCMO in his function as deputy CISO,
- the Head of IT,
- the IT administrators (for security events / incidents related to IT systems),
- depending on the situation, also team leaders, system managers, site managers, business unit managers and the KISTERS Board.

For reporting general security incidents, the Jira Service Desk Information Security SHOULD be used as far as possible, for reporting IT-specific security incidents the Jira Service Desk System Administration.
If clients or partners are affected by the security events or incidents, they shall be notified by the CISO/Data Protection Officer or an authorized representative as soon as possible.
If possible, measures SHOULD also be taken to remedy or contain possible damage:

- Independent personal rectification of deficiencies, e.g.
  - Closing open entrances (windows, doors, etc.),
  - Securing information (e.g., printouts on printers, flipcharts, etc.),
  - Blocking/shutting down unused/unprotected IT systems if possible;
- Pointing out potential errors caused by the lack of attention or lack of awareness to colleagues,
- Notifying the supervisor and the person responsible for the information or system affected, if known.

14.1 Whistle blowing

If an employee wishes to report a security event related to a suspected or actual violation of national and international laws, regulations or ethical standards, this event SHOULD be reported to the internal reporting office in accordance with the KISTERS Whistleblowing Policy. The whistleblowing team MUST, while maintaining the confidentiality of the reporting person, follow up on this report and inform the relevant responsible parties in order to prevent or at least mitigate any potential damage.
For reporting, the Jira Service Desk Whistleblowing SHOULD be used as far as possible.

15 Disciplinary actions

If, during the analysis of a security event or incident by the CISO, BCMO or Head IT, the suspicion arises to the effect that the cause lies in the culpable conduct of an employee, e.g., through potential violations of laws, rules, regulations or internal guidelines, the responsible MUST investigate the case further.
If the suspicion is confirmed, the responsible person MUST take further action:

- In the case of slightly negligent conduct with minor damage, employees MUST be advised of the relevant guidelines. This MAY be done directly by the CISO, a representative or the employee's immediate supervisor.
- In case of slightly negligent behaviour with high damage, the immediate supervisor and the management of the business unit concerned MUST be informed. The latter CAN issue an admonition and initiate the suspension or revocation of existing access rights. Furthermore, the management of the Business Unit MAY inform the KISTERS Board.

- In the case of grossly negligent or intentional actions that threaten the security of data, information, applications or IT systems, the KISTERS Board MUST also be informed. Such actions are for example:
    - misuse of data that can cause financial loss,
    - unauthorised access to or alteration and transmission of information,
    - illegal use of information from the KISTERS Group,
    - endangering the information security of the KISTERS Group or business partners,
    - endangering the data protection of employees or business partners,
    - damaging the reputation of the KISTERS Group or its business partners.

The KISTERS Executive Board MAY impose further disciplinary and labour-law action such as written warning or termination for special reason.

Independently of the disciplinary measures, further steps MAY be taken, such as civil and criminal proceedings, in which liability claims and recourse claims may also be asserted.

16 Additional applicable documents

- KISTERS Classification of Assets - Physical, Logical and Data Access Control (part of this guideline)
- KISTERS Password Guideline (part of this guideline)
  KISTERS IS Guideline for Administrators (extension of this guideline for all employees with administrative rights on KISTERS IT Systems)
- KISTERS IS Guideline for Dealing with External 3rd Parties (extension of this guideline for all employees who are the contact persons for customers, partners, suppliers and service providers)
- KISTERS IS Policy and Guideline on Cryptographic Controls (extension of this guideline).
- Corporate Policy on the Use of Artificial Intelligence Tools
- KISTERS Whistleblowing Policy

17 Document history

This document is checked at least once a year to ensure that it is up to date and amended if necessary. The official version of this document is managed online. Before using electronic copies or printed versions, these must be checked to ensure that they are up to date.

Version	Date	Editor	Action
5.6	2025-07-10	J. Rade	Additions in the area of data protection, addition of regulations on voice assistants, privacy screens and AI assistance systems, addition of BCM in the area of compliance with the obligation (in projects)
5.5	2024-10-18	J. Rade	Addition of mailbox “mailsecurity@kisters.de” as contact address for forwarding and processing (potentially) malicious emails.
5.4	2024-09-05	H.-J. Schlebusch	Approval of facial recognition for unlocking smartphones, additions: time limit for exceptions, internet services requiring approval, additional applicable documents
5.3	2024-07-18	H.-J. Schlebusch	Additions: installation of software (release), correction: behaviour in case of suspected malware

Version	Date	Editor	Action
5.2	2023-11-14	H.-J. Schlebusch	Handling of deviations and exceptions; various minor corrections and additions
5.1	2023-09-08	H.-J. Schlebusch	Extension “contact persons”; amendment of “acceptable use”; adaptation of “whistle blowing” to comply with “Whistleblowing Policy”
5.0	2022-09-19	H.-J. Schlebusch	Use of recording devices supplemented, use outside KISTERS business sites specified, adjustments due to use of cloud services, various editorial changes.
4.4	2021-08-24	H.-J. Schlebusch	Information on encryption of mobile data storage devices
4.3	2021-03-12	H.-J. Schlebusch	Review, minor editorial corrections
4.2	2020-11-11	H.-J. Schlebusch	Adjustments for conversion of email from IBM Notes to Outlook
4.1	2020-08-04	H.-J. Schlebusch	Amendments on usage of email, Home-offices; transport and use outside KISTERS locations
4.0	2020-04-17	H.-J. Schlebusch	New chapters: Software installation, private devices; Extensions: additional guidelines for teleworking sites, “confidentiality” of 3rd party business data
3.9	2020-01-14	H.-J. Schlebusch	Extension to unlocking of smartphones
3.8	2019-07-15	H.-J. Schlebusch	Use outside KISTERS premises; use of internet-based services in co-operations
3.7	2019-03-08	H.-J. Schlebusch	New Chapter “Disciplinary Actions”, minor error corrections
3.6	2018-08-08	H.-J. Schlebusch	Data Protection, backup vs. archive, editorial changes
3.5	2017-11-15	H.-J. Schlebusch	Concretization “Clean desk - clear screen”
3.4	2017-07-20	H.-J. Schlebusch	Securing of evidence
3.3	2017-07-09	H.-J. Schlebusch	Disciplinary actions, Bluetooth/NFC for mobile devices
3.2	2017-04-19	H.-J. Schlebusch	“KISTERS Information Security Guideline for Administrators” as separate document
3.1	2017-01-30	H.-J. Schlebusch	Minor additions and modifications after review Chr. Aust
3.0	2016-11-10	Bernd Kisters, H.-J. Schlebusch	Restructuring of the document; separate documents for “KISTERS Password Guideline”, “KISTERS Physical, Logical and Data Access Control”
2.3	2016-10-05	Bernd Kisters, H.-J. Schlebusch	Various additions; IT Security -> Information Security; Key terms as per RFC2119
2.2	2016-06-08	Bernd Kisters	Revision/Amendments
2.2	2016-07-04	H.-J. Schlebusch	Intranet Publication
2.1	2016-06-03	H.-J. Schlebusch	Scope, Amendment for communication tools
2.0	2015-10-09	H.-J. Schlebusch	Revision according to ISO 27001
1.0	2013-08-09	Bernd Kisters	Creation