Information Security Requirements for Third Party Access

The Supplier hereby enters into obligation to comply with the following requirements:

1. **Scope**
   These requirements apply to all affiliated companies of the Mercedes-Benz Group China Ltd.(hereinafter referred to as "Mercedes-Benz") external partners, suppliers, contractors and all other individuals or companies such as consultants or maintenance and support staff who require access to Mercedes-Benz company information (“Third Party” or “Third Parties”)as part of their contractual agreement with Mercedes-Benz Group China Ltd. or its affiliated Company.

2. Requirements

2.1 General Requirements

2.1.1. All Third Parties that require access to Mercedes-Benz information must comply with Mercedes-Benz information security requirements.

2.1.2. Contractor and other Third Party access must be limited to the information resources required to fulfill their contractual requirements with Mercedes-Benz.

2.1.3. The Third Party organization must restrict access to Mercedes-Benz information to only those employees which require access in order to fulfill the Third Party contractual obligations.

2.1.4. Third Parties are not permitted to provide other organizations, such as subcontractors or partners, with access to Mercedes-Benz information without prior written approval from Mercedes-Benz.

2.1.5. After the fulfilment of the contractual obligations by the Third Party or, where applicable, the termination of contractual relationship, Third Party is obliged to return or destroy all documents or stored data, including copies, received from Mercedes-Benz. The complete return or destruction of all information must be confirmed in writing to Mercedes-Benz if requested by the latter. Third Party shall have no right to retain data, documents and other materials of Mercedes-Benz.

2.1.6. The Third Party shall inform Mercedes-Benz without delay in case of a suspected violation of any information security and data protection requirements which could affect Mercedes-Benz, and—in coordination with Mercedes-Benz immediately initiate all necessary.

2.1.7. Should personal data (of clients or employees of Mercedes-Benz or its affiliated companies) be processed or accessed by the Third Party within the scope of this Agreement, the Third Party shall sign Agreement on Data Processing on Behalf.

2.1.8. Mercedes-Benz is allowed to log and evaluate all activities of Third Party on its owned systems.

2.1.9. Third Party must report all information security incidents and issues affecting Mercedes-Benz to the responsible person. This also applies to information

security incidents and issues occurring within the area of responsibility of the Third Party and could negatively affect Mercedes-Benz.

2.1.10. Information security incidents and issues occurring within the area of responsibility of the Third Party must be handled by the Third Party in a way to minimize the risk to Mercedes-Benz.

2.1.11. All Third Parties are obligate to participate in regular information security audits to confirm information security compliance as requested by Mercedes-Benz.

2.2 Third Party Information Use and Responsibilities

2.2.1. Third Parties must use Mercedes-Benz information resources responsibly and only for the expressed purpose of meeting the contractual requirements with Mercedes-Benz. Third Parties are prohibited from using or sharing Mercedes-Benz information for other purposes than those stipulated in the Third Party contract.

2.2.2. Third Parties must adhere to specific security requirements for staff in sensitive areas, which may require security screening for individual employees.

2.2.3. Third Party organizations must inform all their employees and contractors, who will access Mercedes-Benz information, of the security responsibilities associated with such access.

2.2.4. Third Parties must keep VPN account properly and disable it once the contractual business activates ended.

2.3 Third Party Equipment Use

2.3.1. Third Parties must adhere to contractual restrictions regarding the processing of corporate information on non- Mercedes-Benz equipment as determined by the contact person defined in the contract or the third-party contact.

2.3.2. Third Parties must get permission from local IT Networking and the Supplier Champion to connect non-Mercedes-Benz equipment to Mercedes-Benz networks. Permission must be based on adherence this document as well as local network access policies that detail the acceptable use of Third Party's equipment.

2.3.3. Malware protection measures should be in place on non-Mercedes-Benz equipment used by Third Parties.

2.3.4. Third Parties should take reasonable precautions (such as the timely application of critical software security patches) to ensure that their non-Mercedes-Benz equipment does not introduce security weaknesses that affect the Mercedes-Benz infrastructure.

2.3.5 Third Parties shall notify the third party contact once there is service team change and initiate the request of any access changes to Technical Owner or Information Owner whenever off boarding or transfer occurs.