项目采购编号：JSZC-320400-JZCG-G2026-0347

2026年常州市电子政务网安全保障服务项目合同书

甲　　方：常州市大数据管理中心（常州市电子政务中心）

乙　　方：江苏瑞新信息技术股份有限公司

签订时间：　2026年11月

项目名称：2026 年常州市电子政务网安全保障服务项目

项目编号：JSZC-320400-JZCG-G2026-0347

甲方：（买方）常州市大数据管理中心（常州市电子政务中心）

乙方：（卖方）江苏瑞新信息技术股份有限公司

甲、乙双方根据常州市政府采购中心 2026 年常州市电子政务网安全保障服务项目公开招标的结果，签署本合同。

一、合同内容

1.1 标的名称：2026 年常州市电子政务网安全保障服务项目

1.2 标的质量：按照甲方需求

1.3 标的数量（规模）：按照甲方需求

1.4 履行时间（期限）：合同生效之日起一年

1.5 履行地点：常州市大数据管理中心

1.6 履行方式：现场实施

二、合同金额

2.1 本合同金额为（大写）：贰佰零肆万陆仟元整（¥：2046000 元）人民币。其中不含税金额 1930188.68 元，税率 6%，增值税税额 115811.32 元。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的货物）的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知

识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

本项目不收取履约保证金。

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

八、合同款项支付

8.1 分期付款：合同签订后，自收到发票后 10 个工作日内，甲方向乙方支付合同总额的 50%作为预付款，即人民币：壹佰零贰万叁仟元整（¥：1023000.00 元）；项目服务期满后，验收通过后，在收到发票后 10 个工作日内，甲方向乙方支付合同尾款，即人民币：壹佰零贰万叁仟元整（¥：1023000.00 元）。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方依据招标文件要求和投标文件承诺，制定验收标准，依法组织履约验收工作。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供服务的，甲方向乙方偿付拒绝接受服务合同价款总值 5%的违约金。

11.2 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额 5‰ 每日向乙方支付违约金，但违约金总额不超过逾期付款总额的 5%。

11.3 乙方逾期提供服务或无故中止服务的，乙方应按逾期提供服务合同总额每日6‰向甲方支付违约金，由甲方从待付合同款项中扣除。超过约定日期10个工作日不能提供服务的，甲方可解除本合同。乙方因逾期提供服务或无故中止服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同价款总额5% 的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

11.4 乙方所提供服务的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

十二、不可抗力事件处理

12.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响 期相同。

12.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

12.3 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

十三、解决争议的方法

13.1双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。守约方在争议解决过程中发生的费用（包括但不限于诉讼费、公证费、律师费、鉴定费、差旅费、保全费、担保费等），应由违约方承担。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

14.2本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

14.3 本合同正本一式两份，具有同等法律效力，甲方、乙方各执一份。

（此页无正文）

甲方：常州市大数据管理中心

地址：常州市锦绣路2号

法定代表人或授权代表：

经办人：韩波

联系电话：0519-85685035

乙方：江苏瑞新信息技术股份有限公司

地址：常州市新北区太湖东路9-2号3楼

法定代表人或授权代表：杨粉

经办人：蒋春燕

联系电话：0519-81236533 15851967128

签订日期：2026 年 11 月 18 日

附件 1:《保密协议》

保 密 协 议

甲方：常州市大数据管理中心（常州市电子政务中心）

乙方：江苏瑞新信息技术股份有限公司

为加强“2026 年常州市电子政务网安全保障服务项目”相关系统数据的安全保密管理，贯彻落实《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》、《中华人民共和国网络安全法》《中华人民共和国密码法》等有关法律法规，确保数据的安全保密，促进数据合法、有效利用，防止发生失泄密事件，防范非法使用行为，本着平等、自愿、协商一致、诚实信用的原则，就乙方为甲方提供软件修改完善、数据处理和技术支持服务（下称项目）等工作中的保密事宜达成如下协议。

一、 保密信息

（一）在项目中所涉及的项目设计、图片、开发工具、流程图、工程设计图、计算机程序、数据、专利技术、招标文件等内容（在项目中向社会公众提供信息公开和服务的图片、网页、信息数据不包含在内）；

（二）甲方在项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

（三）甲方在项目实施中涉及的业务及技术文档，包括方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据等；

（四）其他甲方合理认为，并告之乙方属于保密的内容。

二、保密范围

（一）甲方已有的技术秘密；

（二）甲方敏感信息和知识产权信息；

（三）乙方持有的科研成果和技术秘密，经双方协商，乙方同意被甲方使用的。

三、保密条款

（一）乙方明确所接收的文件（包括电子和纸质）为甲方所有，甲方拥有以上文件的知识产权。乙方承认甲方在本协议规定的保密信息上的利益和一切有关的权利，乙方应当考虑甲方的利益对该信息予以妥善保存，防止有意或无意的泄漏；

（二）乙方应采取尽可能的措施对所有来自甲方的信息严格保密，包括执行有效的安全措施和操作规程；

（三）甲方为基础数据的管理和提供方，甲方拥有所有数据的全部所有权，乙方需在甲方的授权下使用数据。乙方承诺对甲方以书面、口头、电子文本、电子数据等方式提供的保密信息承担保密义务；

（四）乙方同意仅在为实施本项目时使用保密信息，绝不为与该项目无关的目的使用保密信息；

（五）未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息和其中的任何部分，披露或透露给任何第三方（仅可向有知悉必要的乙方内部人员披露，同时仅为甲方项目所需使用）。乙方有义务妥善保管上述文件和数据，不得复制、泄漏或遗失。乙方亦不得依据甲方提供的任何保密信息，就任何问题，向任何第三方作出任何建议；

（六）若乙方确有需要向第三方展示甲方数据信息及成果，需提前向甲方以一事一议的形式提交书面申请，由甲方签字盖章同意后方可施行。未经同意，严禁乙方将甲方数据向第三方展示。如有违反，乙方须承担全部后果，甲方有权向乙方追责；

（七）项目维护过程中，如因业务需要，乙方需采购第三方软件或软件服务的。乙方需以数据最小化为原则，明确数据范围及用途，并与第三方签订数据安全保密协议，确保甲方数据安全；

（八）乙方需加强自身保密意识及保密措施，从管理及技术方面保障甲方数据安全，与员工签订保密协议，约束监督员工，防止个别员工将甲方数据泄露；

（九）乙方的职员违背上述承诺，向第三方披露保密信息，或依据该等保密

信息向第三方作出任何建议，都将被视为乙方违反本协议；

（十）甲方保留在甲方认为必要的情况下收回所提供的文件、数据及其使用权的权利；

四、保密信息的所有权

以上所提及的保密信息均为甲方所有。

五、保密期限

（一）本协议的保密期限为 5 年；

（二）在本协议失效后，如果本协议中包括的某些保密信息并未失去保密性的，本协议仍对这些未失去保密性的信息发生效力，约束双方的行为；

（三）本协议是为防止甲方的保密信息在协议有效期发生泄漏而制定。因任何理由而导致甲、乙双方的合作项目终止时，乙方应归还甲方所有有关信息资料和文件，但并不免除乙方的保密义务。

六、关系限制

本协议不作为双方建立任何合作关系或其他业务关系的依据。

七、违约责任

乙方未遵守本协议的约定泄露或使用了保密信息甲方有权终止双方的合作项目，乙方应按合作项目金额作为违约金支付甲方，并按照有管辖权的人民法院认定的赔偿金额赔偿甲方遭到的其他损失，甲方有权进一步追究其一切相关法律责任。

八、其他事项

（一）本协议未尽事宜，由甲乙双方协商解决；

（二）本协议自甲、乙双方盖章之日起生效。

甲方：（章）常州市大数据管理中心（常州市电子政务中心）

乙方：（章）江苏瑞新信息技术股份有限公司

附件 2：《安全服务项目内容》

一、管理咨询服务

服务内容：针对电子政务网，为采购方提供涵盖网络安全规划、应急响应预案、网络安全和数据安全培训等方面的专业分析、方案制定及实施指导，以保障其网络安全。同时积极配合采购方深化与第三方供应链的网络安全技术交流，畅通沟通渠道，协同筑牢供应链安全防线。

服务频率：根据甲方要求。

服务成果：提供网络安全规划、应急响应预案、网络安全和数据安全培训等方面的专业分析报告和方案，建立与第三方供应链的网络安全技术交流机制和成果记录。

二、安全检测服务

政务信息化项目管理平台检测任务

服务内容：针对政务信息化项目管理平台中服务器开通、访问控制开通或调整、互联网权限开通等工作任务，需第一时间开展安全扫描与检测，全程跟踪问题修复进度，确保各项安全隐患得到彻底整改，形成闭环管理。

服务频率：实时动态。

服务成果：输出安全扫描检测报告，记录问题及整改情况，形成闭环管理文档。

互联网系统渗透测试

服务内容：针对 1228 个互联网系统，选取部分重要单位重要系统的互联网系统采用远程和现场方式进行一年四次的全面安全检测，一旦发现安全风险立即精准通报，并全程跟踪问题修复进度，确保隐患彻底整改到位。其他部分单位的互联网系统进行一年二次的周期检测，全程跟踪问题修复进度，确保隐患彻底整改到位。

服务频率：重点系统每季度一次，普通系统每半年一次。

服务成果：出具详细的渗透测试报告，包括风险详情、整改建议，跟踪记录整改结果。

电子政务网系统渗透测试服务

服务内容：针对重点系统的电子政务网系统，开展全面安全检测，一旦发现

安全风险立即精准通报，并全程跟踪问题修复进度，确保隐患彻底整改到位。电子政务网普通系统也按相应周期检测。

服务频率：重点系统每半年一次，普通系统每年一次。

服务成果：出具详细的渗透测试报告，包括风险详情、整改建议，跟踪记录整改结果。

风险评估服务

服务内容：针对采购方计划外新建项目，配合完成系统上线的安全检测评估服务，并全程跟踪问题修复进度，确保隐患彻底整改到位。

服务频率：动态。

服务成果：提供采购方计划外项目上线安全检测报告和整改跟踪记录。

增量系统安全检测

服务内容：完成年度新迁移到电子政务网上的新增系统的安全检测，并后期根据系统重要性进行周期性的安全检测。

政府网站群安全监测服务

服务内容：持续稳定地对 89 个常州市政府门户网站群及相关系统开展 7*24 小时实时监测服务，每月按时按要求提供月度监测报告和事件漏洞预警处置报告。

具体要求：

1、网站内容安全监测

采用中文关键词以及语义分析技术对网站进行敏感关键字监测，实现精确的敏感字识别，确保网站内容符合互联网相关规定，避免出现敏感信息及不良信息。

2、疑似篡改监测

监控网站首页、二级栏目以及其他重点栏目内容判断是否被黑客篡改。

3、挂马监测

采用特征分析和沙箱行为等分析技术对网站进行木马监测，从而实现快速、准确的发现和定位网页木马。

4、暗链、黑链监测

监测平台采用暗链、黑链数据库对比分析、暗链特征提取等技术，及时发现网站中被植入的暗链和黑链，及时通告并预警。

5、漏洞安全检测

采用多种扫描工具交叉扫描，避免单一扫描器缺陷。发现容易被黑客利用攻击的脆弱点和漏洞，发现网站系统中存在的安全漏洞和安全隐患，人工进行验证并确认危害程度。

6、系统安全漏洞检测

采用多种系统漏洞检测工具，重点检测操作系统、数据库、WEB 服务器软件、中间件、第三方插件的安全隐患和漏洞，人工进行验证并确认危害程度。

服务频率：7*24 小时实时监测

服务成果：常州市政府门户网站群安全检测报告（月度）、信息安全检测服务工作总结和分析报告（月度）、全年信息安全检测服务工作总结和分析报告（年度）、重大节日/活动期间安全值守总结报告、信息安全事件应急处理报告、新上线网站安全检测报告（按需）

数据安全评估合规评估服务

针对常州市公共数据平台、常州市公共数据授权运营平台、常州城市可信数据空间平台开展一次数据安全风险评估与合规评估，并进行业务数据流向梳理、数据目录梳理、数据合规管理评估、安全技术评估等工作，为公共数据安全合规流通与开发利用提供有力支撑。评估应坚持依法合规、最小必要、原始数据不出域、数据可用不可见、全程可控、可追溯等原则，形成"摸清家底—识别风险—评估合规—提出整改—支撑流通"的闭环。

1、评估对象与范围

评估对象包括常州市公共数据平台、常州市公共数据授权运营平台、常州城市可信数据空间平台及其支撑系统、接口、连接器、沙箱、隐私计算组件、数据产品、运维服务链路等。评估范围覆盖数据归集、治理、存储、共享、开放、授权运营、可信流通、销毁/退出等全生命周期，涉及公共数据、授权运营数据、数据产品、个人信息、重要数据、核心数据、匿名化/去标识化数据等。

评估依据主要包括：《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《江苏省公共数据授权运营管理暂行办法》《江苏省数据条例》《公共数据资源授权运营实施规范（试行）》等法律法规和政策文件；

GB/T 45577-2025《数据安全技术 数据安全风险评估方法》、GB/T 43697-2024《数据安全技术 数据分类分级规则》、GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等标准；以及《常州市公共数据分类分级规范》、省公共数据授权运营平台和省数据交易所相关对接规范。具体以现行有效版本为准。

2、服务内容

2.1 业务数据流向梳理

（1）数据资产盘点

对常州市公共数据平台、常州市公共数据授权运营平台、常州城市可信数据空间平台开展全方位数据资产盘点，理清数据来源、处理环节、流向及使用情况。参照常州市公共数据分类分级规范，按资源属性、共享开放属性、主题、行业等多维度进行分类梳理。识别核心数据、重要数据、一般数据，并单独识别个人信息、敏感个人信息、匿名化/去标识化数据。绘制数据资产全景图，形成数据资产清单、数据血缘关系和责任清单。

（2）数据流转链路绘制

梳理数据从归集、治理、存储、共享、开放到授权运营、可信流通、销毁/退出的全生命周期流转路径。绘制涵盖数据全生命周期的流转图谱，明确数据来源、流转方向、流转节点、承载系统、接口、责任主体及控制措施。重点覆盖：公共数据平台向授权运营平台的数据供给链路、授权运营平台向开发主体的数据加工链路、可信数据空间的多方主体数据交互链路、各平台与省级平台及省数据交易所的数据对接链路，以及第三方运维、服务商等外部参与链路。

（3）数据流转风险识别

识别数据流转过程中的安全风险点，包括但不限于数据传输安全、接口调用安全、跨域流转管控、权限边界清晰度、日志审计完整性、脱敏加密措施、批量导出、汇聚关联、二次加工、再识别、跨境流动等风险。评估"原始数据不出域、

数据可用不可见"原则的落实情况。对城市可信数据空间平台，应重点关注匿名化/去标识化数据在多方交互、连接器传输、沙箱计算和数据产品输出过程中的风险。输出《数据流转风险识别清单》，作为整体数据安全风险评估的输入，避免与整体风险评估结论混淆。

2.2 数据目录梳理

（1）公共数据资源目录梳理

对三个平台的数据资源目录进行系统梳理，核查目录的完整性、准确性、时效性和元数据规范性。对照《常州市公共数据分类分级规范》要求，核查数据分类分级标识的规范性。评估数据目录与省公共数据授权运营平台、省数据交易所的对接情况，包括目录同步、接口兼容、更新机制和权限映射等。

（2）数据产品目录梳理

梳理授权运营平台上架的公共数据产品，包括数据接口、数据模型、数据报告、数据服务等类型。核查数据产品与所使用公共数据资源的对应关系，评估数据产品中是否涉及原始数据直接输出、是否包含个人信息或敏感数据、是否涉及匿名化/去标识化数据。核查数据产品出域前的安全审查、登记、溯源和下架退出机制。

（3）目录管理机制评估

评估数据目录的更新机制、审核流程、质量管理措施。核查数据目录是否实行统一管理，是否推动实现"一数一源"，数据更新频率及质量情况是否满足应用需求。补充评估目录版本管理、数据血缘关联、责任主体明确性，以及目录与数据产品、授权运营活动之间的关联管理情况。

2.3 数据合规管理评估

（1）法律法规符合性评估

对照《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《江苏省公共数据授权运营管理暂行办法》及相关配套文件，逐项评估三个平台的合规现状，形成合规义务清单和符合性矩阵。

（2）授权运营合规评估

评估授权运营活动中各方主体责任的落实情况，包括运营主体的安全管理制度建立情况、开发主体的准入条件审核、授权协议的签订与执行、合规监测机制的运行情况。核查运营主体是否定期向数据主管部门报告授权运营整体情况。补充评估数据产品上架审核、授权范围控制、收益分配合规性、退出机制及违规处置机制。

（3）个人信息保护合规评估

如平台涉及个人信息处理，参照《个人信息保护合规审计管理办法》要求，评估个人信息处理活动的合法性基础、告知同意机制、个人信息主体权利保障等。重点关注处理超过 1000 万人个人信息时的合规义务履行情况，包括个人信息保护影响评估、合规审计、负责人指定、社会责任报告等义务。对匿名化数据，应核查其是否真正达到"无法识别特定自然人且不能复原"的标准；如可结合其他数据重标识，仍应纳入个人信息保护合规管理。

（4）管理制度与流程评估

评估数据安全组织架构、岗位职责、人员管理、制度流程的健全性和执行有效性。核查是否建立数据分类分级管理、访问控制、安全审计、应急响应等制度，制度是否覆盖数据全生命周期。补充评估第三方合作管理、保密协议、人员离岗离职管理、培训考核、问责追责等机制。

2.4 安全技术评估

（1）技术防护措施评估

参照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》，评估现有数据安全技术能力。重点评估：数据分类分级技术手段、数据访问控制机制、数据风险监测能力、数据防泄漏措施、数据加解密技术、数据脱敏技术等。补充评估隐私计算、可信执行环境、联邦学习、多方安全计算、数据水印、数据溯源、密钥管理等技术措施的有效性。

（2）平台安全评估

对三个平台开展安全评估，包括身份认证与权限管理、接口安全、数据存储安全、数据传输安全、日志审计、安全监控等。重点关注授权运营平台与可信数据空间平台的安全隔离措施、连接器安全机制、沙箱环境安全性。补充评估等级保护合规情况、密码应用、供应链安全、容器与微服务安全、API 网关安全、零信任访问控制等。

（3）数据安全场景化评估

结合平台业务特点，针对数据归集、共享交换、授权运营、可信流通等典型场景，开展场景化风险评估。重点评估"原始数据不出域"的技术保障措施有效性、数据产品出域前的安全审查机制、多方主体数据交互的信任管控机制。补充评估沙箱逃逸、模型反演、成员推断、属性推断、梯度泄露等新型风险。

（4）匿名化与去标识化有效性评估

针对常州城市可信数据空间平台中涉及匿名化处理的数据，开展匿名化手段有效性评估。梳理匿名化/去标识化数据对象、处理场景、算法参数、输出物及发布控制措施，评估其是否达到无法识别特定自然人且不能复原的要求。重点测试重标识风险、关联攻击、差分攻击、模型反演、成员推断等风险。明确区分匿名化与去标识化：去标识化数据仍可能属于个人信息；匿名化处理后如可复原或可重识别，应按个人信息保护要求管理。核查匿名化数据在连接器、沙箱、接口、数据产品出域等环节的策略配置、审计记录和水印溯源能力。

2.5 服务输出

《数据安全风险评估报告》《业务数据流向图谱》《数据资产目录架构》《数据合规管理评估报告》《安全技术评估报告》《整改建议方案》

三、安全保障服务

省、市网络安全监管平台管理及配合服务

服务内容：密切关注省、市两级网络安全监管平台动态，确保第一时间接收相关通报信息，迅速开展处置工作并及时反馈处置结果，保障每一份通报都能得到高效、规范的闭环处置。积极配合甲方完成其他检测人员的网络接入配置、权限审核等工作，确保接入流程合规、权限分配精准，为检测工作高效开展提供支

撑。

服务频率：动态。

服务成果：建立通报处置记录文档，反馈处置结果报告，完成的网络接入配置和权限审核记录。

流量分析服务

服务内容：依托中心 SOC 平台，对安全风险告警信息进行深度分析，一旦发现安全风险隐患，立即启动处置流程并全程跟踪处置进展，确保风险闭环清零。

服务频率：每日。

服务成果：记录每日安全风险告警，风险处置过程和结果。

重要时期保障服务

服务内容：在重大会议、节假日、网安专项行动等特殊时期内，安排安全攻防经验丰富的安全专家，对业务系统进行重保前专项安全检查、现场值守与发生异常情况的应急响应。

服务频率：根据甲方要求。

服务成果：提供重保前专项安全检查报告、现场值守记录和应急响应处理报告。

应急响应服务

服务内容：提供 5×8 小时的现场应急响应和 7×24 小时的远程安全应急响应，接到安全事件通知后，立即对安全事件进行分析、抑制、溯源，最大程度降低安全事件对客户带来的损失。

服务频率：发生安全事件时。

服务成果：出具安全事件分析报告、抑制措施报告和溯源报告。

报告分析服务

服务内容：针对安全扫描、渗透测试、设备安全态势、标段二两家中标方发现的风险隐患等成果输出详尽的运营服务分析报告供领导决策参考，通过分析报告帮助单位持续优化网络安全防护体系。

服务频率：每月一次。

服务成果：每月提交运营服务分析报告，提出网络安全防护体系优化建议。

驻场服务

服务内容：提供专业的驻场安全保障服务，组建不少于 6 人的保障团队，成员需具备丰富的网络安全相关经验和专业技能，涵盖网络安全工程师、安全分析师、应急响应专家等不同专业角色。驻场团队负责日常电子政务网的安全巡检、监控工作，及时发现并处理潜在的安全隐患；协助配合其他各类安全服务的开展，如安全检测时提供现场支持、应急响应时迅速采取行动等；与电子政务中心的工作人员保持密切沟通，及时了解业务需求和安全状况变化，为网络安全保障工作提供有力的现场支持。

服务频率：实行 5×8 小时现场驻场服务，在工作日的正常工作时间内确保团队成员在岗，随时响应各类安全相关事务。同时，安排专人负责 7×24 小时应急联络，确保在非工作时间也能对紧急安全事件做出及时响应。

服务成果：每周出具一份驻场工作周报，总结本周的安全工作情况、安全态势分析以及下周的工作计划；定期与甲方进行沟通反馈，根据实际情况提出网络安全优化建议。