KISTERS
Policy on
Information Security, Data Protection and Business Continuity

v.4.1, 2025-09-22

Owner:

KISTERS CEO

Table of contents

1 Introduction

The KISTERS Group, consisting of the KISTERS AG headquartered in Aachen, Germany, and its national and international subsidiaries, is a worldwide successful provider of software and hardware solutions and professional services. The KISTERS portfolio includes solutions for sustainable resource management of energy, water, weather and environment, for occupational safety and compliance; software solutions for 3D viewing, IT Hardware such as large-format printers (3D/2D) and scanners as well as professional services in environmental consulting (urban water management, municipal civil engineering, infrastructure development and hydrology engineering). KISTERS also provides professional services to complement its hardware and software solutions, including the operation of KISTERS software solutions in the KISTERScloud.

2 Motivation and objectives

Information and its processing are key for our ability to fulfil our business activities. Therefore, the protection of this information, especially of personal data, against unauthorized access, illegitimate modification or distribution as well as non-tolerable unavailability is essential.
All of our significant strategic and operational functions and assignments are substantially supported by IT systems. An outage or a compromise of these systems must be avoided or at least compensated for in the short term such that the course of business is sustained or restored as fast as possible.
As a provider of software solutions and KISTERScloud services, we assume responsibility not only for our own information security, but also for the information security of our clients and partners. It is therefore necessary to develop our solutions and KISTERScloud services according to the security requirements of our clients and partners and to design the development processes, tools and environments accordingly. This applies in particular to software solutions deployed for the processing of personal data or as critical components in the field of critical infrastructures.

Therefore, the KISTERS Board has adopted this policy on information security to incorporate information security, data protection and business continuity as important components of our corporate strategy.

2.1 Information security

The objective of information security within KISTERS is to support the protection of our organization and our business activities by:

- the assurance of confidentiality, integrity, availability and authenticity in our information, processes and systems,
- the protection of our interests and our trustworthiness in the eyes of our clients through securing our work capacity as it relates to our IT systems, programs and data, as well as products and services,
- the protection of our clients' and partners' interests through the secure and continuous deployment of our software solutions, systems and services as well as our confidential treatment of all their company data,
- the protection of the interests of the users of our software solutions by complying with information security regulations in our software solutions, consistently applying best practices and principles of secure software development and securing our development environments,

- the protection of our organization, our clients, partners and employees through compliance with applicable statutory regulations and other legally binding provisions.

From this we have as derived goal to guarantee

- the confidentiality of this information, especially of personal data,
- the availability of our infrastructure and our entire business information,
- the integrity of all IT systems and information,
- the authenticity of all actors and stakeholders involved in information processing,
- the information security of our software solutions,
- the protection of our business against data loss and information leak.

2.2 Data protection and privacy

The protection of natural persons in relation to the processing of personal data is a fundamental right. The objective of data protection and privacy within KISTERS is to guarantee:

- the protection of all personal data of clients, partners, suppliers and employees in our IT systems and processes to ensure the informational autonomy and the protection of privacy of all data subjects,
- the protection of the interests of the users of our software solutions and KISTERScloud services by complying with data protection regulations in our software solutions.

2.3 Business continuity

In case of an emergency or a crisis, our business processes or the fulfilment of our assignments are at risk due to the lack or non-availability of resources like staff, information, infrastructure and service providers. However, our clients, partners, staff and other stakeholders expect that KISTERS takes appropriate precautions to quickly, systematically and adequately limit and repair any damage incurred. The non-availability of essential resources has to be compensated for in the short term such that the course of business is sustained or restored as fast as possible.

The objective of business continuity management within KISTERS is to maintain our business activities and the fulfilment of our contractual obligations during emergencies to:

- protect our staff at all times during emergencies,
- enable the continuous execution of all our critical business processes,
- enable the continuous fulfilment of our assignments and the delivery of our services such as support and KISTERScloud operations to our clients and partners,
- maintain our interests and our trustworthiness in the eyes of our clients and partners by adequate and systematic emergency planning,
- mitigate any negative consequences of emergencies for clients, partners and suppliers,
- mitigate or compensate for emergencies at our clients, partners and suppliers which affect our business activities or services,
- keep personal data protected from leakage, misuse and manipulation.

This shall be achieved by proactive/preventive measures and controls (emergency planning) as well as reactive measures (emergency response) to

- enhance the resilience of our business processes and service provisioning against disrupting interference,

- continue critical business processes and services – potentially in reduced or limited form – during emergencies.

3 Scope

This policy defines the KISTERS general strategic approach to a manage information security, data protection and business continuity. It applies to all business units, locations and employees of the KISTERS Group, including our entire IT infrastructure and the IT systems operated herein.

4 Roles, responsibilities and dependencies

The overall responsibility for information security, data protection and business continuity is carried by the Board of KISTERS AG. The Board of KISTERS AG supports the systematic pursuit of the security goals by establishing an organisation for the development and operation of a management system for information security management (ISMS), data protection management (DPMS) and business continuity management (BCMS).

The Board delegates the implementation of the management system to formally assigned officers, which report directly to the Board of KISTERS AG:

- The KISTERS Chief Information Security Officer (CISO) is responsible for the development and execution of the information security concepts and the surveillance over their compliance.
- The KISTERS Data Protection Officer (DPO) is responsible for the development, execution and supervision of data protection concepts to ensure compliance of all business activities with applicable data protection and privacy regulations.
- The KISTERS Business Continuity management Officer (BCMO) controls and contributes to the activities regarding the emergency preparation for the KISTERS. He is responsible for the development, implementation, maintenance and continual improvement of the business continuity management and its associated processes and documents.

The appointed officers are designated as mutual substitutes. They are supported by information security teams and business continuation teams (IS teams, BCM teams) who are responsible for the implementation of this policy in specified business or application areas. IS teams and BCM teams are assembled according to roles and responsibilities for individual business or application areas.

The Board shall make ample financial and temporal resources available to the officers and the IS teams and BCM teams in order that they may regularly advance their knowledge, to keep informed and to achieve the objectives on information security, data protection and business continuity that the Board has specified.

The officers are to be included at an early stage in all projects in order to already consider aspects of information security, data protection and business continuity during the planning stages.

The IS teams, BCM teams and the officers are to be supported in their work by all employees. Employees must hold to the instructions of the officers in all matters relating to information security, data protection and business continuity.

5 Applicable legal and other requirements

The requirements on information security, data protection and business continuation are defined by the requirements of stakeholders, regulatory requirements, our business objectives, and industry best practices. The most relevant stakeholders are clients, partners, suppliers and employees.
Due to the variety in services offered by KISTERS and its worldwide business operation, the requirements from stakeholders and authorities may vary depending on the specific circumstances. Stakeholder requirements are manifested in individual contracts which must be considered for executing this policy. National and international laws and regulations applicable to KISTERS business operations or service offerings are reviewed regularly by the assigned officers or delegated specialists. A cadastre of applicable laws and regulations is maintained within the ISMS.
For the compliance with industry best practices, we align our systems and business practices to national and international standards such as ISO/IEC 27001, ISO/IEC 22301, BSI Grundschutz, BSI Standard 200-4, SOC 2, BSI C5, AICPA SOC 2 and other applicable frameworks. Whenever required and feasible, we are aiming to pursue independent audits and certifications according to these standards.

6 Controls and procedures

The KISTERS information security policy follows the principle that the effort taken on controls and processes must always be set in relation to the achieved gain in security, the benefits of the affected stakeholders and the value of the assets to be protected. All security controls shall be chosen in such a way that they are suitable and appropriate. They shall minimize the risks as much as possible and shall stand in a suitable relationship to the costs or loss that might result in case a damage occurs.
The controls and procedures outlined in this policy shall be elaborated by additional specific guidelines, work orders and other suitable regulations.

6.1 Information security

For all operational assets - information, processes, IT applications, IT systems, etc. – system or service owners shall be appointed who determine the respective protection requirements, classify information and assign access authorizations. For all responsible functions, substitutes shall be nominated. It must be established through briefings and adequate documentation that system and service owners and their substitutes are able to fulfil their assignments.
Based on the analysis of protection requirements as well as identified and evaluated risks, appropriate personnel, organizational and technical controls shall be defined.
Buildings and rooms shall be protected through adequate access controls. The access to IT systems shall be protected through appropriate access controls and the access to information through a restrictive authorization concept, especially in case of personal data.
Computer virus protection programs shall be installed on all IT systems. All internet gateways shall be protected with a suitable firewall. All protective programs shall be configured and administrated so that they present effective protection and that unauthorized access and manipulation is prevented. All IT systems shall be monitored in order to be able to detect possible security events as quickly as possible. Furthermore, IT users shall support these security measures by working in a security-conscious manner and shall inform the corresponding contact persons in the event of anomalies.

Data losses can never be completely ruled out. Comprehensive data security shall assure that IT operations can be restored quickly if parts of the operational data pool are lost or obviously defective. In order to limit or prevent damage or loss for KISTERS or KISTERS clients as a consequence of security events, the response to security events must happen quickly and resolutely following an established incident management process. Emergency controls shall be summarized in an emergency preparedness concept. Our goal is to maintain or own critical business processes as well as those of our clients, especially KISTERS-cloud clients, and restore the availability of failed systems within a tolerable period of time. This shall be supported by the backup of information and IT systems and tested recovery procedures for critical systems.

To the extent that services are outsourced to external third parties, specific information security requirements shall be prescribed in the contractual agreements. The right to control shall be established.

The software development considers the aspects of information security and data protection in the entire development process, from the requirement capture up to the delivery and the operation of the software solutions. Regulatory requirements as well as those of our clients and current "best practices" are considered in the design and programming and verified by appropriate quality assurance. The development environments shall be protected against unauthorized access and the integrity of the deliverable software solutions shall be guaranteed.

KISTERS employees shall regularly participate in training on information security and information security as well as the correct usage of IT services and the security controls related to them.

6.2 Data protection and privacy

The handling of personal data shall follow the principles of transparency, the necessity of the processed data, data avoidance and data minimization. As a matter of principle, the collection, processing or use of personal data shall only be carried out to the extent that this is necessary for the establishment, execution or termination of business activities by KISTERS. Personal data shall only be processed or used in accordance with the intended purpose which is known to the data subjects. A change or extension of the intended purpose shall only be made if it is legally permissible, the data subjects have been informed thereof and if the data subjects have given their consent.

6.3 Business continuity

To achieve the objectives of business continuity management, the business processes, services and assets are analysed, their criticality for the organization classified, and critical resources supporting them identified. The goal is to establish measures for emergency prevention and emergency response and to provide corresponding resources which are adequate and economically feasible. The evaluation shall account for the relevant requirements and constraints, such as statutory, contractual or regulatory requirements.

As a general strategy, the implementation of proactive measures shall be preferred where possible and economically feasible, to reduce the likelihood and/or impact of emergencies to the minimum possible. However, since there is no way to fully exclude the occurrence of an emergency, adequate plans for emergency responses shall be in place.

A business impact analysis (BIA) shall provide information about critical business processes and resources. For these critical processes and resources, the impact of a partial or complete loss or failure shall be eval-

uated as a function of time. The BIA shall be carried out individually for each scope of interest. The evaluation shall also consider dependencies between the identified scopes as well as dependencies on external suppliers and service providers.
The analysis shall be used to define emergency recovery goals, which include the Recovery Time Objective (RTO), the Recovery Point Objective (RPO) and the minimum amount of replacement resources (staff, information, infrastructure and service providers) which have to be available during an emergency to achieve the required level of recovery.
A BCM risk analysis (BCM-RA) for all identified resources of critical processes shall be carried out to determine the possibility of implementing preventive measures and provide guidance on their priority.
Based on the results of BIA and BCM-RA, possible strategies and solutions to support business continuity are developed. From these, strategies and solutions to be implemented are selected, and their implementation will be developed and described in Business Continuity Plans (BCP) and Emergency Procedures (EP).

7 Continual Improvement

For continuous improvement of information security, data protection and business continuation management, the entire ISMS shall be regularly checked for actuality and effectivity. In this context, internal and external changes and developments must be taken into account, among other things with regard to customer requirements, regulatory requirements, threat situations, the geopolitical situation or climate change, the state of the art or internal organization of the KISTERS Group. Besides that, the controls taken shall also be examined regularly to see whether affected employees are familiar with them, whether they are feasible, and whether can be integrated into the operational processes.
Through a continuous revision of the regulations and compliance with them, the desired level of information security, data protection and business continuation shall be established. To that end, internal and external audits, including security tests and exercises on emergency management and recovery procedures, shall be conducted. The results of the revisions and audits shall be used to identify opportunities for further improvements of the information security, data protection and business continuation.

8 Obligation and Effective Date

All employees of the KISTERS Group are obliged to actively contribute to information security, data protection and business continuation management and to comply with the corresponding guidelines. Grossly negligent and intentional violations of the guidelines by employees or third parties shall be prosecuted and penalized to the extent legally possible.

This revision of this policy has been adopted by the Executive Board of KISTERS AG and comes into effect the day after its publication.

Aachen, Oct. 01, 2024

Klaus Kisters, CEO, KISTERS AG

9 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
4.0	2023-08-29	Klaus Kisters	Review and Release
4.0	2023-08-29	H.-J. Schlebusch	Extensive rework due to merge of IS- and BCM-Policy
3.6	2022-07-18	Klaus Kisters	Review and Release
3.6	2022-07-18	H.-J. Schlebusch	Explicit reference to KRITIS, error corrections
3.5	2021-07-30	Klaus Kisters	Review and Release
3.5	2021-07-30	H.-J. Schlebusch	Editorial changes and error corrections
3.4	2020-08-25	Klaus Kisters, H.-J. Schlebusch	Review and Release without changes
3.3	2019-07-29	Klaus Kisters	Review and Release
3.3	2019-07-29	H.-J. Schlebusch	Business Division “Environmental Informatics” removed
3.2	2019-02-19	Klaus Kisters	Review and Release
3.2	2019-02-14	H.-J. Schlebusch	Additions for software development
3.1	2018-05-20	Klaus Kisters	Review and Release
3.1	2018-05-10	H.-J. Schlebusch	Error corrections
3.0	2018-03-20	Klaus Kisters	Review and Release
3.0	2018-01-31	H.-J. Schlebusch	Extensive rework under specific consideration of the protection of personal data
2.0	2016-11-04	Klaus Kisters	Review and Release
2.0	2016-09-15	H.-J. Schlebusch	Extensions and Adaptations: KISTERS AG -> KISTERS Group; IT-Security -> Information Security
1.0	2015-09-01	Klaus Kisters	Review and Release
1.0	2015-08-21	Klaus Kisters H.-J. Schlebusch	Creation