Information Security Management System.

Information Security at Bühler.

V1.0, March 2020

Innovations for a **better world.**

BÜHLER

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.

Information Security Management System

Bühler operates an Information Security Management System (ISMS) which is certified according to ISO/IEC 27001:2013 (herein referred to as “ISO standard”). The certification scope covers the design, development and operations processes of the internal IT services, myBühler, Bühler Insights and Mercury. 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 CEO regularly releases a set of information security policies, which are valid and mandatory for every employee 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, etc.

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 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 in general.

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 114 controls in 14 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 Information security policies
Bühler has a defined set of information security policies and requirements, which are regularly reviewed and adjusted as required.

A.6 Organization of information security
A dedicated team with defined responsibilities and duties is handling information security. The team has regular exchanges with peers in other companies or authorities to stay up to date about current threats.

A.7 Human resource security
Human resources processes for on- and offboarding are defined including necessary screening activities and contractual requirements which define the responsibilities regarding information security and protecting valuable information which includes data of or about our customers.

A.8 Asset management
Information assets are defined and used for the information security risk management process. IT assets are managed in a global asset management database and follow defined processes for creation and disposal including secure erasure of data. Handling requirements for different information classification levels are defined.

A.9 Access control
Access to sensitive information such as data of or from our customers, follow defined access management requirements. For example, processes for granting and approving access permissions.

Global password requirements 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.10 Cryptography
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 VPN connections between all locations. For web applications reachable over public networks "https" or equivalent secure protocols are required by our policies.

A.11 Physical and environmental security
Physical perimeter protection ensures that only authorized individuals can enter Bühler premises or sensitive areas such as data centers.

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 27001:2013 and SOC II.

On-premise datacenters follow defined policies and are

secured by physical access controls and specific equipment such as cooling systems, fire extinguishers, UPS, etc.

A.12 Operations security
A defined change management process ensures that all modifications to critical assets are properly documented and approved.

All computers and servers are protected by an antivirus solution which is operated by a dedicated team.

Information security relevant logs are centrally collected, and potential security incidents are analyzed and acted on by the information security team.

A.13 Communications security
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 controlled and assets are located in segregated network zones.

A.14 System acquisition, development and maintenance
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.

A.15 Supplier relationships
A global procurement organization ensures harmonized purchasing of services and suppliers of goods. Information security relevant suppliers (for example cloud service providers or external consultants) are evaluated including information security and need to sign a document called “Minimum technical and organizational information security requirements for suppliers” which binds suppliers to apply similar levels of information security controls as Bühler does.

A.16 Information security incident management
All employees are asked to immediately report (potential) information security incidents so the necessary preventive or corrective measures can be taken. A systematic approach is used to ensure that lessons learned are carried out and similar issues are not happening again.

A.17 Information security aspects of business continuity management
Business critical IT services are designed with availability architecture in mind. If disasters occur, IT follows defined processes for “IT Service Continuity”. Regular tests are carried out to ensure these processes are working as designed.

A.18 Compliance
Relevant laws and regulations with potential impact to the ISMS and information security in general, are identified and monitored to be able to react on changes.

Bühler has a worldwide data protection organization and applies GDPR principles globally or, if more strict, local regulatory requirements regarding data privacy.

Bühler regularly reviews its information security by reviews performed internally or together with external partners by conducting penetration tests or similar security testing.

Compliance with information security policies is regularly reviewed and monitored and violations follow defined sanctioning processes.

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.

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.

myBühler
The myBühler customer portal is the digital contact gate for our customers and therefore your entry point to the digital solution portfolio of Bühler. Available in more than 120 countries worldwide and 8 languages, more than 6,000 customers enjoy access to information about installed machines, parts, orders and important documentation like spare parts catalogs and user manuals. myBühler enables easy ordering of spare & wear parts and can be integrated into existing purchasing systems for smooth purchasing processes. The software development and operations activities follow the 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 AG

Gupfenstrasse 5
CH-9240 Uzwil
Switzerland

www.buhlergroup.com

Version: 1.0, March 2020