对于第三方访问的信息安全要求

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、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. 一般要求

2.1.一般要求

2.1.1.所有需要访问梅赛德斯-奔驰信息的第三方必须遵守梅赛德斯-奔驰的信息安全要求。

2.1.2.承包商和其他供应商访问必须仅限于为满足其与梅赛德斯-奔驰的合同要求所需的信息资源。

2.1.3.第三方组织必须将对梅赛德斯-奔驰信息的访问限制在为履行第三方合同义务所必须的员工范围内。

2.1.4.未经梅赛德斯-奔驰事先书面批准，第三方不得向其他组织（如分包商或合作伙伴）提供梅赛德斯-奔驰信息的访问权限。

2.1.5.第三方在履行合同义务后，或者在合同关系终止（如适用）后，有义务将从梅赛德斯-奔驰处收到的所有文件或存储的数据（包括副本）归还或销毁。如果梅赛德斯-奔驰要求，必须书面确认所有信息的完全归还或销毁。第三方无权保留梅赛德斯-奔驰的数据、文件和其他材料。

2.1.6.若有涉及可能影响梅赛德斯-奔驰的任何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，并在与梅赛德斯-奔驰协调的情况下立即采取一切必要的行动。

2.1.7.如果第三方在本协议范围内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，第三方必须签署委托数据处理协议。

2.1.8.梅赛德斯-奔驰有权记录和评估第三方在其拥有的系统上的所有活动。

2.1.9.第三方必须向负责人报告所有影响梅赛德斯-奔驰的信息安全事件和问题。这也适用于发生在第三方责任范围内且可能对梅赛德斯-奔驰造成负面影响的信息安全事件和问题。

2.1.10.发生在第三方责任范围内的所有信息安全事件和问题必须由第三方以对梅赛德斯-奔驰最小化风险的方式处理。

2.1.11.所有第三方有义务参与定期的信息安全审计，以确认梅赛德斯-奔驰要求的信息安全合规性。

2.2.第三方信息使用和责任

2.2.1.第三方必须负责地使用梅赛德斯-奔驰的信息资源，并且仅用于履行与梅赛德斯-奔驰的合同要求。第三方不得将梅赛德斯-奔驰的信息用于与合同约定目的以外的其他用途。

2.2.2.第三方必须遵守敏感区域员工的特定安全要求，这可能需要对个别员工进行安全审查。

2.2.3.第三方必须告知其所有将访问梅赛德斯-奔驰信息的员工和承包商与此类访问相关的安全责任。

2.2.4.第三方必须妥善保管 VPN 账户，并在合同业务结束后将其禁用。

2.3.第三方设备使用

2.3.1.第三方必须遵守合同中定义的联系人或有关在非梅赛德斯-奔驰设备上处理公司信息的合同限制。

2.3.2.第三方必须获得本地 IT 网络和第三方负责人的许可，才能将非梅赛德斯-奔驰设备连接到梅赛德斯-奔驰网络。许可必须基于遵守本文档以及详细说明第三方设备可接受使用的本地网络访问策略。

2.3.3.第三方使用的非梅赛德斯-奔驰设备应具备恶意软件保护措施。

2.3.4.第三方应采取合理的预防措施（例如及时应用关键软件安全补丁），以确保其非梅赛德斯-奔驰设备不会引入影响梅赛德斯-奔驰基础设施的安全威胁。

2.3.5.第三方应在服务团队变更时通知第三方联系人，并在离职或调动发生时向技术负责人或信息负责人发起相关访问权限变更请求。

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。