Information Security Requirements for Software Development

The Supplier hereby enters into obligation to comply with the following requirements in this Information Security Requirements for Software Development (“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. General Security Requirements

2.1 As part of the service provided by the Supplier, the Supplier and its staff will obtain access to Mercedes-Benz information. The Supplier undertakes to comply with all information security and data protection policies and guidelines issued by Mercedes-Benz to protect this information.

2.2 If the Supplier involves subcontractors or freelancers it must first obtain prior written consent of Mercedes-Benz. The contractual arrangements between the Supplier and the subcontractor or freelancer must be set up in such a way that they correspond with these requirements. In particular, the Supplier must ensure that the Right of Audit by Mercedes-Benz can be carried out at the subcontractors or freelancers.

2.3 The Supplier must ensure that the subcontractors comply with the technical and organizational requirements in the same way as the Supplier itself. If subcontractors are replaced or added during the course of the contractual relationship, the Supplier must first obtain written consent of Mercedes-Benz.

2.4 The Supplier 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 actions to resolve the situation and prevent further data protection and information security violations.

2.5 The Supplier shall inform Mercedes-Benz without delay of any menace to data as a result of distrait, confiscation or any other governmental access, insolvency/settlement procedures, other events or measures of third parties. The Supplier shall inform without delay all persons responsible in this context that the power of disposition regarding the above mentioned data belongs to Mercedes-Benz.

2.6 The Supplier must appoint a security manager that acts as liaison to Mercedes-Benz security staff and serves as a first point of contact for investigating information security and/or data protection incidents. The appointed security manager must have sufficient authority and resources to investigate security incidents and remedy any arising information security issues.

2.7 The Supplier must support source code audits (i.e. by providing access to

developers and auxiliary documentation).

2.8 Information systems acquisition, development and maintenance are intended to ensure there is a process in place to manage changes to the outsourced production or development environment. The Supplier must have a change management process in place and obtain Mercedes-Benz approval for changes to the production environment including applications.

2.9 The Supplier is strictly prohibited from incorporating undocumented and unapproved system entry points, such as maintenance backdoors, into Mercedes-Benz systems.

2.10 The Supplier is strictly prohibited from willfully incorporating malicious code into systems under development.

2.11 Source code of the software developed under the outsource contract should be owned by Mercedes-Benz during and after development and provided to Mercedes-Benz before project closure. And also, the software will become intellectual property of Mercedes-Benz. Alternatively, there is a source code escrow agreement in place for the case that the Supplier will not be able to further develop or maintain the application.

3. Technical Protection Controls

3.1 To protect Mercedes-Benz information provided to the Supplier, the Supplier is obliged to keep its communication infrastructure protected, which includes but is not limited to anti-malware protection, timely patching, proper configuration, not using default passwords–and to verify that known security weaknesses are checked against and remediated without undue delay. If the Supplier cannot comply with this requirement, Mercedes-Benz has to be informed about this without undue delay.

3.2 The Supplier shall comply with the principles of proper data processing while fulfilling their contractual obligations. The principles include virus protection and backups, compliance with data protection regulations and all precautions and measures considered state of the art within the IT sector.

3.3 Data deployed by the Supplier must be checked for viruses in accordance with the common technical IT-standards. If a virus is detected, the Supplier may not deploy this data. If the Supplier detects a virus on a data medium of Mercedes-Benz, the Supplier shall inform Mercedes-Benz promptly and is entitled to suspend performance until the virus has been removed.

3.4 Information security weaknesses, that are publicly known or become known to the Supplier, or are communicated to the Supplier by Mercedes-Benz, have to be remediated without undue delay, as far as there is no agreement with Mercedes-Benz about a diverging time schedule.

4. Confidentiality

4.1 In addition to the Confidential Information described in Article 14 of the general Terms and Conditions, Confidential Information in data processing includes without limitation

4.1.1 All technical data concerning or relating to Mercedes-Benz or its affiliated companies,

4.1.2 Trade secrets, know-how, formulas, techniques for software development, compositions of matter, inventions, techniques, processes, programs, diagrams, schematics, technical information, customer and financial

information, sales and marketing plans, and

4.1.3 The terms of this Requirements and any negotiations relating thereto.

4.2 Notwithstanding the foregoing, the following shall not constitute Confidential Information:

4.2.1 Information which is disclosed in patents or otherwise generally known to the public or in the trade or becomes generally known without breach of this Requirements by the Supplier;

4.2.2 Information of Mercedes-Benz which is shown by written record to have been known by Supplier prior to its disclosure hereunder; and

4.2.3 Information which is received without restriction of confidentiality from a third party who is not in breach of an obligation of confidentiality in making such disclosure; and

4.2.4 Information of Mercedes-Benz which is shown by written record to have been independently developed by the Supplier or in cooperation with Supplier without any use of or reliance upon Confidential Information of Mercedes-Benz; and

4.2.5 Information of Mercedes-Benz which is or will be transferred to Supplier by this Requirements (e.g. transfer of usage rights or property rights, patent rights); and

4.2.6 Information with the purpose to be used in the public or combined with the right of publication (e.g. software with respective right of usage); and

4.2.7 Information which has to be disclosed due to legal obligations.

4.3 Supplier agrees to hold all Confidential Information of Mercedes-Benz in strict confidence at all times, and to secure and protect it from unauthorized disclosure using the same degree of care employed in the protection of its own Confidential Information, and in any event using not less than a reasonable degree of care to satisfy its obligations hereunder.

4.4 Confidential information may only be passed on to third parties after the written approval by Mercedes-Benz.

4.5 Supplier guarantees to commit its respective staff, assignees employees, agents, and if applicable also its sub-contractors, to comply with the confidentiality regulations set forth herein. Employees shall be required to be bound to a confidentiality commitment, as legally possible, which shall also be valid for the time after their employment relationship with Supplier. This Section shall also apply to such affiliated companies which sign individual agreements with the Supplier.

4.6 Notwithstanding the foregoing, Supplier may make disclosure of Confidential Information if such disclosure is mandatorily required by law or by legal process, provided that prior to making such disclosure that Supplier shall inform Mercedes-Benz of such fact and shall permit Mercedes-Benz to intervene in the applicable proceedings to protect its interests by seeking a protective order and other appropriate relief.

4.7 Supplier shall use their best efforts to assist Mercedes-Benz in identifying and preventing any unauthorized use, copying or disclosure of the Confidential Information or any portions thereof. Without limitation of the foregoing, Supplier shall advise Mercedes-Benz immediately in the event the Supplier learns or has reason to believe that any person to whom Supplier has given access to the

Confidential Information, or any portion thereof, has violated or intends to violate the terms of this Requirements, and the Supplier will, at its own expense, cooperate with Mercedes-Benz in seeking injunctive or other equitable relief against any such person.

4.8 If this Requirements expires or is terminated for any reason, Supplier shall promptly, and in any event within ten (10) business days following such termination, return to Mercedes-Benz or destroy all notes, memoranda, documentation, and other tangible materials embodying Confidential Information of Mercedes-Benz, and if requested, will certify as to such return or destruction by delivering to Mercedes-Benz a certificate signed by it Mercedes-Benz s president or chief execute officer.

4.9 The provisions on confidentiality stipulated herein shall survive this Requirements.

5. Data Protection

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

6. Right of Audit

6.1 Mercedes-Benz or its representatives shall have the right to carry out checks on compliance with the requirements. The Supplier shall provide the desired information and, at the request and within a reasonable period, submit documentary evidence that it has met its obligations.

6.2 Subject to advance notice, representatives of Mercedes-Benz shall be granted access to the offices and IT systems in/on which the data of Mercedes-Benz is used or processed so that the implementation of the contractual agreements and the appropriateness of the technical and organizational data security measures can be verified.

7. Onsite-Support and Remote Access

7.1 Mercedes-Benz shall, if and insofar as employees of the Supplier are deployed by mutual agreement to the premises of Mercedes-Benz for the performance of contractual obligations, grant the Supplier’s staff the required access to the premises and also provide adequate and appropriate workspace including appropriate working equipment.

7.2 In case that the Supplier’s staff does not use Mercedes-Benz computing devices, but devices of the Supplier, the Supplier shall ensure that these are protected according to the state of the art, including implementation of an approved malware scanning software. If the Supplier cannot comply with this requirement, Mercedes-Benz has to be informed about this without undue delay. Mercedes-Benz shall be allowed to scan the device for technical vulnerabilities and proper malware protection upon request.

7.3 The Supplier’s staff working in Mercedes-Benz facilities will be obliged to sign a non-disclosure agreement and comply with the security regulations applicable at the premises of Mercedes-Benz, including participation in security awareness trainings.

7.4 Mercedes-Benz is allowed to log and evaluate all activities on its systems.

7.5 All access rights to the systems or the premises of Mercedes-Benz which have been granted to the Supplier shall be revoked on termination of this Requirements. Furthermore, the Supplier shall ensure to take care for an

immediate return of any identification cards provided by Mercedes-Benz, via a channel to be determined by Mercedes-Benz.

7.6 Remote access to hardware and software of Mercedes-Benz, and to other data protected by this Requirements, is only allowed upon prior approval by Mercedes-Benz, and must occur through access points approved by Mercedes-Benz. Supplier shall ensure that IT systems of the Supplier used for remote access must be protected comprehensively against unauthorized or improper access.

7.7 If the Supplier performs Services via remote access, the Supplier shall explicitly comply with the currently applicable security guidelines of Mercedes-Benz for remote access and refrain from any actions that would violate these guidelines.

8. Secure Development

8.1 The Supplier will deploy a qualified Security Architects during the system design. The qualification shall include:

8.1.1 Formal education or training in the area of security architecture and design,

8.1.2 Demonstrated experience in secure information system design, and

8.1.3 Preferably formal certification.

8.2 Only qualified System Developers with demonstrated secure programming knowledge will be involved in the development of the systems. Supplier shall meet the requirement of the following qualification:

8.2.1 Formal education or training in the area of security programming,

8.2.2 Demonstrated experience in secure development, and

8.2.3 Preferably formal certification.

8.3 Upon request, the Supplier shall provide proof of the proper qualification of its staff. This may comprise, without limitation, curricula vitae, trainings, certificates etc. Mercedes-Benz is entitled to withhold its approval to deploy a particular person if there are legitimate doubts about the qualification of the person.

8.4 The Supplier is obliged to keep the quality of the source code, regarding information security, at the state of the art. This includes, but is not limited to, being free from vulnerabilities listed by OWASP. Upon request of Mercedes-Benz, the Supplier shall support source code audits and/or security scans performed by Mercedes-Benz (or a third party entrusted by Mercedes-Benz), by providing cooperation and access to supporting documentation.

8.5 The Supplier is obliged to remediate the security weaknesses in coordination with Mercedes-Benz without additional charges. If security weaknesses are revealed in connection with the acceptance procedure, Mercedes-Benz can refuse the acceptance. The Supplier shall provide immediate support to remediate the identified weaknesses.

8.6 Software outsourced for development is subject to Mercedes-Benz's quality assurance and systems security assurance requirements.

8.7 Security testing must be performed as part of systems acceptance and at pre-defined milestones during development, if required

8.8 Software developed must be tested in a controlled environment to detect anomalies prior to being accepted.

9. Others

9.1 This Requirements is the supplementary guarantee from Supplier to the General

Terms and Conditions and constitutes the entire agreement of the Mercedes-Benz and Supplier. In all other respects the General Terms and Conditions is hereby confirmed.

9.2 This Requirements shall prevail in case of any conflicts between this Requirements and the General Terms and Conditions.

9.3 This Requirements shall become effective as the same date as the General Terms and Conditions. The expiration date of this Requirements shall be the same date as that of the General Terms and Conditions.