对于软件开发的信息安全要求

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—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、承包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.作为第三方提供服务的一部分，第三方及其员工将获得访问梅赛德斯-奔驰信息的权限。第三方承诺遵守梅赛德斯-奔驰发布的所有信息安全和数据保护政策和指南。

2.2.如果第三方涉及分包商或自由职业者，必须首先获得梅赛德斯-奔驰的事先书面同意。第三方与分包商或自由职业者之间的合同安排必须与第三方要求相一致。特别是，第三方必须确保梅赛德斯-奔驰对分包商或自由职业者的审计权。

2.3.第三方必须确保分包商与第三方本身同样遵守梅赛德斯-奔驰的技术和组织要求。如果在合同关系的过程中替换或添加分包商，第三方必须首先获得梅赛德斯-奔驰的书面同意。

2.4.如果存在涉及可能影响梅赛德斯-奔驰的信息安全和数据保护要求的疑似违规行为，第三方应立即通知梅赛德斯-奔驰，并与梅赛德斯-奔驰协调，采取一切必要措施解决问题，防止数据保护和信息安全违规行为的恶化。

2.5.由于干扰、没收或任何其他政府访问、破产/结算程序等第三方的其他事件或措施导致数据面临威胁时，第三方应立即通知所有梅赛德斯-奔驰对上述数据拥有处置权的人员。

2.6.第三方必须指派一名安全经理，作为与梅赛德斯-奔驰安全人员的联络人，并作为调查信息安全和/或数据保护事件的第一联系人。指定的安全经理必须具备足够的授权和资源，以调查安全事件并解决所有可能出现的信息安全问题。

2.7.第三方应支持源代码审计（通过提供相关开发人员和辅助文档等）。

2.8.信息系统的获取、开发和维护旨在确保遵循流程来管理外包生产或开发环境的变化。第三方必须制定变更管理流程，并获得梅赛德斯-奔驰批准，才能对生产环境（包括应用程序）进行变更。

2.9.严禁第三方在梅赛德斯-奔驰系统中引入未记录和未经批准的系统入口，例如运维后门。

2.10.严禁第三方故意将恶意代码植入到梅赛德斯-奔驰的系统中。

2.11.在外包合同下开发的软件的源代码在开发期间和项目关闭前应归梅赛德斯-奔驰所有，并在项目结束前移交给梅赛德斯-奔驰做为梅赛德斯-奔驰的知识产权。如果第三方无法进一步开发或维护该应用程序，应设立源代码托管协议。

3. 技术保护控制

3.1.为了保护提供给第三方的梅赛德斯-奔驰的信息，第三方有义务保护其通信基础设施，包括但不限于反恶意软件保护、及时打补丁、正确配置、不使用默认密码，并验证已知的安全漏洞是否得到检查和修复，不得无故拖延。如果第三方无法遵守此要求，则必须立即通知梅赛德斯-奔驰。

3.2.第三方在履行合同义务的同时，应遵守正当处理数据的原则。这些原则包括病毒防护和备份，遵守数据保护法规以及 IT 行业内公认的注意事项及预防措施等。

3.3.第三方部署的数据应基于常见的信息技术标准进行病毒检查。如果检测到病毒，第三方不得部署此数据。如果第三方在梅赛德斯-奔驰的数据介质上检测到病毒，应立即通知梅赛德斯-奔驰，并有权暂停做业直至病毒被清除为止。

3.4.针对已公开或已知的信息安全漏洞，或由梅赛德斯-奔驰向第三方告知的漏洞，第三方应在规定期间内完成整改，除非与梅赛德斯-奔驰达成了额外的时间安排。

4. 保密性

4.1.除一般条款和条件第 14 条所述的机密信息外，数据处理中的机密信息包括但不限于：

4.1.1.与梅赛德斯-奔驰或其关联公司有关的所有技术数据；

4.1.2.商业秘密、专有技术、公式、软件开发技术、合成物质、发明、技术、流程、程序、图表、原理图、规格参数、客户和财务信息、销售和营销计划；

4.1.3.除以上信息外本要求的条款以及与之相关的任何谈判内容。

4.2.尽管有上述规定，以下内容不构成机密信息：

4.2.1.专利中披露的信息，或者以其他方式为公众或行业普遍所知，或在第三方不违反本要求的情况下广为人知的信息；

4.2.2.书面记录显示第三方在本协议项下披露之前已知晓的梅赛德斯-奔驰信息;

4.2.3.接收到无保密义务的第三方发送的不加保密限制的信息；

4.2.4.通过书面记录显示由第三方独立开发或与第三方合作开发过程中不使用不依赖梅赛德斯-奔驰的机密信息的信息；

4.2.5.根据本要求转让给第三方的梅赛德斯-奔驰信息（例如使用权或所有权、专利权）；

4.2.6.用于公共目的或有公开权（例如具有使用权的软件）的信息；

4.2.7.根据法律义务必须披露的信息。

4.3.为保护机密信息不被未经授权的披露，第三方同意在任何时候对梅赛德斯-奔驰的所有机密信息严格保密，以其保护自身机密信息的谨慎程度，并在任何情况下不低于合理程度来履行本协议所述义务。

4.4.仅在获得梅赛德斯-奔驰的书面批准后，保密信息才能传递给其他第三方。

4.5.第三方保证其员工、受让人、雇员、代理人和适用该规定的分包商，遵守此处规定的保密条款。雇员必须承担保密承诺，以法律允许的范围，该承诺也适用于其与第三方的雇佣关系结束后的时间。本章节也适用于与第三方签署单独协议的关联公司。

4.6.除上述规定以为，如遇法律或法律程序强制要求披露机密信息，在披露之前，第三方应将此类事实告知梅赛德斯-奔驰后第三方方可披露机密信息，并应允许梅赛德斯-奔驰干预适用的程序，通过寻求保护令和其他适当的整改措施来保护其利益。

4.7.第三方应尽最大努力协助梅赛德斯-奔驰识别和防止任何未经授权使用、复制或披露机密信息或其他信息的行为。无论在何种情况下，一旦第三方得知或有理由相信第三方提供任何内部保密信息，第三方内部任何人违反或意图违反本要求的条款，第三方应立即通知梅赛德斯-奔驰，并尽可能与梅赛德斯-奔驰合作，寻求针对此类人员的禁令或其他适当补救措施。

4.8.如果本要求因任何原因到期或终止，第三方应及时，在终止后十（10）个工作日内，将梅赛德斯-奔驰的所有内部保密信息的笔记、备忘录、文档和其他有形资料归还或销毁，并在请求时，通过向梅赛德斯-奔驰的总裁或首席执行官交付由其签署的证书，以证明此类归还或销毁。

4.9.此处规定的保密条款应在本要求终止后仍然有效。

5. 数据保护

5.1.如果在本要求的范围内第三方需要处理或访问梅赛德斯-奔驰或其关联公司的客户或员工的个人数据，第三方应当签署《委托数据处理协议》。

6. 审计权

6.1.梅赛德斯-奔驰或其代表有权对是否符合本要求的合规性进行审查。第三方应提供所需信息，并根据要求，在合理期限内提交证明其已履行义务的文件证据。

6.2.在事先通知的情况下，梅赛德斯-奔驰的授权人应有权访问使用或处理梅赛德斯-奔驰数据的办公室和 IT 系统，以便验证合同协议的实施以及技术和组织数据安全措施的适当性。

7. 现场支持和远程访问

7.1.如果第三方的员工经双方同意被授权到梅赛德斯-奔驰的场所以履行合同义务，梅赛德斯-奔驰应授予第三方员工进入场所所需的访问权限，并提供充足和适当的工作空间，包括适当的工作设备。

7.2.如果第三方的员工不使用梅赛德斯-奔驰计算设备，而是使用第三方的设备，第三方应确保根据最新技术水平保护这些设备，包括实施经批准的恶意软件扫描软件。如第三方不能遵守此要求，应立即通知梅赛德斯-奔驰。梅赛德斯-奔驰有权扫描其设备以检查是否存在技术漏洞和适当的恶意软件防护。

7.3.在梅赛德斯-奔驰场所工作的第三方员工将被要求签署保密协议，并遵守适用于梅赛德斯-奔驰场所的安全规定，包括参加安全意识培训。

7.4.梅赛德斯-奔驰有权记录和评估其系统上的所有活动。

7.5.在本要求终止时，已授予第三方的系统或场所访问权限将被撤销。此外，第三方应确保立即归还由梅赛德斯-奔驰提供的任何身份证明并由梅赛德斯-奔驰确认。

7.6.经梅赛德斯-奔驰事先批准后，第三方方可远程访问梅赛德斯-奔驰的硬件、软件和受本要求保护的其他数据，且必须通过梅赛德斯-奔驰批准的接入点进行访问。第三方应确保用于远程访问的第三方 IT 系统具备防未授权访问或防不当访问的能力。

7.7.如果第三方通过远程访问执行服务，第三方必须明确遵守梅赛德斯-奔驰当前适用的远程访问安全指南，并避免任何违反这些指南的行为。

8. 安全开发

8.1.第三方要在系统设计期间安排合格的安全架构师。资格应包括：

8.1.1.安全架构和设计领域的正规教育或培训；

8.1.2.在安全信息系统设计方面具有丰富的经验；

8.1.3.必要时需有相关资质认证。

8.2.只有具有安全编程知识的合格系统开发人员才能参与系统的开发。第三方应符合以下资格要求：

8.2.1.安全编程领域的正式教育或培训；

8.2.2.在安全开发方面具有丰富的经验；以及，

8.2.3.必要时需有相关资质认证。

8.3.根据要求，第三方应提供其员工适当资格的证明，包括但不限于简历、培训、证书等。如果对特定人员的资格有合理怀疑，梅赛德斯-奔驰有权拒绝使用该人员。

8.4.第三方有义务在信息安全方面保障源代码的质量，这包括但不限于没有出现 OWASP 列表中的漏洞。应梅赛德斯-奔驰的要求，第三方应通过提供合作和访问支持文档来配合梅赛德斯-奔驰（或梅赛德斯-奔驰委托的第三方）执行的源代码审计和安全扫描。

8.5.第三方有义务协助梅赛德斯-奔驰修复安全漏洞，不收取额外费用。如果在验收过程中发现安全漏洞，梅赛德斯-奔驰可拒绝验收。第三方应立即提供支持，以纠正已识别的漏洞。

8.6.外包开发的软件应遵守梅赛德斯-奔驰质量保证和系统安全保证的要求。

8.7.如需要，安全测试必须作为系统验收的一部分执行并作为预定义的开发过程中的里程碑。

8.8.开发的软件必须在受控环境中进行测试，以在被验收之前检测异常情况。

9. 其他事项

9.1.本要求是第三方对一般条款和条件的补充保证，构成梅赛德斯-奔驰和第三方的完整协议。在所有其他方面，以一般条款和条件为准。

9.2.在本要求与一般条款和条件之间存在冲突的情况下，应以本要求为准。

9.3.本要求将于与一般条款和条件的同一日期生效。本要求的到期日期应与一般条款和条件的到期日期相同。

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。