Information Security Management System

Information Security at Bühler

V3.0, July 2025

Information Security at Bühler

Scope and purpose of this document

Information, data and its supporting processes, information systems and networks are vital to the business of Bühler and our customers and other business partners. The preservation of confidentiality, integrity and availability of valuable information is even more important the more business processes are digitalized. This document describes the approach of Bühler to safeguard information and data Bühler is processing about or on behalf of our customers.

The most recent version of this document can be found in the Information Security section on www.buhlergroup.com.

Information Security Management System

Bühler operates an Information Security Management System (ISMS) which is **certified according to ISO/IEC 27001:2022** (herein referred to as "ISO standard"). The certification scope covers the design, development and operations processes of the internal IT services, myBühler, Bühler Insights, Mercury, Data Science and Joint Forces. In the next chapters, you will find a description of the information security management processes structured along the chapters of the ISO standard and how Bühler has implemented these requirements.

Context of the Organization

Bühler identified and manages the interested parties and internal and external issues that have interest or relevance to Bühler's information security. This includes for example customers, employees the current activities in the digital business, political, regulatory and economic changes, etc.

Leadership

Information security is a top priority for Bühler. Senior management is closely involved in the operations of the ISMS. Regular reporting of the ISMS ensures that management is aware of new risks or potential issues within the management system.

Policy

The company management regularly releases a set of information security policies, which are valid and mandatory for every employee and every contractor in the Bühler Group. The policies include all relevant topics such as acceptable use of IT assets, handling of (customer) information/data, technical requirements for IT systems or access management.

Organizational roles, responsibilities and authorities

The ISMS is governed and managed by the ISMS Steering Committee which contains members from all relevant departments such as senior management, digital business, information technology, legal, compliance, human resources and business representatives.

The roles and responsibilities regarding information security for every employee up to the Board of Directors are defined in our policies.

Planning

An information security risk management process ensures that threats and vulnerabilities are identified, tracked and their mitigation follows a clearly defined process.

Bühler aims to reduce risks whenever reasonable and other risk treatment options such as acceptance or risk sharing with third parties (e.g. via insurance) are only applied when risk levels are within tolerable limits.

Objectives regarding information security are defined, measured, evaluated and reported at regular intervals to ensure the ISMS is always achieving its intended outcomes and expectations.

Support

Bühler has a dedicated information security team lead by the Head of Information Security (CISO) which has global authority for the whole Bühler Group regarding information security.

Every employee (internal and external) which is using Bühler IT resources or has access to sensitive information is required to perform computer-based information security training as part of the onboarding process. Additional computer-based or classroom trainings take place when an additional need is identified.

The information security team is maintaining an Intranet site where news or educational content about information security is distributed to all employees.

Operation

As the core of the ISMS, information security-relevant risks are identified and reviewed, and the relevant risk treatment activities are planned and tracked until they are completed, and the risk level has reached an acceptable value.

Performance evaluation

ISMS performance and effectiveness evaluation is following defined metrics and intervals and is reported to senior management. Potential adjustments of the ISMS are defined within the ISMS Steering Committee and carried out by the responsible teams.

Bühler has a defined process to perform internal ISMS audits, which are following a defined and approved audit program to ensure that all relevant in-scope areas are audited as required by the ISO 27001 standard.

The ISMS Steering Committee performs regular management reviews of the ISMS where the effectiveness of the ISMS, changes in internal/external issues, the status of nonconformities and risk management activities, etc. are analyzed and potential necessary activities are defined and initiated.

Improvement

The ISMS is continuously adapted to ensure continuous improvement of the ISMS and information security maturity.

Technical and organizational measures

Besides the main clauses in the ISO standard, where the general and formal requirements of an ISMS are defined, the “Annex A” defines 93 controls in 4 controls chapters which cover the relevant topics of information security. Such controls are countermeasures or safeguards and can be for example tools, processes or policies. Below you can find information about how Bühler addresses these controls.

A.5 Organizational measures

Chapter 5 of Annex A describes the organizational measures necessary to establish and maintain an effective information security management system in a company like Bühler. These measures include the development and regular updating of information security policies and the assignment of responsibilities for security management. The CISO and the Information Security team are responsible for implementation. It emphasizes that Bühler's management is actively involved in the implementation of security measures and that the interests of relevant parties are taken into account.

In addition, Bühler has conducted an inventory and control of information assets (asset management) and implemented appropriate protective measures. Raising awareness and training of employees regarding information security is also of central importance and takes place continuously. Security requirements are integrated into human resources processes, and applicants are screened for security risks.

The risk management process was also implemented, which includes the identification, assessment, and treatment of risks and is regularly reviewed and adjusted. This process has been extended to include and manage 3rd party and supplier risks

Supporting processes are established for identity and access management, threat intelligence control, security monitoring for detection and response or interest groups and governmental cyber security authority exchanges are followed to learn about new threats and trends.

Furthermore, procedures are in place to ensure legal or regulatory compliance including intellectual property rights.

Overall, these measures are crucial to ensuring information security at Bühler and protecting the integrity, confidentiality, and availability of company information. Through systematic implementation and regular review, Bühler protects its information assets against threats and vulnerabilities.

A.6 Personal measures

Chapter 6 of Annex A describes security-related measures related to personnel, which are also of great importance to Bühler. It stipulates that clear roles and responsibilities regarding information security must be assigned within Bühler and have been assigned.

Before hiring, candidates will undergo a thorough screening process depending on their role to ensure they are suitable for handling sensitive information. Bühler employees will be regularly informed about security policies and procedures as well as confidentiality rules through training and awareness programs. This includes the understanding that violations of information security policies may lead to appropriate disciplinary action.

Upon the departure of an employee or upon a change of employment, measures will be taken to ensure that access to information is terminated in a timely manner and that confidential information remains protected.

Overall, these measures aim to minimize personnel risks and ensure information security at Bühler.

A.7 Physical measures

Chapter 7 of Annex A covers the physical and environmental security measures necessary to ensure the physical security of information within an organization like Bühler and to minimize threats such as unauthorized access, natural disasters, and other physical hazards. Bühler implements entry control measures to ensure that only authorized personnel are granted access to sensitive areas. These include access control systems such as card readers and security guards.

In addition, Bühler restricts physical access through the use of barriers such as fences, doors, and locks, and uses security locks and alarm systems to prevent unauthorized access. The company also ensures that risks from fire, floods, earthquakes, and other natural disasters are minimized by implementing fire protection systems, monitoring temperature and humidity, and developing emergency plans.

Bühler defines security zones with different security levels and implements additional access controls and monitoring measures within these zones. Another important aspect is equipment security. Bühler protects information processing equipment from physical damage and theft, performs regular maintenance, and stores equipment securely. When transporting information and equipment, the company ensures its protection by using secure transport containers and procedures to prevent data loss and theft.

These physical measures are essential components of a comprehensive Information Security Management System (ISMS) at Bühler, which is compliant with ISO 27001, and help ensure the physical integrity and availability of information.

The main datacenters of Bühler which host the central and business-critical IT services are managed by professional datacenter providers with adequate information security certifications such as ISO/IEC 27001and SOC II.

On-premises datacenters follow defined policies and are secured by physical access controls and specific equipment such as cooling systems, fire extinguishers, UPS, etc.

A.8 Technical measures

Chapter 8 of Annex A focuses on technical measures to ensure information security. These are particularly important for Bühler to protect the integrity, confidentiality, and availability of data. Bühler's systems are fault-tolerant and quickly recoverable, with robust backup and recovery strategies in place.

The Bühler corporate network is centrally operated and has harmonized equipment in place. Network security related

controls such as URL and malware filtering add an additional level of defense to prevent threats to the IT infrastructure.

Access to the Bühler corporate network is restricted to registered systems and assets are operated in segregated network zones.

All endpoints and all on-premises- or cloud-based services are closely monitored on availability and security events. Specialized teams are responsible for the detection and response of any off-standard activity.

Encryption technology is used to protect sensitive information, for example by encrypting the local disks of client and desktop computers and by using a global company network with encrypted connections between all locations. For web applications reachable over public networks “https” or equivalent TLS enforced protocols with strong encryption levels are required by our policies.

Global password standards are defined, and strong authentication methods (for example multi-factor authentication) are used to access critical services, i.e. if they are reachable from public networks or process sensitive information.

A secure development process is maintained and adapted by the different development teams. This process also includes defined activities and output requirements for the different phases of the software development processes. Source code is regularly checked for vulnerabilities with automated tools and manual code reviews/approvals ensure that four-eyes principle is followed for code changes.

External and internal penetration tests are carried out to identify potential security issues in software or services.

Bühler Digital Solutions

In addition to the general information security controls mentioned in the chapters above the following specific controls are applied in our Digital Solutions to ensure customer data is protected.

The software development and operations activities follow the defined policies and processes and are certified according to ISO 27001.

Bühler Insights

Bühler Insights is the strategic platform for Bühler's digital solutions provided to customers. Bühler Insights collects telemetry data from machines at customer sites with an edge gateway and transmits the data to the Bühler Insights platform. On the platform, the data is stored and processed, and customers can access various visualizations of the data in respective dashboards.

Transparency and control

All activities on Bühler Insights are logged to ensure the traceability of any action taken. Any activity can only be performed by authorized operators who must securely authenticate to the services. None of the data is forwarded to third parties without anonymization or consent of the customer.

Encrypted communications

The main communication between customer installation and Bühler Insights is performed directly or by gateways as intermediary systems. Algorithms used for encryption may vary over time and implemented devices/equipment. Adequate encryption is applied when data is transmitted over public networks (i.e. AES-128, RSA 2048bit keys, SHA256 hashing, TLS 1.2 or better). Where applicable data is also encrypted at rest with securely stored keys.

Microsoft Azure

The infrastructure of Bühler Insights is based on Microsoft Azure services. Azure holds multiple state-of-the-art information security certifications such as ISO 27001, 27017 and 27018 and SOC for the processes and activities Microsoft is responsible for. The full list can be found here.

For the activities Bühler is responsible for, the ISMS and information security controls are certified according to ISO 27001 apply.

myBühler

The myBühler customer portal is the digital gate for our customers, thereby making it your entry point to the digital solution portfolio of Bühler. Available in more than 170 countries worldwide and 8 languages, more than 9,000 customers enjoy easy ordering of spare & wear parts and access to information about installed machines, parts, orders, and important documentation like spare parts catalogs and user manuals. The software development and operations activities follow the defined policies and processes and are certified according to ISO 27001.

Automation Solutions

Mercury MES

Mercury MES forms the automation basis for customers who are on one side operating with complex processes and on the other side need a high automation degree. Mercury enables a seamless exchange of information throughout all production process systems. Supported by Bühler, customers can optimize workflows through communication between enterprise resource planning (ERP), quality control, maintenance, and other systems. Data availability and real-time feedback enable smart decision-making enhancing plant performance and productivity. The software development process and other applicable activities for this new web-based automation platform follow the globally defined policies and are certified according to ISO 27001.

Joint Forces - PlayOne

PlayOne is Bühler's advanced HMI software platform, designed to make machine operation simple, intuitive, and user-friendly. Used throughout Bühler to build diverse standardized machine HMIs, PlayOne ensures a consistent and streamlined experience for operators. The platform provides a wide range of functionality and supports standard interfaces of the industry e.g. OPC UA for easy integration into higher-level control systems but also for data exchange with any kind of cloud-based platforms. The HMI software platform development follows secure software development policies and processes and is certified according to ISO 27001.

AI & Data Science

Bühler AI & Data Science platforms use digital technologies to drive business excellence and optimize processing lines globally. Building on Bühler's processing and manufacturing expertise, the team combines data with advanced machine learning methods to develop AI-powered solutions for established industry and business pain points. The software development, data handling, and operations activities follow defined policies and processes and are certified according to ISO 27001.

IT Services

The internal IT services are operating all IT infrastructure and applications for Bühler globally. To ensure all valuable information is protected at any time the ISMS includes the controls applicable to the internal IT activities provided by the five IT Service Centers and are certified according to ISO 27001.

Shared Responsibility

To protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Bühler products and solutions only form one element of such a concept.

The customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Bühler products and solutions undergo continuous development to make them more secure. Bühler strongly recommends applying product updates as soon as they're available and to always use the latest product versions. This does not apply to Digital Services and/or the underlying systems and components, including Embedded Software, which are updated by Bühler.

The use of product versions that are no longer supported and failure to apply the latest updates may increase customer's exposure to cyber threats.

Further Information

In case you want to have more detailed information about information security please get in contact with your sales representative or via the contact form. Bühler may not share sensitive details about information security but possibly specific topics can be discussed with the relevant team(s).

Disclaimer

This document is not part of and/or subject to the agreement regulating the use of the services or any purchase. The information in this document is not a commitment, promise, or legal obligation to deliver any material or service or to develop and provide any specific security feature or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Bühler assumes no responsibility for errors or omissions in this document, except if such damages were caused by Bühler intentionally or grossly negligent.

Bühler Group

Gupfenstrasse 5
9240 Uzwil
Switzerland

www.buhlergroup.com

Version: 3.0, July 2025