Information Security

Minimum Technical and Organisational Requirements for Suppliers.

Innovations for a **better world.**

BÜHLER

Minimum Technical and Organisational Information Security Requirements for Suppliers.

Scope.

As a global technology provider, Bühler is committed to information security in order to provide reliable and sustainable digital solutions and to protect its own as well as the information of customers and business partners. This objective can only be achieved if all stakeholders within the value chain submit itself to comparable high information security standards. Bühler therefore expects all Suppliers to abide by the requirements set forth in this document.

Terms.

Bühler Information is all information transferred from Bühler to the Supplier or of which the Supplier has been made aware of by Bühler.

Sensitive Bühler Information is all Bühler Information which is considered as not been publicly known and where Bühler has extended interests of protection against loss of confidentiality, integrity, and availability. Such information includes for example, but not limited to, internal procedures, business strategies, intellectual property, financial information, Personal Data, etc.

Personal Data is any information that relates to an identified or identifiable individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute Personal Data.

Supplier describes all suppliers, service providers or other business partners of Bühler, including their parent and subsidiary entities, as well as sub-tier suppliers and contract agencies if Supplier:

- is processing Sensitive Bühler Information in the context of the fulfilment of the agreement with Bühler;
- is providing services to Bühler which have a high impact on the confidentiality, integrity or availability of Bühler's Information.

TOMs

Supplier implements, operates and regularly updates adequate technical and organisational measures (TOMs) to protect the confidentiality, integrity, and availability of Bühler Information by following state of the art best practices ("TOM"). While adhering to its TOM the Supplier commits to adhere at any time at least to the minimum requirements as listed below:

Information Security Governance.
Supplier defines and implements information security policies following best practices and industry standards.

Supplier has effectively enrolled a responsible person for information security (e.g. CISO).

Supplier provides a contact person or contact possibility for questions or issues with regards to information security.

Bühler Information Security.
Bühler operates an Information Security Management System including relevant information security policies. If Supplier's personnel is accessing or using Bühler information systems, Supplier's personnel is aware of and complies at any time to the requirements of the Bühler Information Security Management System (ISMS).

Human Resources.
Supplier ensures that it has, prior to the appointment to perform and/or access Sensitive Bühler Information or perform critical activities (system administrators, etc.), run adequate background checks for all of its respective personnel.

Supplier has contractually obligated all of its employees, subcontractors or other third parties to adequately ensure the confidentiality of Bühler Information even after the termination of the employment or business relationship.

Training and Awareness.
Supplier ensures that all of its personnel, contractors and third parties under its control having access to Bühler Information have received adequate information security training.

Access Control.
Supplier ensures that only authorized personnel can access Bühler Information and in particular, but not limited to, Personal Data, based on a need-to-know principle.

Supplier regularly reviews access rights to ensure that the allocation is adjusted if necessary.

Supplier ensures that access to critical systems and Sensitive Bühler Information is additionally protected such as by using strong authentication methods (e.g. multi-factor), extensive logging/monitoring of activities, etc.

Cryptography.
Supplier ensures that Sensitive Bühler Information is adequately protected by cryptographic controls for data at rest and in transit as for example with full disk encryption, transport encryption for data passing public networks, etc. Special care needs to be applied for portable media such as USB drives containing Bühler Information.

Supplier is using established and known best practices for cryptographic technology.

Physical Security.
Supplier protects information or information systems processing or storing Bühler Information against unauthorized physical access, damage or theft by using adequate perimeter and entry controls.

Change Management.
Supplier operates a process to prevent and record unauthorized changes to information systems affecting the confidentiality, integrity and availability of Bühler Information.

Malware Protection.
Supplier operates adequate and state of the art measures against malware such as viruses and trojans to prevent infection of data being transferred to Bühler and/or unauthorized modification of Bühler Information stored at Supplier's information systems.

Supplier ensures that these malware protection measures are frequently updated.

Protection of Information.
Supplier established processes and rules for handling and storing information to prevent unauthorized disclosure or misuse of Bühler Information.

Supplier disposes Bühler Information securely by following industry standards.

Supplier agrees that upon Bühler's request or termination of the business relationship between Bühler and the Supplier, Supplier will within due time dispose (e.g. erase, destroy or render unreadable) any and all Bühler Information that are in possession of Supplier, its affiliates or subcontractors and provide Bühler with detailed report within due time confirming the deletion. No deletion is necessary if:

- Supplier must keep the information for legal or regulatory purposes; such information are to be deleted as soon as the legal retention periods have expired;
- Bühler has requested the Supplier in writing to keep Bühler Information archived for legal hold purposes
- Supplier will use anonymization and/or pseudonymization techniques whenever possible. The key for de-pseudonymization is kept secure and secret.
- Supplier takes adequate measures when transporting information systems, storage media, etc. containing Bühler Information, especially but not limited to, if portable storage such as USB drives are used.

Monitoring.
Supplier actively monitors its information systems and networks for any potential unauthorized or harmful access and/or other activity. Supplier further undertakes to immediately inform Bühler in case of an unauthorized access or other breach of its information systems and/or networks.

Supplier protects logging and monitoring results adequately against unauthorized access or modification.

Vulnerability Management.
Supplier regularly applies updates and patches to its information systems processing Bühler Information to ensure the continuous adherence of the Minimum Technical and Organisational Information Security Requirements for Suppliers set forth herein.

Network Security.
Supplier ensures that its networks are adequately protected against threats by implementing and maintain (web application) firewalls, intrusion detection systems, network segregation, as well as other network security measures necessary.

Supplier ensures that remote access to its networks are safeguarded by secure transmission technology (e.g. VPN) using encrypted channels.

System and Software Development.
Supplier follows a defined process for secure software development.

Supplier performs secure coding practices such as static code analysis, code audits or similar.

Supplier's development activities are in accordance with industry best practices (e.g. OWASP).

Supplier performs regular independent information security reviews (e.g. pen tests) and agrees to share results of such reviews in detail or as summary to Bühler.

Third Parties.
Supplier ensures that its subcontractors and other third parties adhere to Suppliers' policies and information security requirements while adhering at any time at least to the Minimum Technical and Organisational Information Security Requirements for Suppliers set forth in this document.

Security Testing.
You acknowledge and agree that Bühler is under the obligation to continuously check and improve its cyber security standards. Therefore, Bühler needs to perform security testing (including but not limited to ethical hacking by third parties in the context of a bug bounty program) to ensure the security of its systems and services are compliant with the state-of-the-art standards from time to time ("Security Testing"). Security Testing can include automated scanning for vulnerabilities, outdated components, or security misconfigurations and will be performed on all domains owned by or related to Bühler. As a supplier of IT systems or infrastructure to Bühler, your scope might also be targeted within any Security Testing. Security Testing is performed in an automated and random way so a prior notification regarding upcoming activities is not feasible. Nevertheless, should we specifically request a Security Testing including any of your systems we will, as far as reasonable, try to inform you in advance. You confirm that you have been informed and agree that Security Testing performed by Bühler and/or any third party on behalf of Bühler might involve the IT systems and/or infrastructure provided by you. Should you face any issues or have further questions regarding the Security Testing, please contact **security@buhlergroup.com**

Information Security Incident Management.
Supplier is capable to adequately react and take appropriate measures in case of an information security incident.
Supplier agrees to report information security incidents affecting Bühler Information within 48h to Bühler. Information security incidents shall be reported to **security@buhlergroup.com**

Business Continuity.
Supplier performs backups to preserve availability of Bühler Information and protects backups and backup facilities with similar measures as the source systems.
Supplier operates adequate business continuity plans to ensure that the Minimum Technical and Organizational Information Security Requirements for Suppliers set forth in this document are adhered at any time even during adverse situations. Supplier regularly tests its recovery plans.

Legal and Regulatory Requirements.
Supplier complies at any time with the legal and regulatory requirements applicable for the Bühler Information. Further the Supplier ensures that it's processing of Personal Data always complies with any applicable data protection laws, regulations and agreements in this regard concluded with Bühler. Suppliers processing Personal Data agree to adhere at any time to the principles set forth in the General Data Protection Regulati-on (EU) 2016/679 ("**GDPR**") and to duly support Bühler in its fulfilment of the obligations and requirements under the GDPR including but not limited in case of a request by a data subject. Suppliers processing Personal Data of Bühler as processor will adhere to the terms and conditions as agreed in the respective Data Processing Agreement concluded with Bühler.

Deletion of Information.
The supplier undertakes to delete as far as legally permissible any Intellectual Property rights (IP), personal data, project data and/or other information received and/or otherwise disclosed by Bühler whether in writing, orally or by perception ("Bühler Data") within 90 (ninety) days after the respective project is completed. If Bühler so requests supplier will confirm in writing that any Bühler Data has been completely deleted.

Right for Information.
Supplier agrees that Bühler may request further information to check Supplier's compliance with the Minimum Technical and Organizational Information Security Requirements for Suppliers set forth in this document: Supplier undertakes to timely deliver the requested information at no additional costs for Bühler.

Acknowledgement.

We, the undersigned, duly authorized to bindingly sign for the below mentioned company, hereby confirm that we understand and accept the content of this Minimum Technical and Organisational Information Security Requirements for Suppliers, and are committed to fully complying with it.

Name of company _____

Name and title _____ **Signature** _____

Company stamp/seal _____

Company business registration/statutory ID/cod/number _____

Information security contact name and e-mail _____

Date and place _____

Version: July 2023

Bühler Group

Gupfenstrasse 5
9240 Uzwil
Switzerland

www.buhlergroup.com