Information security policy for suppliers and Contractor of the Schmalz Group

§ 1 Information security

1. The Contractor shall take appropriate state-of-the-art organizational and technical measures to ensure the confidentiality, authenticity, integrity and availability of the Supplier's operations as well as its deliveries and services. These measures shall be customary in the industry and shall include an appropriate information security management system in accordance with standards such as ISO/IEC 27001 or IEC 62443 (as applicable).
   "Supplier's Operations" means all goods, processes and systems (including information systems), data (including Customer Data), personnel and locations temporarily used or processed for the performance of this Agreement.
   The Contractor shall grant the Client access to its facilities after reasonable notification in order to satisfy itself that suitable technical and organizational measures have been implemented.

2. On the entire company premises as well as in all premises of the client, it is prohibited to make picture and sound recordings of any kind without prior written consent.

3. If deliveries or services include software, firmware or chipsets:

   Supplier shall implement appropriate, industry-standard standards, processes and methodologies in accordance with standards such as ISO/IEC 27001 or IEC 62443 (as applicable) to prevent, identify, assess and remediate any vulnerabilities, malicious code and security-related events in the Supplies and Services;
   the Supplier shall offer repair, update, upgrade and other maintenance services and provide patches to eliminate vulnerabilities for a reasonable period of the life of the Supplies and Services;
   the supplier shall provide a parts list showing all third-party software components used in the supplies and services. Third party software components must be up to date at the time of delivery;
   the Customer shall be entitled, but not obliged, to test the Supplies and Services for malicious code and vulnerabilities at any time, either itself or through third parties, in which case the Supplier shall provide the Customer with reasonable support.

4. The Contractor shall designate a contact for information security issues (reachable during business hours) to the Client.

5. The Supplier shall take appropriate measures to impose on its employees, subcontractors and suppliers, within a reasonable period of time, obligations that comply with the obligations of general data protection under GdPDU, as well as this Policy.

§ 2 Secrecy

1. The Contractor undertakes to keep confidential or strictly confidential information strictly secret and to use it exclusively for the purpose of processing the order. This shall also apply after the end of the contract and the departure of employees, vicarious agents or subcontractors.
   Confidential Information may include, but is not limited to, the following information and/or items (individually or in the aggregate):
   technical information, in particular product, development or functional descriptions, requirement or specifications specifications, sketches, graphics, drawings and other technical documents as well as manuals, technical procedures and processes and other know-how, in particular technical knowledge,
   Information on existing or future legal positions, in particular rights of use and license, license rates, applications for patents and patentable inventions, utility models, design patents or trademark rights, and all other rights,

Information on corporate strategies, schedules, goals, ideas, planned projects, sales channels, and commercial data, especially sales and margins,
Information obtained by the Contractor in the course of service or repair work on a machine or component supplied by the Client concerning its design and mode of operation.
IT know-how such as equipment, processes, programs and licenses, developments, data exchange, security facilities and security measures.
All Confidential Information provided by Customer to Contractor shall remain the sole property of Customer.

§ 3 Reporting obligations

1. Information security incidents must be reported immediately to the project contact and to the e-mail address Informationssicherheit@schmalz.de. The loss event, immediate measures, causes and long-term measures are reported. The contact person will then initiate the information security incident handling process without unwarranted delay. Possible events can be, for example:
   - ineffective security measures,
   - Suspicion of data loss, - theft
   - Breaches of the expected confidentiality
   - Malfunctions of software that affect information security

   The Contractor shall grant the Client access to its facilities in order to convince itself of the implementation of suitable technical and organizational measures for the prevention of such events, as well as for damage limitation in the event of such an event occurring.

§ 4 Data protection

1. Each party is obliged to observe the statutory provisions on data protection, in particular the EU General Data Protection Regulation (GDPR), when executing the agreement and to impose compliance with these provisions on its employees.

2. Each party shall process any personal data of the other party received (e.g. names and contact details of the respective contact persons) exclusively for the performance of this Agreement and shall protect such data by technical security measures (Art. 32 DSGVO) adapted to the current state of the art. Each party is obliged to delete the personal data of the other party as soon as their processing is no longer necessary. Any statutory retention obligations remain unaffected by this.

3. Should one party process personal data on behalf of the other party within the scope of the execution of the contract, the parties shall conclude an agreement on commissioned processing in accordance with Art. 28 DSGVO. Additional processing for own purposes, also in anonymized form, is excluded.

Attachment 1
Information Security Event / Incident Reporting Form

1. General information about the incident

Vendor Name: Name/contact information of the submitter:
Subject of the incident :
Date: Time:
Time of the incident, period affected:
Data processing methods:
Department responsible:
Person responsible for the incident:

Description incident

Affected systems/objects
How did the incident occur?
What consequences have been identified?

Reactions and state of the system

Causes of the incident
Responses/measures to the incident (quick fix and long term measure to prevent reoccurrence).
Current state of the system

2. Incident details

2.1 Nature of Incident:
(Incidents include loss of confidentiality, data theft, destruction or corruption of data, transmission to unauthorized parties, etc.).
2.2 Categories of information / personal data:
2.3 Likely consequences/risks of the breach of the protection of the information *(Here, the possible risks and consequences for the data subjects must be indicated).*

3. Remedial actions initiated

3.1 Measures initiated (Describe the measures that have been initiated here).

3.2 Other intended measures
(Describe here any additional measures planned to be put in place as a result of the incident).