Information Security Terms and Conditions

The following provisions regarding information security define the standards and criteria that Suppliers must meet to ensure the common goal of information security to protect the information of MFBM and/or Supplier.

I. Secure handling of information and protection of systems

To ensure the confidentiality, integrity, and availability of the shared information of MFBM, the contracting parties undertake to effectively protect all such shared information against unauthorized access, modification, destruction or loss, unauthorized transmission, other unauthorized processing, and other misuse in accordance with the current state of the art.

The Supplier shall take reasonable precautions to prevent its systems and its assets from creating security threats that would affect MFBM's infrastructure, in particular, ensuring that relevant systems and computer devices of the Supplier are free of malware (e.g., ransomware).

II. Management of incidents

1. Incident notification

The Supplier is obliged to notify MFBM immediately of all incidents affecting him that jeopardize the confidentiality, integrity, or availability of MFBM information in his possession, insofar as it concerns MFBM information and/or could negatively affect MFBM. This includes cases such as data loss, data misuse, infections with malware, in particular unauthorized access to MFBM information (e.g., cyber-attack), or if circumstances exist that indicate such an incident. Any such incident must be reported to MFBM Cybersecurity team by email (MFBM-cybersecurity@archion-group.com), and respective procurement points of contact.
.

2. Contact persons

The Supplier shall appoint responsible contact persons for information security, who are responsible for reporting security incidents and violations to the MFBM, as well as monitoring the response and remedial measures.

3. Incident remedial action

The Supplier shall ensure that such incidents, information security breaches and critical vulnerabilities are resolved without undue delay. The Supplier commits all necessary measures to mitigate the damage and to support MFBM in restoring information. At MFBM request the Supplier submits a detailed incident report and must include the results of security tests, identified information security risks and information security incidents, and actions taken or to be taken accordingly.

III. Staff awareness

The Supplier shall instruct its employees and contractors, who will have access to MFBM's information about the security requirements and the specific procedures such as

incident management regarding this access, including the acceptable use of MFBM information.

IV. Information security certification

Depending on the type and protection requirements of MFBM's information concerned or the importance of the Supplier's services for the business operations of MFBM, MFBM may require the Supplier to take an appropriate level of security measures for information security throughout business relationship. Upon request, the Partner shall provide information on secured cybersecurity certification levels at the Partner's premises, including but not limited to external certificates such as TISAX® label with Assessment Level 3, ISO27001, SOC2 or other equivalent certification for production material suppliers. MFBM may request the same certification from all other suppliers within the respective procurement contract. The parties may agree a reasonable period for the initial testing of a site in accordance with the respective certificate and or any changed requirements of the appropriate level of information security.

V. Right to inspect

MFBM reserves the right to assess and audit the supplier's cyber security practices, including but not limited to certification validity and implementation effectiveness, with prior notice and mutual agreement, to ensure alignment with MFBM security requirements.
If MFBM becomes aware of a breach of the agreed implementation and maintenance of information security requirements, the existence of an information security incident or if there are reasonable grounds to suspect such a breach, MFBM shall have the right to verify compliance with the information security requirements and the agreed additional information security requirements ("Audits"). The Supplier will cooperate to provide necessary information, to the extent required for the Audit. MFBM may, after timely notification during normal business hours and, to the extent possible and reasonable, also inspect the Contractor's premises, including the relevant IT systems, to verify compliance with the agreed technical and organizational measures without disrupting operational processes. In doing so, MFBM shall observe any confidentiality obligations of the Supplier towards third parties. MFBM shall be entitled to have the Audits carried out by an external, qualified company that is bound to confidentiality vis-à-vis third parties, provided that this company is not a competitor of the Supplier. This shall neither restrict nor exclude MFBM's statutory rights of inspection and information.