Information Security Requirements for System Hosting Service

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

1. General Security Requirements

1.1 Business Continuity plan should be in place and approved by Daimler for the service hosted on Supplier side.

1.2 Compliance requirements must include processes to ensure that the handling and processing of Daimler information and/or devices remains in compliance with applicable laws, statutory, regulatory, contractual obligations and security requirements and to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

1.3 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 Daimler approval for changes to the production environment including applications.

1.4 Patch and vulnerability management must be defined and documented, to ensure system patches relevant with security are regularly and timely deployed and vulnerabilities are recognized, assessed and resolved.

1.5 Processes to backup data, to prepare for emergencies and to restart must be defined for the systems both at Daimler and at the Supplier. A log of the data backups and restarts providing a history of the changes must be guaranteed.

1.6 The Supplier must prepare secure technical means to allow Daimler to get an overview of the network traffic and the infrastructure systems in the hosting environment. This is to be possible at any time, without notice, at the Supplier's premises.

2. Technical Protection Controls

2.1 Supplier should follow detailed technical specifications and requirements from Daimler, or conduct system hardening on the basis of best practices specific to the system concerned after formal aligned with Daimler.

2.2 The Supplier must ensure that the operating status of the systems used within the hosting environment is permanently monitored. When irregularities occur (e.g. increased network traffic, authentication error), the Supplier must find the cause.

2.3 System health checks must be performed quarterly on Internet systems and/or the applications which are identified as business critical; and at least annually on all other

systems supporting Daimler, Daimler business partners or Daimler clients. The system health check must ensure it covers but not limited to below aspects:

- Only approved users hold security administrative or system authorities
- The required anti-virus detection programs are installed and operational
- The required access and activity logs data do exist and are being retained
- Deviations from expected or required results that are detected by routine health checks must be corrected by the Supplier within 30 days.
- The Supplier must provide Daimler management with reports on a pre-defined manner verifying the execution of applicable routine assurance tests, vulnerability scans, and patch/configuration maintenance for those systems/servers and applications supporting Daimler.

3. Right of Audit of DAIMLER

3.1 DAIMLER or its representatives shall have the right to carry out checks on compliance with the requirements of these 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.

3.2 Subject to advance notice, representatives of DAIMER shall be granted access to the offices and IT systems in/on which the data of DAMLER is used or processed so that the implementation of these requirements and the appropriateness of the technical and organizational data security measures can be verified.