对于系统托管服务的信息安全要求

供应商特此承诺遵守以下信息安全要求：

1. 范围

本要求适用于因履行与梅赛德斯一奔驰（中国）投资有限公司或其关联公司（以下简称梅赛德斯-奔驰）的合同时访问梅赛德斯-奔驰公司信息的外部合作伙伴、供应商以及所有其他个人或公司（以下简称"第三方"），例如顾问、运维和支持人员等。

2. 一般安全要求

2.1.针对在第三方托管的服务应当建立业务连续性计划并经过梅赛德斯-奔驰批准。

2.2.合规要求必须包括相关流程，以确保处理梅赛德斯-奔驰信息和/或设备的过程符合适用法律、法规、合同义务和安全要求，以及确保及时传达与信息系统相关的信息安全事件和漏洞并采取及时纠正措施。

2.3.信息系统的获取、开发和维护旨在确保存在一个流程来管理外包的生产或开发环境的变更。第三方必须建立变更管理流程，并获得梅赛德斯-奔驰对生产环境（包括应用程序）的变更的批准。

2.4.第三方应定义和记录补丁和漏洞管理，以确保定期及时部署与安全相关的系统补丁，并识别、评估和修复漏洞。

2.5.第三方应为梅赛德斯-奔驰和自身系统定义备份数据、准备紧急情况和重新启动的流程。必须确保开启记录数据备份和重新启动历史的日志。

2.6.第三方必须准备安全的技术手段，允许梅赛德斯-奔驰随时、无需事先通知的情况下，在第三方的场所获取托管环境中网络流量和基础设施系统的情况。

3. 技术保护控制

3.1.第三方应遵循梅赛德斯-奔驰的详细技术规范和要求，或在与梅赛德斯-奔驰正式达成一致后后，根据相关系统特有的最佳实践进行系统加固。

3.2.第三方必须确保托管环境内使用的系统的运行状态得到持续监控。当发生异常情况（例如网络流量增加、身份验证错误）时，第三方应确保找到原因。

3.3.针对被确认为支持关键业务的和/或面想互联网的应用程序，必须每季度进行系统健康检查；对于支持梅赛德斯-奔驰及其业务合作伙伴或梅赛德斯-奔驰客户的所有其他系统，至少每年进行一次系统健康检查。系统健康检查必须确保涵盖但不限于以下方面：

- 只有经批准的用户拥有安全管理员或系统权限；
- 所需的防病毒检测程序已安装并正常运行；
- 所需的访问和活动日志数据均被保留；
- 通过例行健康检查检测到的与预期或要求不符的结果必须由第三方在 30 天内进行纠正；
- 第三方必须以预定义的方式向梅赛德斯-奔驰管理层提供报告，以验证支持梅赛德斯-奔驰应用程序的系统/服务器和执行了所适用的例行测试、漏洞扫描和补丁/配置维护。

4. 梅赛德斯-奔驰的审计权

4.1.梅赛德斯-奔驰或其代表有权检查第三方是否符合以上要求。第三方应提供所需信息，并在要求下在合理的时间内提交文件证明其已履行义务。

4.2.在事先通知的情况下，梅赛德斯-奔驰的代表应被允许访问使用或处理梅赛德斯-奔驰数据的办公室和 IT 系统，以便验证这些要求的执行情况，并核实技术和组织上的数据安全措施是否得当。

此文件为中文译本，如与英文原版存在任何差异，应以英文原版为准。