西乡县雪亮工程视频专网共享平台建设及存储替换改造项目合同

2026 年 1 月

甲方：西乡县公安局

负责人：徐芳

统一社会信用代码：11610724016040410 3

联系地址：陕西省汉中市西乡县城北街道办事处金牛路 10 号

联系电话：0916-6320702

乙方：中移建设有限公司

负责人：孙卫东

统一社会信用代码：91110108748105996C

联系地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

联系电话：010-51844153

为提升西乡县公安局云计算能力及信息化水平，甲乙双方经友好协商，本着互惠互利、公平公正的原则，一致同意在“西乡县雪亮工程视频专网共享平台建设及存储替换改造项目”开展合作。为明确甲乙双方的权利与义务，根据《中华人民共和国民法典》相关法律法规的规定，双方就有关事宜达成以下协议：

第一条　项目概况

（一）项目名称：西乡县雪亮工程视频专网共享平台建设及存储替换改造项目

（二）施工地址：陕西省汉中市西乡县

第二条　合作方式

合作方式：甲方采用购买服务模式，乙方根据客户的需求为甲方提供西乡县雪亮工程视频专网共享平台建设及存储替换改造项目建设服务。

第三条　项目内容

服务内容如下所示，双方如需延展合作领域，后续以补充协议形式，明确合作内容及双方权益。

（一） 服务内容

通过私有云部署实现项目资源的集约化管理，保障雪亮工程视频监控数据、业务应用数据的本地可控、安全可靠；提升平台数据处理能力、存储容量及访问效率，满足视频专网内多部门、多终端的数据共享需求；实现存储资源的弹性扩容，适配雪亮工程业务拓展需求。

（二）工期：30 日历天。

（三）质保服务期限：5 年。

第四条　费用和结算

（一）费用标准

乙方按照协议约定，对甲方提供视频专网共享平台建设服务；

协议总金额：含税总价¥1978500.00 元（大写：人民币壹佰玖拾柒万捌仟伍佰元整）；不含税总价¥1866509.43 元（大写：人民币壹佰捌拾陆万陆仟伍佰零玖元肆角叁分）；增值税率 6%。

（二）费用支付

1、（1）合同签订生效，全部设备到场，经甲方、监理验货后 ，达到付款条件起 10 日内，支付合同总金额的 30.00%。

（2）设备安装完成，且运行正常，经甲方初步验收合格后 ，达到付款条件起 10 日内，支付合同总金额的 40.00%。

（3）项目最终验收合格，且完成审计后 ，达到付款条件起 10 日内，支付合同总金额的 30.00%。另需向财政专户缴纳合同总金额的 3%为质保金，待质保服务期满后，且设备运行正常，乙方提出申请，甲方同意，退还质保金。

2、双方结算相关信息如下：

甲方名称：【西乡县公安局】

国税纳税人识别号：【11610724016040410 3】

户名：【西乡县公安局】

开户行：【西乡县农商银行营业部】

帐号：【270611010120100005 3734】

乙方名称：【中移建设有限公司】

国税纳税人识别号：【91110108748105 9966】

户名：【中移建设有限公司】

开户行：【招商银行股份有限公司北京分行营业部】

账号：【888801480001 3154】

第五条　双方的权利和义务

（一）权利保证

1、乙方保证对其出售的货物享有合法的权利。

2、乙方保证对其出售的货物上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权。

3、乙方保证对其出售的货物或其任何一部分没有侵犯第三方的专利权、版权、商标权或其他权利。

4、如甲方在使用该货物构成上述侵权的，则由乙方承担全部责任。

（二）包装要求与运输方式

1、除合同另有规定外，乙方提供的全部货物均应按标准保护措施进行包装，该包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全运抵指定地点。

2、每一包装单元应附详细的装箱单和质量合格证。

3、乙方负责货物(产品)运输及运输途中的一切安全责任，货物运输的合理损耗及计算方法乙方支付。

（三）货物验收

1、货物验收由甲方组织，乙方配合，并按下列程序进行：

（1）交货验收时，乙方须提供质检部门产品抽样检查合格的检测报告(或生产厂家自检报告)及所提供货物(产品)的合格证、装箱清单、配件、随机工具、用户使用手册(产品使用说明书)、保修卡等资料交付给甲方；

（2）到货验收：货物到达后，甲乙及监理三方共同勘验货物，同时检查货物外观，是否有划痕或破损的,对产品无任何异议后,三方共同签字确认。

（3）货物初验：乙方应在货物到货之日起，30 日内全部完成安装调试完毕；乙方安装调试完毕后提出验收申请 3 日内完成初步验收；初步验收合格后，进入 15 日试用期；试用期间发生重大质量问题，修复后试用期相应顺延；

（4）货物终验：试用期结束后，甲方组织相关部门人员进行最终验收；

（5）验收合格，双方签署验收报告。

2、货物验收依据：

（1）招标文件；

（2）投标文件；

（3）采购合同及补充协议；

（4）质检部门抽样检查货物(产品)合格的检测报告。

3、货物验收时发现问题的处理办法：

（1）乙方提供不符合磋商文件和本合同规定的货物(产品)，甲方有权拒绝接受；

（2）如发现所交付的货物有短装、次品、损坏或其它不符合标准及本合同规定之情形者，甲方有权要求更换货物(产品)，同时做出详尽的现场记录，或由甲乙双方签署备忘录，此现场记录或备忘录可用作补充、缺失和更换损坏部件或更换整个货物(产品)有效证据，由此产生的时间延误与有关费用由乙方承担，验收期限相应顺延；

（3）如货物经乙方 3 次维修仍不能达到合同约定的质量标准，甲方有权退货；并视作乙方不能交付货物而须支付违约赔偿金给甲方，甲方还可依法追究乙方的违约责任；

（4）乙方不能完整交付货物及本条第一款规定的单证和工具的，必须负责补齐，否则视为未按合同约定交货。

（四）售后服务

乙方应按照国家有关法律法规和“三包”规定以及招标文件要求和投标文件的“服务承诺”提供服务。

（1）乙方须指派专人负责与采购人联系售后服务事宜；

（2）货物(产品)的现场安装、调试和启动监督；

（3）就货物的安装、启动、运行及维护等对采购人的人员进行免费培训。主要培训内容为货物的基本结构、性能、主要部件的构造及处理,日常使用操作、保养与管理、常见故障的排除、紧急情况的处理等，如采购人未使用过同类型货物，成交供应商还需就货物的功能对采购人的人员进行相应的技术培训，培训地点主要在货物安装现场或由采购人安排；

(4)质保期自采购人在货物质量验收单(终验)上签字之日起计算,质保费用

计入总价；

（5）质保期内，乙方负责对其提供的货物整机进行维修和系统维护，不再收取任何费用，但不可抗力(如火灾、雷击等)造成的故障除外；

（6）货物故障报修的响应时间为：工作期间(星期一至星期五 8:00-18:00)为 4 小时；非工作期间为 6 小时；

（7）乙方在接到采购人通知后须 8 小时内完成维修或更换，并承担修理或更换的费用；

（8）所有货物服务方式均为乙方上门服务，即由乙方派员到货物使用现场维修，由此产生的一切费用均由乙方承担；

（9）乙方在质保期内所有硬盘提供免回收服务；

（10）乙方承诺本次所建设的视频专网共享平台与汉中市公安局平台及西乡县公安局平台市县无缝对接。

（11）乙方须遵守甲方保密规定，如有严重违规行为，甲方有权中止合同。

第六条　违约责任

协议期内双方应共同遵守以上协议各项条款，依据《中华人民共和国民法典》《中华人民共和国政府采购法》的相关条款规定和本协议约定，若有违约，履约方可要求违约方限期改正并承担违约责任。

1、甲方逾期付款的，应按逾期付款金额每日万分之一计算，向乙方支付逾期付款的违约金。若甲方在协议规定的时间未能按时支付费用，乙方有权强制停止本次提供的服务，并通过法律程序追缴欠款，因此造成的全部损失（包括诉讼费、案件受理费、律师费、保全费等）由甲方承担。

2、协议履行中甲方违反协议规定拒绝接受服务的，应承担由此给乙方造成的一切损失。

3、如因不可抗力事件的发生导致协议无法履行时，遇不可抗力的一方应立即将事故情况告知另一方，并应在不可抗力事件结束后（30）日内，经双方认可后协商终止协议或暂时延迟协议的履行。本协议所称不可抗力是指不能预见、不能克服、不能避免并对一方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、火灾和风暴等以及社会事件如战争、动乱、政府行为、瘟疫等。

4、如因甲方原因导致工作不能正常进行或中止的，甲方应按照乙方的要求进行协调，并承担因此造成的违约责任，每中止一天，甲方应向乙方支付施工费用总额的 3‰作为违约金，违约金总额不得超过施工费用总额的 10%。

协议期内双方应共同遵守以上协议各项条款；若发生争议，当事人应协商解决；协商不能达成一致时，可向**甲方所在地有管辖权的人民法院**提起诉讼。

第七条　税务条款

协议双方将承担中国有关机构根据中国税务法律向其征收的所有与协议执行有关的税款，在本协议履行过程中无偷漏税等违法行为，双方应各自承担其未按中华人民共和国相关税务法规足额缴纳税款而产生的全部责任。乙方在甲方支付协议款项时，应向甲方开具符合国家法律法规和标准的正式发票。

第八条　廉政条款

甲乙双方不得以任何不正当手段（如向对方领导或经办人行贿、给回扣、提供免费旅游或其他消费娱乐等）谋求对方同意签订协议。如发现有上述行为事实，无过错方有权终止协议。双方领导或经办人不得以任何借口要求对方为其个人提供金钱、物品、免费旅游或其他消费娱乐等不正当利益；如发现有上述行为事实，无过错方应向对方纪检监察部门如实举报，纪检监察部门应依纪依法予以追究查处，并向本单位领导汇报，以便采取措施，保护相对方单位正当的市场销售权益。

第九条　保密条款

任何一方不得将本协议内容向其他方泄露。

未经对方书面许可，任何一方不得将其持有的有关另一方的事务或其事务运行操作方法等保密信息向协议以外的其他方或公众透露，且不得对保密信息进行拷贝和抄写。

因执行本协议的需要，双方均有权向该方人员或该方当地公司及控股公司人员透露或使其接触从另一方获知的工作流程类保密信息，但应当尽量控制知情人员的范围，不得在本单位内部任意扩散对方的保密信息。

双方的职员违背保密承诺，未按照本协议的规定使用保密信息或向其他方披露保密信息，或向其他方做出任何建议，都被视为违反本协议。如任何一方违反本协议，违约方应按照《中华人民共和国民法典》的相关规定承担违约责任。

本保密协议对双方都具有约束力。本协议规定的保密责任的期限为自本协议生效之日起至本协议终止之日止。

第十条　安全条款

一、数据服务

（一）基本安全要求

1.1 乙方应针对本项目设置安全负责人岗位，全面负责和管理本项目的网络安全相关工作。

1.2 乙方应根据甲方数据分类分级情况，采取相应的加密、备份、访问控制及安全审计等措施。

1.3 未经甲方同意，乙方不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析。

1.4 乙方应选择合适的数据存储架构和介质在中国境内存储公安数据，数据存储介质、存储期限按照国家和公安机关有关规定执行。

1.5 乙方收集的数据范围应为实现提供的产品或者服务的业务功能所必需的最小范围。

1.6 乙方应与甲方签订数据处理运维安全责任协议、保密协议。

1.7 乙方人员调离时，须立即终止相关人员权限并完成数据资产交接审计。

1.8 乙方应配合甲方对其开展的远程检测和现场检查。

（二）代建场景

2.1 乙方应协助甲方进行数据分类分级，并明确数据处理的目的、规模、方式、范围、类型、存储期限、存储地点、分类分级说明等。

2.3 乙方在涉及个人信息处理时，应提供个人信息主体授权同意和授权撤回的功能。

2.4 乙方在对个人信息处理进行任何变更，包括但不限于目的、类型、范围和用途时，应通知甲方让个人信息主体重新授权同意。未经个人信息主体的重新授权同意，乙方不得执行任何变更。

2.5 乙方以甲方名义从外部机构收集个人信息前应获得甲方同意，并向甲方说明数据收集的范围、频度、类型以及用途等规则，并获得个人信息主体的授权同意。

2.6 乙方应对数据收集过程进行日志记录，确保信息来源的可追溯性，日志的留存期限不少于 6 个月。

2.7 乙方应按照甲方的数据分类分级情况，对数据传输采取对应的安全管控措施，如签名验签、双向认证、传输通道加密、数据内容加密等。

2.8 乙方应建议甲方在网络边界采用防火墙、入侵检测等具体的安全技术或者设备，以保障数据传输网络的安全性。

2.9 乙方应按照甲方的数据分类分级情况，明确相关人员的访问权限，防止未授权访问。

2.10 乙方应对数据处理建立数据泄露控制规范和机制，防止数据处理过程中的调试信息、日志记录、不受控制输出等泄露受保护的个人信息、重要数据等敏感信息。

2.11 乙方应妥善留存和甲方相关的重要数据、个人信息处理活动记录日志，一般日志留存期限不少于六个月。涉及向他人提供、委托处理重要数据和个人信息的，相关日志留存时间不少于三年。

2.12 乙方应对与甲方相关的重要数据、个人信息的关键操作（如批量修改、拷贝、删除、下载等）设置审批流程和记录日志，以满足访问控制与审计的需求。

2.13 乙方在委托第三方开展与甲方相关的数据处理活动时，应经甲方同意并对数据处理活动进行监督；原则上乙方应使用去标识化处理的数据集，重要数据、个人信息原则上应脱敏后进行数据处理。匿名化或者去标识化处理的数据，非业务所必须，禁止把相关处理技术措施告知其他部门或者企业，防止被重标识，匿名化或者去标识化的数据汇聚融合后，进行集成和分析。

2.14 乙方应采用数据脱敏、数据水印等数据保护技术，控制数据的使用目的、范围和效果，降低数据泄露风险。

2.15 乙方应无偿、积极、有效配合甲方依据协议规定对其数据处理活动开展的审核、评估及内外部审计检查工作，并应配合监管机构针对甲方开展的审查和监管工作。

2.16 乙方向第三方提供个人信息的功能，应通知甲方向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，仅在获得个人信息主体授权同意后才能向第三方提供并记录日志，并进行安全审计。

2.17 乙方向第三方提供重要数据的功能，应通知甲方并记录日志，支持安

全审计。

2.18 乙方应对拟披露数据提供数据脱敏处理、审批流程功能。

2.19 乙方应按甲方要求向其提供为开展前述工作所需的全部信息，且不得隐瞒任何可能对前述工作和甲方合法利益造成影响的信息。

2.20 乙方应积极配合甲方，协助甲方应对监管机构检查、个人信息主体的权利请求以及个人信息主体或者第三方的投诉。

2.21 乙方应采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不可恢复。

2.22 乙方应协助甲方制定重要数据、个人信息的安全事件应急预案。

2.23 乙方应按照甲方的数据分类分级要求对数据分域分级存储，如涉及重要数据、个人信息的应在公共信息网络与存储系统之间提供逻辑隔离措施。

2.24 乙方应提供重要数据备份与恢复功能，支持备份与恢复的范围、频率、工具、过程、日志记录规范、数据存储期限等。

2.25 乙方应提供数据删除技术措施和工具，支持对重要数据及其副本进行删除。

2.26 乙方应通过权威的供应链安全机构的专项软件检测认证。

（三）代理运维（系统运维）服务场景

3.1 甲方应制定数据备份与恢复计划，明确备份与恢复的范围、频率、工具、过程、日志记录规范、数据存储期限等。

3.2 甲方应制定数据安全事件的应急响应计划。一旦发生数据安全事件时，甲方应主导并按照计划快速响应。

3.3 甲乙双方应通过合同等形式，明确双方的数据安全保护责任和义务。

3.4 乙方应确保数据只在甲方环境中传输，若需要传出甲方环境，乙方需在评估数据使用范围、目的、规模等内容后向甲方发起申请，并在征求甲方书面同意后进行传输。

3.5 乙方应根据甲方制定的策略自动化执行备份与恢复相关活动，并记录数据备份与恢复过程。

3.6 乙方应对与甲方相关的重要数据、个人信息所在的数据中心的运维人员建立严格管理制度，对所有运维人员进行安全审查。

3.7 乙方应与与甲方相关的重要数据、个人信息处理人员签订安全责任协议和保密协议，人员调离时应收回组织的软硬件资产，移交调离人员的重要数据、个人信息处理岗位职责，及时终止调离人员的重要数据、个人信息处理权限，并确保其调离后在合理期限内继续履行保密义务。

3.8 乙方在发生数据安全事件时，应在获知信息后的 2 小时之内通知甲方。

3.9 乙方在发生数据安全事件时，应快速协助甲方依照应急响应计划执行，按照事件起因确定责任方，由责任方承担相关损失。通知后 2 小时之内未及时响应的一方也需承担相关责任。

3.10 乙方应积极配合甲方，协助甲方应对监管机构检查、个人信息主体的权利请求以及个人信息主体或者第三方的投诉。

3.11 乙方未经甲方同意，不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析。

3.12 乙方应采用技术工具和措施管理存储介质，追踪与甲方数据相关的介质使用和传递过程，对介质的访问、使用和销毁等全过程行为进行记录和审计，并定期对介质销毁记录及销毁效果进行检查。

3.13 乙方在与甲方相关的重要数据、个人信息的存储介质进行报废处理时，应采用物理损毁等方式销毁介质，以确保重要数据、个人信息不能被恢复。

（四）SaaS（存储数据）服务场景

4.1 甲方在委托乙方开展数据处理活动时，原则上应使用去标识化处理的数据集，重要数据、个人信息原则上应脱敏后进行数据处理。匿名化或者去标识化处理的数据，非业务所必须，禁止把相关处理技术措施告知其他部门或者企业，防止被重标识，匿名化或者去标识化的数据汇聚融合后，进行集成和分析。

4.2 乙方应完成数据分类分级，并明确数据收集目的、规模、方式、范围、类型、存储期限、存储地点等。

4.4 乙方在涉及个人信息处理时，应提供个人信息主体授权同意、授权撤回的功能。个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等环节。

4.5 乙方在对个人信息处理进行任何变更，包括但不限于目的、类型、范围和用途时，应重新获得个人信息主体授权同意，否则乙方不得执行任何变更。

4.6 乙方在从外部机构收集个人信息时，应明确说明数据收集范围、频度、类型以及用途等规则，并获得个人信息主体的授权同意。

4.7 乙方在未获得或者撤回个人信息收集授权的情况下，应提供与个人信息无关的安全功能。

4.8 乙方应对数据收集过程进行日志记录，确保信息来源的可追溯性，日志的留存期限不少于 6 个月。

4.9 乙方在处理和甲方相关的重要数据、个人信息时，应不超出约定的目的、范围和方式。

4.10 乙方应提供不低于甲方的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面。

4.11 乙方应要求重要数据、个人信息接收方提供不低于乙方的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面。

4.12 乙方应按照甲方的数据分类分级对数据传输采取对应的安全管控措施，如签名验签、双向认证、传输通道加密、数据内容加密等。

4.13 乙方在数据传输过程中，涉及甲方的重要数据、个人信息或者关键信息基础设施的，应采用符合《中华人民共和国密码法》和《信息安全技术 信息系统密码应用基本要求》（GB/T 39786）的密码技术进行加密传输，密码技术、服务等应满足密码相关标准规范和要求。

4.14 乙方应提供数据销毁机制，对超过约定期限后对接收的重要数据、个人信息及时销毁。

4.15 乙方在中国境内存储境内收集和产生的重要数据、个人信息，存储的数据中心、云平台等不得位于境外。甲方保留核实所有数据实际存储地点的权利，要求提供云服务使用证明或签署存储位置确认函，确保存储数据所在的物理服务器或数据中心位于中华人民共和国境内。

4.16 乙方应制定数据备份与恢复计划，明确备份与恢复的范围、频率、工具、过程、日志记录规范、数据存储期限等。

4.17 乙方应按照数据分类分级要求对数据采取不同的加密技术，如涉及重要数据、个人信息，应采用符合《中华人民共和国密码法》和《信息安全技术 信息系统密码应用基本要求》（GB/T 39786）的密码技术进行加密存储。

4.18 乙方应根据制定的策略自动化执行备份与恢复相关活动，并记录数据备份与恢复过程。

4.19 乙方应按照数据分类分级要求明确相关人员的访问权限，防止未授权访问。

4.20 乙方应对数据处理建立数据泄露控制规范和机制，防止数据处理过程中的调试信息、日志记录、不受控制输出等泄露受保护的重要数据、个人信息等敏感信息。

4.21 乙方应妥善留存和甲方相关的重要数据、个人信息处理活动记录日志，一般日志留存期限不少于六个月，涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于一年。涉及向他人提供、委托处理、共同处理重要数据和个人信息的，相关日志留存时间不少于三年。

4.22 乙方应对和甲方相关的重要数据、个人信息的关键操作（如批量修改、拷贝、删除、下载等）设置审批流程和记录日志，以满足访问控制与审计的需求。

4.23 乙方应通知甲方关于乙方委托第三方开展数据处理活动的范围、目的、期限、处理方式、数据的种类、保护措施、双方的权利和义务以及第三方返还或者删除数据的方式等。

4.24 乙方在委托第三方开展与甲方相关的数据的处理活动时，应经过甲方同意并对数据处理活动进行监督；乙方应通过合同等形式明确约定委托处理的目的、期限、处理方式、数据的种类、保护措施、双方的权利和义务以及第三方返还或者删除数据的方式等，要求第三方以合同中约定的形式返还、删除接收和产生的数据。

4.25 乙方在委托第三方开展数据处理活动时，应经过甲方同意并对数据处理活动进行监督；原则上乙方应使用去标识化处理的数据集，重要数据、个人信息原则上应脱敏后进行数据处理。匿名化或者去标识化处理的数据，非业务所必须，禁止把相关处理技术措施告知其他部门或者企业，防止被重标识，匿名化或者去标识化的数据汇聚融合后，进行集成和分析。

4.26 乙方应采用数据脱敏、数据水印等数据保护技术，控制数据的使用目的、范围和效果，降低数据泄露风险。

4.27 乙方应对数据加工过程的数据操作行为记录日志，支持安全审计。

4.28 乙方向第三方提供个人信息时，应向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，并取得个人信息主体的单独同意。

4.29 乙方向境外提供重要数据、个人信息时，应遵循国家相关规定和相关标准的要求。

4.30 乙方向第三方提供重要数据、个人信息时，应向数据接收方通过合同等形式，明确双方的数据安全保护责任和义务。

4.31 乙方向第三方提供重要数据、个人信息时，应记录日志，支持安全审计。

4.32 乙方应对拟披露数据的合规性、业务需求、数据脱敏方案、审批流程进行审核。

4.33 乙方应对数据公开披露审批过程和记录留档保存，支持安全审计。

4.34 乙方应及时对具有以下情形的个人信息作删除或者匿名化处理：

a）个人信息超出双方约定的存储期限；

b）网络产品和服务停止运营；

c）个人信息主体注销账号，或者当用户撤回同意。

4.35 乙方应采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不可恢复。

4.36 乙方应对数据删除过程记录日志，记录数据删除的审批、实施过程，以及被删除数据的具体情况，日志的留存期限不少于 6 个月。

4.37 乙方应制定重要数据、个人信息的安全事件应急预案，包括应急组织机构与职责、数据安全事件分类分级、监测与预警、应急处置流程、保障措施等事项。

4.38 乙方应积极配合甲方，协助甲方应对监管机构检查、个人信息主体的权利请求以及个人信息主体或者第三方的投诉。

4.39 乙方未经甲方同意，不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析。

4.40 乙方应在网络边界采用防火墙、入侵检测等安全技术或者设备，以保障数据传输网络的安全性。

4.41 乙方应根据数据分类分级对将数据分域分级存储，如涉及重要数据、个人信息的应在公共信息网络与存储系统之间提供逻辑隔离措施。

4.42 乙方应采用技术工具和措施管理存储介质，追踪介质的使用和传递过程，对介质的访问、使用和销毁等全过程行为进行记录和审计，并定期对介质销毁记录及销毁效果进行检查。

4.43 乙方在重要数据、个人信息的存储介质进行报废处理时，应采用物理损毁等方式销毁介质，以确保重要数据、个人信息不能被恢复。

4.44 乙方应提供数据删除技术措施和工具，对批准后的重要数据及其副本进行删除，包括数据处理过程中备份数据、衍生数据及操作日志数据等，确保删除后的数据以商业手段不可恢复。

4.45 乙方应通过权威的供应链安全机构的专项软件检测认证。

4.46 乙方应当按照《数据安全技术 数据安全风险评估方法》（GB/T 45577—2025）定期对数据处理活动进行数据安全风险评估，并向甲方提交风险评估总结报告。

（五）SaaS（不存储数据）服务场景

5.1 乙方在处理与甲方相关的重要数据、个人信息时，应不超出约定的目的、范围、方式。

5.2 乙方应提供不低于甲方的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面。

5.3 乙方应要求与甲方相关的重要数据、个人信息接收方提供不低于乙方的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面。

5.4 乙方应根据数据分类分级对数据传输采取对应的安全管控措施，如签名验签、双向认证、传输通道加密、数据内容加密等。

5.5 乙方在数据传输过程中，涉及与甲方相关的重要数据、个人信息或者关键信息基础设施的，应采用符合《中华人民共和国密码法》和《信息安全技术 信息系统密码应用基本要求》（GB/T 39786）的密码技术进行加密传输，密码技术、服务等应满足密码相关标准规范和要求。

5.6 乙方在数据传输完成后，应立即清除传输历史缓存数据。

5.7 乙方不得委托第三方开展重要数据、个人信息处理，不得将重要数据、

个人信息存储、披露和提供给第三方。

5.8 乙方应采用数据脱敏、数据水印等数据保护技术，控制数据的使用目的、范围和效果，降低数据泄露风险。

5.9 乙方对数据加工过程的数据操作行为记录日志，支持安全审计。

5.10 乙方应积极配合甲方，协助甲方应对监管机构检查、个人信息主体的权利请求以及个人信息主体或者第三方的投诉。

5.11 乙方应通过权威的供应链安全检测机构的检测认证。

5.12 乙方应当按照《数据安全技术 数据安全风险评估方法》（GB/T 45577—2025）定期对数据处理活动进行数据安全风险评估，并向甲方提交风险评估总结报告。

（六）PaaS 服务场景

6.1 乙方应采用技术工具和措施管理存储介质，追踪介质的使用和传递过程，对介质的访问、使用和销毁等全过程行为进行记录和审计，并定期对介质销毁记录及销毁效果进行检查。

6.2 乙方在重要数据、个人信息的存储介质进行报废处理时，应采用物理损毁等方式销毁介质，以确保重要数据、个人信息不能被恢复。

6.3 乙方应积极配合甲方，协助甲方应对监管机构检查、个人信息主体的权利请求以及个人信息主体或者第三方的投诉。

6.4 乙方未经甲方同意，不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析。

（七）其他

7.1 乙方应按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《网络数据安全管理条例》《关键信息基础设施安全保护条例》《商用密码管理条例》等法律法规及规章制度的要求，履行网络和数据安全保护义务。

二、系统集成

（一）基本安全要求

1.1 乙方应针对本项目设置安全负责人岗位，全面负责和管理本项目的网络安全相关工作。

1.2 乙方应严格审核二级供应商安全资质，建立动态风险评估及替代方案，对二级供应商导致的安全风险承担连带责任。

1.3 集成系统设计、实施至废止的全流程，须嵌入安全管控节点，设计方案要遵守适用的法律法规和行业标准，系统上线前须完成安全检测，废止时确保数据不可恢复。

1.4 乙方应与甲方签订保密协议，明确系统集成过程中接触的敏感信息的保密责任。

1.5 乙方应对参与项目的服务人员进行安全保密教育，因乙方人员违规泄露信息导致的法律责任由乙方承担。

1.6 乙方应配合甲方对其开展远程检测和现场检查。

（二）集成设计

2.1 乙方应确保集成系统的设计方案符合甲方的总体业务目标和项目目标。

2.2 乙方应在集成设计阶段进行安全风险评估工作，对集成系统中可能出现的安全威胁和漏洞进行评估，并向甲方提供评估材料。

2.3 乙方应确保集成设计方案在整个软件生命周期内都遵守适用的法律法规和行业标准。

2.4 乙方在设计过程中应考虑集成系统各单元模块的权限安全，确保每个模块只被授予满足其基本功能需求的最小权限。

2.5 乙方在设计过程中应考虑用户权限，合理限定每个应用和用户的权限范围和有效时间。

2.6 乙方在设计中应对集成系统的敏感数据加密传输和存储。

2.7 乙方应要求二级供应商在开发交付产品时明确说明并提供所有必要的接口和功能，包括但不限于 API 文档、数据格式、调用方式等。

2.8 乙方应设计接口访问控制规则，确保经过身份认证和权限认证的用户才能访问相应的接口。

2.9 乙方在设计过程中应考虑为集成系统配备威胁防护措施，以防止恶意软件和其他侵入威胁。

2.10 乙方设计中存在密钥相关功能的，应有完整的密钥管理模块，该模块包括密钥的生成、存储、分发、更新、吊销等环节。

2.11 乙方在设计过程中应考虑系统参数和配置信息的监控审计机制，及时发现并应对异常行为。

2.12 乙方在设计中应考虑日志和安全事件管理机制，收集系统和网络设备的日志并建立快速响应机制应对威胁。

2.13 乙方在设计中应考虑软件废止的相关管理机制，包括但不限于数据备份迁移策略和数据清理方法等。

2.14 乙方应编制详细的安全需求文档，明确列出集成建设的核心安全目标和参与集成建设的二级供应商必须具备的安全能力和资质。

（三）集成实施

3.1 乙方应制定详尽的故障恢复和灾难恢复计划，包括数据备份策略、备用系统配置等，并定期进行测试演练，确保能够及时响应突发事件。

3.2 乙方应定期对集成系统进行安全补丁更新和系统升级。

3.3 乙方应在实施阶段定期使用相关安全工具对集成系统进行安全漏洞扫描并记录存在的安全漏洞。

3.4 乙方应对实施阶段发现的漏洞和安全隐患制定修复计划，征得甲方同意后，按照计划进行修复。

3.5 乙方应充分熟悉集成系统中所使用的组件或者产品的知识产权，对知识产权进行规范管理，防止侵权。

3.6 乙方应及时提供交付环节变化的通报，以及相关的交付途径安全性分析报告，并对可能造成严重后果的变化快速采取补救措施。

3.7 乙方应在甲乙双方约定的质保期或者过渡期内对实施过程中引入的安全漏洞进行修复。

3.8 乙方应明确集成系统安全交付条件为满足法律法规、标准规范和甲方需求，禁止开启无关功能、捆绑无关软件等交付约定范围外的内容。

3.9 乙方应制定详细的部署计划和流程，包括但不限于完善的回滚机制和必

要的初始化机制，并定期进行部署演练。

3.10 乙方在部署完成后应协助甲方对集成系统的功能和稳定性进行测试和监控。

3.11 在集成系统上线前，乙方应使用安全检测工具进行扫描检测，确保所有高危及以上的漏洞和安全隐患均已被有效修复，并向甲方提供漏洞修复后的检测报告。

3.12 乙方应在部署新系统或者进行系统更新前为甲方提供必要的安全培训和演练。

3.13 涉及软件废止环节的，乙方应负责开展软件卸载、停用及数据备份、迁移以及销毁工作。

（四）集成管理

4.1 乙方应定期同步集成建设过程中的信息，包括需求变更、实施进度、风险评估和后续计划等。

4.2 乙方应建立文档版本管理制度，整理所有集成项目相关的文档资料和记录系统历次的更新操作，保证所有操作可溯源。

4.3 乙方应确保集成管理中有完善的变更流程，并建立变更的申报和审批控制程序。经甲方同意后，确保服务变更以受控的方式得到评估、批准和实施。

4.4 乙方应定期更新集成系统的应急响应计划，并建立安全监控机制，对安全事件进行实时监测和响应，包括安全漏洞和即将到期或者超过授权、维保期限的软件或者组件。

4.5 在发生突发事件时，乙方应在双方约定的时间范围内恢复服务。

4.6 乙方应明确运维人员的访问权限级别，对其访问范围和授权期限进行严格控制。

4.7 乙方应建立并执行离职离岗人员的制度，包括账号、权限、材料等交接、清理。

4.8 乙方应确保与其合作的所有分包商都承担相应的安全义务，并对分包商可能带来的安全风险承担连带责任。

4.9 乙方应对集成系统内的所有子系统和应用进行核查，确保二级供应商所采用的安全政策和程序符合集成系统的安全策略。

4.10 乙方应保证建设的集成系统通过权威的供应链安全检测机构的检测认证。

4.11 乙方应识别和评估与二级供应商相关的所有潜在风险，并针对供应链安全风险较高或者未整改风险的供应商采取额外的监控和审查措施。

4.12 发现乙方提供的产品或者服务存在安全漏洞的情况时，乙方应及时组织技术团队对安全漏洞进行修补，并在确认修补方案后，向甲方提供修补计划。乙方还应提供必要的技术支持，包括但不限于远程协助和现场服务等，确保甲方系统能够尽快恢复正常运行，且漏洞得到妥善解决。

4.13 乙方应定期对安全测试工具进行评估和更新，确保能够有效地识别到最新的安全威胁和漏洞。

4.14 在乙方无法履行其责任义务或者由于其他不可抗力无法继续履行责任义务的情况下，甲方有权直接与二级供应商沟通，在本项目中行使乙方与二级供应商约定的权利。

4.15 乙方应对集成建设系统进行周期性安全评估，确保符合现行法律、法规和行业标准，并记录合规性要求。

4.16 乙方应建立持续的风险监测机制，定期审查和评估集成系统的风险状态和现有风险处置应对措施的有效性。

4.17 乙方应定期评估二级供应商的安全事件应对能力和供应产品的安全性，确保供应产品符合安全政策。

4.18 乙方应定期审查和更新集成系统的安全架构，评估现有安全架构的健壮性，并采取必要的改进措施。

4.19 乙方应定期审查所需硬件在仓储和物流过程中安全措施的有效性，并根据需要进行调整。

第十一条 附 则

（一）本协议未尽事宜，由双方协商提出书面补充或修改意见，其补充和修改意见及所有协议附件是本协议的有效组成部分，与本协议有同等法律效力。

（二）本协议有效期：自协议签署日起伍年。

（三）本协议一式肆份，甲、乙方各执贰份，由各方负责人或授权签字人签字并加盖双方公章之日起生效。

【签署页】

甲 方	乙 方
（盖章）	（盖章）
负责人/授权签字人：	负责人/授权签字人：
日期：2026 年 1 月 6 日	日期：2026 年 1 月 13 日