延锋国际汽车技术有限公司信息安全标准

1. 范围及总则

本安全标准遵循延锋信息资产创建、收集、接收、转让或以其他方式获得或披露给供应商的与服务有关的安全要求(安全措施和程序)作出规定。

如果本标准的规定与其他合同规定之间有任何冲突，应以对延锋信息资产更有保护性的规定为准。

为了满足延锋的高安全性和合规标准，供应商应实施充分和适当的技术和组织安全措施，以确保延锋信息资产不受意外或非法的破坏或意外损失、变更、未经授权的泄露或访问——特别是当处理涉及到通过网络传输数据时——考虑到处理所带来的相关风险。这些措施应在考虑到当前技术水平和实施成本的情况下，确保一定程度的安全，以适应处理所带来的风险和受保护数据的性质。

供应商应根据不低于行业标准的保护方法，定期审查和更新这些措施，并保持不变。在不限制其在本协议中另行规定的义务的情况下，供应商应遵守与其处理延锋信息资产相关的所有适用法律。

供应商保证并声明已实施符合或超过本安全附录所罗列的安全措施。供应商需要向延锋提供足够的文档以证明其遵守了该安全标准。

不履行这些义务构成严重违反本安全标准的，除延锋的其他权利外，延锋有权选择终止本协议。

2. 定义

“延锋”	应与本协议中所指的相同
“延锋信息资产”	应包括任何被定义、组织和管理为单一单位的、具有可识别和可管理的价值、风险、内容和生命周期的延锋信息或知识的任何主体。它包括延锋的信息计算系统和数据，具体包括个人数据。
“协议”	应包括任何种类的主服务协议、工作说明书（SOW）或延锋与供应商之间关于服务的任何其他种类的协议。
“安全事件”	a) 表明信息系统、服务或网络的安全性可能已被攻破或危害; b) 表示可能违反了信息安全策略或安全措施可能失败; c) 指具有负面后果或潜在负面后果的日志条目，如系统崩溃、网络数据包泛滥、未经授权使用系统特权、未经授权访问敏感数据或执行破坏数据的恶意代码。
“安全漏洞”	指导致意外或非法损毁、遗失、更改、未经授权披露或进入延锋信息资产（包括传送、储存或以其他方式处理的个人资料）的安全事件。
“个人数据”	指与已识别或可识别的自然人（“资料当事人”）有关的任何资料; 一个可识别的自然人是一个可以被直接或间接识别的人，特别通过参考身份标识符，例如姓名、身份证号码、定位数据、网上身份标识符，或参考一项或多项特定身体、生理、基因、心理、经济、文化或社会标识的个人。

“处理”	指针对个人数据或多组个人数据进行的任意一项或任意一组操作（无论是否属于自动操作），比如采集、记录、组织、结构化、储存或修改、检索、咨询、使用，通过传输、传播、提供等方式披露、调整、组合、阻拦、擦除或销毁。
“安全规则”	适用于供应商的关于信息安全的一般规则，包括有关信息安全的规则和最新标准，以及源自适用法例的规则（例如隐私法)。
“服务”	指本协议中所述的服务，或双方已签署的其他经双方一致同意的书面服务描述。
“分包商”	指由供应商或任何其他分包商聘请的直接或间接对延锋信息资产提供服务的服务供应商或提供方。包括任何涉及处理、访问、沟通、托管或管理延锋信息资产的服务，或将服务或产品添加或终止到现有信息中（由供应商聘用或包含到服务中的人员提供）。
“供应商”	处理延锋信息资产的除延锋以外的任何一方，包括云供应商和服务提供商。

3. 管理

3.1 人事

在授予个人对涉及延锋信息资产的设施，系统或数据的物理或逻辑访问权限之前，供应商应采取合理步骤，以确保其员工，在其授权下行事的其他人员以及在相关工作地点的其他人员（包括第三方用户，租户和/或客户）具有法律约束力的义务，这些义务要达到或超过本安全标准中提到的安全措施，相关机构已经实施或将要实施的措施或适用的安全规则所规定的（分包商的部分请参阅下面第 3.2 节）。

根据当地法律、法规、道德规范和合同约束，所有供应商的候选人和第三方应接受与所访问的数据分类、业务要求和可接受风险成比例的背景验证。供应商应确保其进入延锋信息资产的员工充分了解并具备保护延锋信息资产的技能。

3.2 分包商

当供应商将与延锋信息资产有关的工作分包给分包商时，任何时候必须始终遵守本安全标准规定的适用要求。供应商应根据要求提供分包商名单和适用的证明。如新的分包商对延锋信息资产的安全构成不可接受的风险，延锋可书面反对使用新分包商。

根据当地法律、法规、道德规范和合同约束，所有供应商的分包商均应接受与所访问的数据分类、业务要求和可接受风险成比例的背景核查。供应商应确保所有接触延锋信息资产的供应商分包商持有适用的安全证书，并遵循安全最高的措施。
供应商应确保所有分包商均受协议约束，包括与本标准一致并符合适用的安全规则的所有相关安全要求的明确范围。分包商特别需要使其人员承担上文第 3.1 节规定的基本类似的义务。
供应商应证明其遵守信息安全与机密性、服务定义和第三方合同中包含的交付水平协议。第三方报告、记录和服务应按计划的时间间隔进行审核和复核，以管理和保持对服务提供协议的遵守。
供应商仍须就其分包商在保护延锋信息资产方面的任何及所有表现向延锋负责。

3.3 应用程序的开发

供应商应用程序的设计应符合行业公认的安全标准（即用于 web 应用程序的 OWASP），并应遵守适用的法规和业务要求。
供应商应建立系统监控和评估程序，以确保质量标准得到满足，包括但不限于所有外包软件开发。供应商应监督和监控所有软件的开发，并应包括安全要求、由认证个人对环境进行的独立安全审查、对软件开发人员进行的认证安全培训以及代码审查。为实施本控制而进行的认证应定义为 ISO/IEC 17024 认可的认证或适用立法管辖范围内的法律认可的许可证或认证。
至少，供应商应在发布时提供错误列表和代码分析。

4. 技术和组织措施

供应商应实施以下技术和组织措施以确保延锋信息资产的安全:

4.1 物理访问控制

供应商应采取适当措施，防止未经授权的人员以任何方式访问延锋信息资产处理、转移或使用的数据处理设备。这可以通过以下方式来实现，例如，为数据处理设施（存放应用服务器、计算机硬件、数据库和相关设备等的房间）设置可上锁的入口。

4.2 准入控制

供应商应采取适当措施，防止未经授权的人员使用其数据处理系统。

4.3 虚拟访问控制

供应商应采取合适的措施，包括授权和解除授权流程，以确保授权使用处理系统的人员只能够在需要访问（授权）的范围内访问延锋信息资产,，并按照业务、安全、合规和服务水平协议（SLA）要求访问延锋信息资产,，并且在处理过程中和登录后，未经适当授权，延锋信息资产不能被读取、复制、修改或删除。
供应商应在员工、承包商、客户、商业伙伴或第三方的身份发生变化时，包括终止雇佣、合同或协议、变更雇佣或组织内部调动时，应及时取消、撤销或修改用户访问权限。
在供应商授予延锋信息资产和系统访问权限之前，所有已确定的安全、合同和监管要求应在适用情况下进行纠正。

4.4 传输控制

供应商应采取适当措施，确保在电子传输、运输或保存到数据载体上时，延锋信息资产未经授权不得被读取、复制、修改或删除，并确保可被检查以确定将延锋信息资产通过数据传输设施移交给哪些机构。

适用于提供网络服务的供应商

应设计和配置供应商网络环境，以限制可信和不可信网络之间的连接，并按计划的间隔进行审查，记录所有使用的服务、协议和端口的业务理由，包括那些被认为不安全的协议的基本原理或补偿控制。网络架构图必须清楚地标识可能对合规性有影响的高风险环境和数据流。

4.5 作业/分配控制

供应商应采取适当措施，以确保在委托加工延锋信息资产的情况下，延锋信息资产严格按照延锋的指示进行加工。

4.6 能力和资源规划/业务连续性/可用性控制

4.6.1 能力与资源规划

供应商应根据法规、合同和业务要求，计划、准备和测量其系统的可用性、质量、足够的当前和预防能力和资源，以交付所需的系统性能。供应商应根据要求向延锋提供容量/资源规划指标和适用评估的副本。

4.6.2 业务连续性

供应商应实施并保持业务连续性计划；确保供应商服务（即客户服务、技术支持、事件管理）的连续性。供应商应每年进行一次业务连续性作业，并应在延锋要求的 30 天内提供业务连续性演练的证明。证明应包括作业的日期和时间、作业的范围、概述和结论。

4.6.3 可用性控制

供应商应采取适当措施，以确保延锋信息资产不受意外破坏或损失及服务攻击。

对提供托管服务的供应商的额外备份/灾难恢复要求:

供应商应确保所有延锋信息资产定期备份，以便在发生灾难时快速恢复。应用程序和系统架构应该支持延锋的灾难恢复时间目标（RTO）和恢复点目标（RPO）。

供应商应实施和维护灾难恢复程序；确保本协议提供给延锋的技术、应用和软件服务的连续性。供应商应每年进行一次灾难恢复演习，并应在延锋要求的 30 天内提供灾难恢复演习的证明。证明应包括：

- 演习范围
- 概述与结果
- 达到的恢复时间目标
- 达到的恢复点目标
- 用于验证 RPO 的方法

具体而言，供应商应采取措施确保：

-至少每天进行备份；

-磁带备份存储在异地，当数据库服务器的数据存储设备出现故障时可以进行恢复；

-只有延锋可授权恢复备份（如有）或将数据移至存放物理数据库的地点以外，并会采取安全措施，以避免资料在被转移后遗失或未经授权被查阅；

-备份磁带只有在以下情况下才可重复使用：未包含企业专有信息或者在重用后无法通过任何技术手段重新恢复其中的数据；除可重用的可移动介质之外废弃不用时应当被销毁；备份的恢复测试应当按计划进行。

4.7 输入控制和记录

供应商应保留审计日志，记录用户访问活动、任何数据的修改或删除、授权和未经授权的访问尝试、系统异常和信息安全事件，并遵守适用的政策和法规。供应商应至少每天检查审核日志和文件完整性（主机）和网络入侵检测（IDS）工具，以帮助及时检测。通过对分析，调查得出根本原因，并对事件做出响应。

4.8 分离控制

供应商应确保延锋信息资产与其他客户数据的清楚分离。必须在包括应用程序在内的逻辑级别上确保分离，最好在物理级别上进行分离。

供应商应确保为不同目的收集的数据可以单独处理。

4.9 其他可行的安全措施

4.9.1 漏洞/补丁管理

供应商应建立针对供应商漏洞和补丁管理的政策和程序并实施机制，确保应用程序、系统和网络设备漏洞得到评估，并及时应用供应商提供的安全补丁，采用基于风险的方法对关键补丁进行优先处理。

4.9.2 杀毒/反恶意软件

供应商应确保所有杀毒程序都能够检测、删除和保护所有已知类型的恶意软件或未经授权的软件，且防病毒定义至少每 12 小时更新一次。

4.9.3 安全检查

供应商应提供持续的安全检查，以确保数据安全，并防止由于应用程序中的安全漏洞或通过员工恶意造成的破坏。

4.9.4 未经授权的软件安装

供应商应制定政策和程序，并实施机制来限制未经授权软件的安装。供应商应报告任何例外情况，并在安装前得到延锋的批准。

4.9.5 生产变化

供应商提供的延锋生产环境的变更应记录下来并进行测试，并在实施前得到延锋的批准。生产软件和硬件的变化可能包括应用程序、系统、数据库和网络设备，需要补丁、服务包和其他更新和修改。

5. 信息安全管理系统

5.1 一般管理系统

供应商应保持适当的信息安全管理程序，并充分传达给员工、供应商和其他相关外部方。

5.2 第三方管理报告

供应商应提供安全控制及其有效运行的证据，并向延锋提供一份可接受的年度第三方安全报告，该报告的范围仅限于延锋从供应商和所有接触延锋数据的供应商分包商处采购的特定服务，例如 SSAE-16（美国）、CSAE-3416（加拿大）、ISAE-3402（国际）SOC 2 第 2 类年度报告。本年度安全报告将遵循 SOC 2 第 2 类报告的 AICPA 标准，并将包括与 AICPA 信任服务原则和标准相关的供应商控制的测试和有效性，这些原则和标准与安全性、保密性、处理完整性、隐私和可用性相关。

供应商同意以商业上合理的方式和时间框架纠正该报告中披露的任何重大缺陷。
供应商还应每年提供一份可接受的第三方系统/应用渗透安全报告和漏洞评估安全报告。

适用于延锋信息资产的供应商

供应商应制定、记录、批准和实施信息安全管理计划（ISMP），其中包括行政、技术和实物保障措施，以保护资产和数据不受损失、滥用、未经授权的访问、披露、更改和破坏，如 ISO 27001:27005

5.3 审计/检查

此外，在计划的时间内和事先书面通知的情况下，延锋可以检查供应商的操作设施或进行审计，以确保供应商符合政策、程序、标准和适用的法规要求，并确定是否符合本标准。延锋或一个独立的审计小组可以进行检查。供应商应充分配合延锋发起的任何此类审计和调查程序。

6. 风险管理

供应商应开发和维护企业风险管理框架，将风险管理到可接受的水平。供应商应至少每年或按计划的时间间隔进行正式的风险评估，以确定所有已识别风险的可能性和影响。

供应商应将风险降低到可接受的水平。基于风险标准的接受水平应根据合理的解决时间框架和执行批准建立并形成文件。
供应商应提供网络安全保险的证据，即隐私/网络安全（网络）责任保险，针对(1)安全违规（无论怎么发生）；(2)系统漏洞；(3)服务中断；(4)恶意软件代码的引入、植入、传播；(5)未经授权而进入或使用电脑系统提供责任保护。本政策没有任何先决条件，包括对未加密的便携设备/媒体的任何排除/限制。最低保险限额- 10,000,000 美元。

7. 事件、事故、威胁和漏洞管理/安全事件和违反通知

供应商应制定政策和程序，对安全相关的事件进行分类，并确保及时和彻底的事件管理。
若发生潜在的安全漏洞，供应商应立即通知延锋。资料须提供有关延锋信息资产的细节，包括：

- 有关受影响人士的信息，例如受影响人士的类别及人数；
- 非法披露性质的描述；

- 联系人的身份和联系方式 ；
- 潜在的安全漏洞可能造成的后果，以及
- 建议的措施，以尽量减少可能的损害。

供应商应提供延锋要求的所有额外信息，以调查潜在的安全漏洞。此外，如果（i)供应商或其人员、关联公司或分包商违反本标准下的安全规则或义务；（ii)处理过程中发生重大故障；或（iii)对本款第（i)、（ii)项规定的事件的发生存在合理怀疑，供应商应立即通知延锋。供应商在与延锋协商后，应采取适当措施确保延锋信息资产的安全，并限制对延锋和任何人可能造成的不利影响。
若因安全漏洞而导致的跟进行动需要采取法律行动，则须受有关司法管辖区所管限，在有关司法管辖区的管辖下，供应商及任何分包商须执行适当的法律程序，包括保管链，以收集、保留及出示证据，并应在提出要求时提供。

8. YANFENG IA 的退还和删除

在合约条款终止后，除非适用规则要求储存，卖方应根据延锋的决定，退回延锋或销毁并删除所有从延锋处理的延锋信息资产及其他包含延锋信息资产的资料。此外，所有延锋信息资产应从任何计算机、服务器、媒体、存储或类似设备中删除，包括由供应商或其分包商存储或处理的备份存储。供应商应证明这是应延锋的要求所做的。
供应商应建立政策和程序，并实施安全处置和完全移除所有供应商存储的延锋数据的机制，并对适当处置进行认证。