

# 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 Daimler Truck external partners, suppliers, contractors and all other individuals or companies such as consultants or maintenance and support staff who require access to Daimler Truck company information (“Third Party” or “Third Parties”) as part of their contractual agreement with Daimler Truck.

## 2. **Requirements**

### 2.1 General Requirements

- 2.1.1. All Third Parties that require access to Daimler Truck information must comply with Daimler Truck 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 Daimler Truck.
- 2.1.3. The Third Party organization must restrict access to Daimler Truck 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 Daimler Truck information without prior written approval from Daimler Truck.
- 2.1.5. After the fulfilment of the contractual obligations by the Third Party or, where applicable, the termination of these requirements, Third Party is obliged to return or destroy all documents or stored data, including copies, received from DAIMLER TRUCK. The complete return or destruction of all information must be confirmed in writing to DAIMLER TRUCK if requested by the latter. Third Party shall have no right to retain data, documents and other materials of DAIMLER TRUCK.
- 2.1.6. The Third Party shall inform DAIMLER TRUCK without delay in case of a suspected violation of any information security and data protection requirements which could affect DAIMLER TRUCK, and—in coordination with DAIMLER TRUCK—immediately initiate all necessary
- 2.1.7. Should personal data (of clients or employees of DAIMLER TRUCK 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. DAIMLER TRUCK or its Affiliated Company is allowed to log and evaluate all activities on its systems.

- 2.1.9. Third Party must report all information security incidents and issues affecting Daimler Truck 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 Daimler Truck.
  - 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 Daimler Truck.
  - 2.1.11. All Third Parties are obligated to participate in regular information security audits to confirm information security compliance as requested by Daimler Truck.
- 2.2 Third Party Information Use and Responsibilities
- 2.2.1. Third Parties must use Daimler Truck information resources responsibly and only for the expressed purpose of meeting the contractual requirements with Daimler Truck. Third Parties are prohibited from using or sharing Daimler Truck 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 Daimler Truck information, of the security responsibilities associated with such access.
- 2.3 Third Party Equipment Use
- 2.3.1. Third Parties must adhere to contractual restrictions regarding the processing of corporate information on non-Daimler Truck equipment as determined by the Supplier Champion.
  - 2.3.2. Third Parties must get permission from local IT Networking and the Supplier Champion to connect non-Daimler Truck equipment to Daimler Truck networks. Permission must be based on adherence to 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-Daimler Truck 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-Daimler Truck equipment does not introduce security weaknesses that affect the Daimler Truck infrastructure.