Special Purchase Conditions

Annex - Information Security

These Special Conditions of Purchase are an integral part of the General Conditions of Conditions of Purchase ("GCC") governing the supply of Goods and/or between Mercedes-Benz do Brasil Ltda. ("MBBRAS") and the Supplier to whom the contract is addressed, relating to the security of the information security, defining the standards and criteria that Suppliers must comply with to ensure the common objective of security of information of MBBRAS and/or the Supplier.

Section I – Information security

1. Secure handling of information and systems protection

To guarantee the confidentiality, integrity and availability of the information shared by MBBRAS, the contracting parties undertake to protect all 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 preventive measures to prevent its systems and assets from creating security threats that could affect MBBRAS' infrastructure, in particular by ensuring that the Supplier's relevant computer systems and devices are free from malware (e.g. ransomware).

2. Incident management

2.1. Notification of incidents

If MBBRAS or the Supplier becomes aware of incidents involving a breach of information security and/or which jeopardize the confidentiality, integrity or availability of MBBRAS information in its possession, insofar as it concerns MBBRAS information and/or may adversely affect MBBRAS, or if there are indications for MBBRAS or the Supplier that justify the suspicion of such information security incidents, taking into account a reasonable assessment, the Supplier shall, without any undue delay, notify MBBRAS. This includes cases such as loss of data, misuse of data, malware infections, unauthorized access to MBBRAS information (e.g. cyber attack), vulnerabilities, other security threats or if there are any other circumstances that may affect MBBRAS.

2.2. Responsible person

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

2.3. Corrective measures for incidents

The Supplier shall ensure that such incidents, information security breaches and critical vulnerabilities are resolved without undue delay and without additional charge. Immediately after becoming aware of the security incident, the Supplier undertakes to provide all the necessary support to MBBRAS, including mitigation measures and their implementation, complying with the deadlines indicated in this Annex to mitigate the damage and support MBBRAS in restoring the information. At the request of MBBRAS, the Supplier shall submit a detailed incident report and shall include the results of the security tests, information security risks identified and information security incidents identified, and measures adopted or to be adopted.

The Supplier undertakes to maintain a contingency plan for the contracted services, which must contain detailed plans for business continuity and business recovery in the event of a Security Incident.

3. Staff awareness

If the Supplier has access to MBBRAS data processing tools or those used by MBBRAS, any access granted to unauthorized persons will only be allowed with the prior approval of MBBRAS, for use within the scope necessary for the execution of the contract. The Supplier must also keep its employees, subcontractors and other persons involved in the provision of the services, with access or privileges of access to such tools, informed of the information security guidelines and specific procedures, such as incident management in relation to such access, including the limitations on the use of MBBRAS information.

4. Information security certification

Depending on the type and protection requirements of the MBBRAS information in question or the importance of the Supplier's services for MBBRAS' business operations, MBBRAS may require the Supplier to adopt an appropriate level of security measures for information security throughout the business relationship. The Supplier shall provide evidence of an appropriate level of information security at the Supplier's premises, in particular by presenting the TISAX® seal with Assessment Level 3 for suppliers of production material. MBBRAS may request the same seal from all other suppliers within the respective contract. The parties may agree on a reasonable period for the initial testing of a site in accordance with the respective certificate and/or any changes in requirements at the appropriate level of information security.

5. Right of inspection

If MBBRAS becomes aware of a breach of the implementation and maintenance of the agreed information security requirements, of the existence of an information security incident or if there are reasonable grounds to suspect such a breach, MBBRAS shall have the right to verify compliance with the agreed information security requirements and additional information security requirements (“Audits”). The Supplier shall cooperate to provide the necessary information to the extent required for the Audit. MBBRAS may, upon timely notification, during normal business hours and to the extent possible and reasonable, also inspect the Supplier's premises, including the relevant IT systems, to verify compliance with the agreed technical and organizational measures without interrupting operational processes. In doing so, MBBRAS shall observe any confidentiality obligations of the Supplier towards third parties. MBBRAS shall be entitled to have the audits carried out by an external and qualified company that is bound by confidentiality towards third parties, provided that this company is not a competitor of the Supplier. This shall not restrict or exclude MBBRAS' right of inspection and information.

Section II - Provision of Automation Services, Acquisition and Modification of Machinery and Equipment

6. Specific Application

Without prejudice to the above provisions, which apply to all contracts, in the specific cases of the provision of automation services, the acquisition and modification of machinery and equipment, the provisions of this Chapter II shall also apply.

7. Training

Every year, MBBRAS shall provide training to the Supplier on the information security directives applicable to the Contract, and the Supplier must formally declare, by signing a specific document, that it is aware of the content taught and that it is fully complied with. In the event of the Supplier's refusal to take part in the training or to comply with MBBRAS's rules on information security, the services or contract will be suspended, as well as the respective payment. Unjustified non-compliance with the directives provided by MBBRAS may result in the justified and early termination of the contract of services provision.

8. Vulnerability Correction

8.1. The Supplier is responsible for correcting any cyber security vulnerabilities identified in the equipment supplied to MBBRAS. If equipment is purchased from a third-party company, the Supplier will be responsible for the billing process and compliance with the SLA by the third-party company.

8.1.1. Correction of vulnerabilities must be carried out in accordance with industry best practices and with the utmost urgency in order to mitigate any risk to MBBRAS' security.

8.1.2. In the event of the need to correct a vulnerability, the Supplier shall:
(i) Provide MBBRAS with a detailed description of the remediation method for each identified vulnerability, which shall contain step-by-step instructions for implementing the remediation and any additional tools required;
(ii) Release a fix for the vulnerability within a timeframe according to the vulnerability's risk rating: if critical, one (1) month; if high, two (2) months; and if low, three (3) months, counting from the date the vulnerability was identified. The risk analysis will be carried out by MBBRAS using a specific tool for identifying cyber security vulnerabilities.

8.1.3. In the event of non-compliance with the deadline established in item (ii) of Clause 8.1.2. or failure to correct the vulnerability, during the period in which MBBRAS's information and systems are exposed to the risk arising from the vulnerability, the Supplier shall be responsible for assisting MBBRAS in the recovery of the affected environment and for any damage caused to MBBRAS, including but not limited to those arising from cyber attacks on the contracted systems or equipment, with MBBRAS having the right to adopt appropriate measures to protect its infrastructure.