Cyber Security Governance.

Information Security Governance for Bühler Digital Services.

Innovations for a **better world.**

BÜHLER

Content.

Cyber Security Governance

1. Scope and Purpose of this document

Information, data and its supporting processes, systems and networks are vital to the business and of Bühler and its customers. The security of this information is even more important. This document describes the technical and organizational security measures implemented by Bühler to create, operate and provide Digital Business Services to its customers. The general purpose is to understand how Bühler addresses current and future cyber security threats as well how Bühler will ensure availability, integrity and confidentiality of all information processed for customers. Bühler fully understands the importance of cyber security to the customers and is in a continuous process to apply and improve the high level of security standards. Bühler's Digital Officer and security group regularly review and ensure that best practice is applied to Bühler Digital Services.

This document will be updated on regular basis. Please do not hesitate to approach your Bühler contact to request more detailed information.

2. Security Exposure and Importance

The customer on-premise plant network interconnects all critical production process assets such as machines, PLCs and operator computer stations. The classical deployment usually requires this to be intentionally disconnected from corporate or even public networks. However, to use Bühler Digital Services these networks require a secure external connectivity. The planning, implementation and maintenance of the used devices is crucial to security.

The interconnection of components is realized using a variety of industry standards, including, for example, sensor-to-machine, machine-to-machine, or machine-to-cloud networks. Communication from the customer on-premise plant network can be by public or private IP networks to Bühler Digital Services Platforms built using best in class services. For secure external communication a secure gateway system may be installed at the customers site. This gateway is part of the platform and the main secure endpoint of the communication applying access control, data encryption as well as access logging. It is vital to the quality and security of the service, that all stages must ensure availability, integrity and confidentiality of the data transmitted and stored.

Potential risks include malware connectivity from plant network to internet, attacks from corporate network to plant network, malfunction of corporate network impacting plant network, eavesdropping of data transmitted, tampering of plant control hardware or software, etc.

Potential mitigations of risk on the customer site are implementation of endpoint security software such as antivirus on computers and servers, well defined firewall rules allowing only required protocols from/to defined endpoints, use of encrypted traffic protocols, continuous update of all used operating systems and software components to avoid vulnerabilities to be exploited, restrict physical access to the equipment, etc.

The responsibility of operation of the customer networks is assigned to the customer and Bühler engineers are trained to advise or support for a secure setup. Any additionally required hardware or software is installed and documented by skilled personnel to ensure a qualified setup.

Bühler develops and builds high level technology products and services as it also provides enhanced retrofit kits to bring legacy equipment to the newest level of functionality and efficiency. Modern products often rely on advanced information technology (IT) components for processing data and connecting its components. As such IT components are exposed to security threats as regular professional IT equipment is. However as such threats are inherited, also the counter measures from professional IT are adopted.

Bühler fully understands the importance of cyber security and applies state of the art IT security standards and expertise into the modern products developed and systems built. These mechanisms enable the design and development of cyber security solutions that are specifically for industrial automation and control systems, and which utilize proven technology. Customers can rely on system solutions where reliability and security have the highest priority.

Cyber security was identified as a key requirement and Bühler is committed to provide customers with products, systems and services that clearly address this issue. Besides continuously adapting security requirements to keep up with changing demands, the internal security organization develops guidelines to proactively support R&D embracing future trends as well as fast and efficient security improvements. This means that cyber security is addressed at each step of our product life cycle, from design and development to maintenance.

Furthermore all internal knowledge-worker staff is trained by continuous information security awareness campaigns.

3. Security Components and Approaches

Bühler has developed and will continue to develop Digital Services which allow and will continue to allow existing and future equipment to be interconnected enabling new business and service models to maximize benefits and value. The aim is to provide safe and secure services to the customer and also focus on information security as a cornerstone of the solution as well as an integral discipline of our organization.

The objective of information security management is to implement technical and organizational measures that reduce to an acceptable degree the risks involved with processing and dissemination of information by ensuring the necessary level of confidentiality, integrity, availability and accountability as defined below.

Confidentiality: To ensure that information is made available or accessible only to authorized persons, groups of persons, entities or system processes according to their classification.

Integrity: To ensure that the content of information is consistent, that no changes can be made without proper authorization, and that data cannot be lost unnoticed.

Accountability: To ensure that any entity involved in the creation, validation, manipulation or deletion of information can be conclusively identified. Data on every level has an ownership.

Availability: To ensure that information, information systems or information resources are accessible and usable by authorized entities as needed.

In order to accomplish the above mentioned principles

Bühler has implemented the following technical and organi zational security measures and all our partners helping us to provide Digital Services to our customers have to provide sufficient guarantees that they implement and maintain these measures accordingly.

3.1 Transparency and control

All activities on the Bühler Digital Services are logged to ensure 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.

3.2 Encrypted communications

The main communication between customer installation and the Bühler Digital Services is performed directly or by gateways as intermediary system. 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.

3.3 System wide security

Bühler provides products and solutions with security functions that support the secure operation of plants, systems, machines and networks.

4. Security measures on customer's side

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial 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 to apply product updates as soon as available and to always use the latest product versions. This does not apply to DS Services and/or the underlying systems and components, including Embedded Software, which are updated by Bühler. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

General 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

CH-9240 Uzwil
Switzerland

Version: 1.0, May 1, 2017