软件供应链安全管理自查表（供应商）

供应商单位名称：西安长天长软件股份有限公司

| 检查项分类 | 子类 | 检查项 | 结果（是/否） | 备注 |
| --- | --- | --- | --- | --- |
| 供应商检查 | 安全管理体系检查 | 1.是否建立了完善的信息安全管理体系，如具有ISO27001 等相关认证 | 是 | ISO27000 |
| 软件生命周期安全检查 | 网络安全措施 | 2.系统开发、测试环境是否具有安全防护措施，如防火墙、入侵防范、安全审计等 | 是 |  |
| 代码仓库及关键文档管理 | 3.代码仓库是否存在权限管控，代码仓库、关键文档（包含但不限于网络拓扑图、需求文档、设计文档、开发文档、测试文档、互联网协议地址规划等）放置位置是否在内网。 | 是 |  |
| 安全测试规范 | 4.产品交付或上线前，是否进行漏洞扫描、安全测试、源代码审计、性能测试、渗透测试和功能测试等措施。 | 是 |  |
| 发布管理规范 | 5. 是否制定软件安全发布管理流程，包含但不限于责任人、发布流程（包含发布时间、发布内容、异常处理措施、发布审核等）、发布方式方法等内容 | 是 |  |
| 交付 | 6.是否提供对产品中的所有功能模块、外部接口，以及私有协议用途的说明文件 | 是 |  |
| 7.是否明确告知用户产品中预置的所有账户和默认口令 | 是 |  |
| 8.是否提供操作指南、安全配置指南等指导性文档，以说明产品的安装、启动和使用的过程 | 是 |  |
| 下线 | 9.下线产品是否协助需方进行数据迁移，迁移完成后是否进行数据完整性校验 | 是 |  |
| 合规性与知识产权检查 | 合规性检查 | 10.是否在合同不允许的情况下，将需方单位项目进行转包或分包 | 否 |  |
| 知识产权检查 | 11.软件中使用的所有第三方组件和库是否具有合法的使用权限 | 是 |  |
| 运维与更新检查 | 运维管理 | 12.是否按照运维管理制度和流程进行实施，包括故障处理、应急响应等 | 是 |  |
| 13.运维人员内部的账号分配权限设置是否合理，是否遵循最小化授权原则 | 是 |  |
| 14.运维人员访问受控网络前是否经过授权审批 | 是 | 访问前需申请VPN账号及堡垒机，通过授权后可使用 |
| 15.软件安装与升级前是否获得需方单位的同意 | 是 |  |
| 16.运维人员进行远程维护是否经过安全连接 | 是 | Vpn+堡垒机 |
| 17.在对设备进行系统维护前，是否提前告知服务单位将开展的维护内容、风险及应对措施 | 是 |  |
| 18.是否对维护过程留存不可更改的日志记录，记录内容至少包括维护时间、维护内容、维护人员、远程维护方式及工具等 | 是 |  |
| 漏洞管理 | 19.对已发现漏洞，是否及时进行修复并发布安全更新 | 是 |  |
| 数据安全 | 20.数据是否按照需方单位要求进行备份 | 是 |  |
| 21.是否对供方数据的拷贝、导出、多供应商之间数据共享等操作 | 否 |  |
| 人员与培训检查 | 安全教育培训 | 22.是否对相关人员进行了软件供应链安全教育培训，培训内容是否包括安全法律法规、安全威胁与防范（如钓鱼邮件）等方面 | 是 |  |
| 23.开发人员是否进行开发安全技能培训，如源代码编写安全培训、安全架构培训 | 是 |  |

供应商单位签字：

日期：