

智慧建邺网络信息系统安全运维服务合同（服务）

智慧建邺网络信息系统安全运维服务合同（服务）

项目名称：智慧建邺网络信息系统安全运维服务项目

项目编号：JSZC-320105-SJGC-C2025-0013

甲方：（采购人）南京市建邺区城市数字治理中心

乙方：（供应商）南京大数据安全技术有限公司

甲、乙双方根据江苏苏建工程项目管理咨询有限公司智慧建邺网络信息系统安全运维服务项目竞争性磋商的结果，签署本合同。

一、合同内容

1.1 标的名称：智慧建邺网络信息系统安全运维服务项目

1.2 标的数量（规模）：

服务类别	服务名称	服务内容	服务频次	单位	数量
识别	基线核查	安全基线核查：制定系统安全配置基线规范，根据基线规范采用自动工具检查加人工审核的方式，对系统进行基线核查，检出信息系统与相关IT设备配置的不合规部分。配置审查：对信息系统进行专家人工安全审核，发现信息系统配置中存在的安全弱点。其中技术手段采用EDR方案，EDR终端支持部署安装在信创主机环境。	每月1次	套	1
	安全威胁分析技术服务能力（互联网区）	政务外网互联网区出口节点各旁路部署态势感知设备，对现网流量进行实时安全分析	实时	套	1
	安全威胁分析技术服务能力（公共区）	政务外网互公共区出口节点各旁路部署态势感知设备，对现网流量进行实时安全分析	实时	套	1
保护	服务器主机防病毒	采用主机安全（EDR）方案对服务器主机进行防病毒。每月应组织专项行动，对全量资产进行病毒、木马查杀、清理。EDR终端支持部署安装在信创主机环境。	实时检测与查杀	套	1

服务类别	服务名称	服务内容	服务频次	单位	数量
	云WAF安全防护	南京市建邺区新一代电子政务外网Web服务尽最大可能纳入云WAF安全防护,在远程云端对攻击流量进行监测和拦截,适用反向代理和域名访问方式的Web服务	实时	套	1
	本地WAF安全防护	本地硬件WAF安全防护能力,满足南京市建邺区新一代电子政务外网网络信息系统Web服务本地WAF安全防护要求。本地WAF作为云WAF安全防护的补充,需兼容云WAF,主要补充南京市建邺区新一代电子政务外网部分Web服务采用IP加端口方式访问WAF防护能力。同时,为确保互联网侧网络业务连续性,本地WAF应作主备冗余部署,提升网络可用性。	实时	套	2
	DNS云解析及防护	DNS攻击全力防御服务许可1年,满足南京市建邺区新一代电子政务外网所有域名的解析及防护需求	实时	套	1
	蜜罐服务	在互联网侧部署高仿真业务页面,主动诱导攻击行为,提前感知针对建邺区资产的各类网络攻击;实时监测内网扫描与异常访问,快速定位威胁来源,并结合蜜罐告警与防火墙联动机制,自动封堵攻击源IP,有效实现攻击预警、响应拦截和溯源追踪。	实时	套	1
	安全堡垒机	在南京市建邺区新一代电子政务外网云平台上新增部署堡垒机服务1套(信创软件版本、部署于南京市建邺区新一代电子政务外网阿里云平台、支持纳管主机数量不低于1000台、支持纳管信创主机、经检测认证的国密密码产品且安全等级为2级及以上),满足南京市建邺区新一代电子政务外网主机防护需求	实时	套	1
检测	安全漏洞扫描	对网络和系统进行安全扫描	每3月1次,1年4次	套	1
	安全渗透测试	对网络和系统进行模拟黑客方式进行攻击测试	每3月1次,1年4次	套	1
	违规外联安全检测	通过部署一套违规外联探测设备,开展对政务外网公共区所有连接的持续实时监控,自动识别违规行为。	实时	套	1
	日志管理	对电子政务外网区域内所有跨边界流量的原始日志(包括源IP、目的IP、端口、协议、会话时长等关键数据)进行统一留存,日志存储周期不少于6个月,确保日志数据的完整性与安全性,支持安全事件快速溯源和精准取证。	实时	套	1

服务类别	服务名称	服务内容	服务频次	单位	数量
响应与恢复	安全威胁监测综合分析	安全工程师现场驻场2名,对南京市建邺区新一代电子政务外网进行安全运维、漏洞闭环、风险评估、资产管理、网络安全研判分析,南京市建邺区新一代电子政务外网安全技术手段的安全告警分析与处置,安全事件7*24小时应急响应及恢复,每日报送工作日报	实时	套	1

1.3 标的质量:

服务开始后,每月进行服务考核,全年服务质量考核款为合同总金额的60%。根据考核结果计算每月的服务质量考核款(每月服务质量考核款最高为合同总价的5%),考评条件如下:(1)全月考核总得分小于80,扣除100%的服务质量考核款;(2)80≤全月考核总得分<90,扣除50%的服务质量考核款;(6)90≤全月考核总得分,支付全部的服务质量考核款。

项目考核办法(月度)			
考核周期:项目服务期内按月度进行考核			
评分项	内容	评审标准	分值
服务内容要求	1、制定并提供完善的《安全配置基线规范》,每月开展安全基线核查。 2、在南京市建邺区新一代电子政务外网出口节点旁路部署态势感知设备,并及时处置政务外网公共区、互联网区出口态势感知设备发出的告警信息。 3、在南京市建邺区新一代电子政务外网互联网侧部署高仿真业务蜜罐,并及时处置蜜罐设备的告警信息。 4、开展网络安全规划、网络安全建设方案咨询、网络安全管理咨询工作,根据需求输出《现状调研报告》、《网络信息安全发展规划》、《网络安全相关管理制度》等文档。 5、在指定设备上部署主机安全(EDR)agent,及时处置入侵风险并至少组织一次全量的病毒、木马查杀工作。 6、将南京市建邺区新一代电子政务外网互联网web服务纳入云WAF保护范围之内。 7、南京市建邺区新一代电子政务外网网络中部署本地WAF,将南京市建邺区新一代电子政务外网网络信息系统Web服务互联网暴露	每有1个点未达到内容要求扣4分,本项最多扣40分。	40

	面纳入本地硬件 WAF 进行安全防护范围。 8、购买云解析DNS及防护服务许可1年。 9、部署违规外联安全检测设备，并及时处置设备的告警信息。 10、延期南京市建邺区新一代电子政务外网现网云平台堡垒机维保服务1年。 11、每两个月进行一次全量的漏洞扫描工作，提供总计6份《漏洞扫描评估报告》，并协助整改。 12、每三个月进行一次业务系统渗透测试工作，提供总计4份《渗透测试报告》，并协助整改。 13、专人每日对南京市建邺区新一代电子政务外网所有安全技术手段的安全告警进行分析与处置，协助安全管理并出具《安全运维服务日报》，网络安全事件应急处置。		
安全事件通报	省、市级以上的中高危及以上网络安全事件有效通报数量	本项最高扣30分： 安全漏洞通报： 1、每有1个省级及以上高危有效通报扣20分，每有1个省级及以上中高危有效通报扣15分，最多扣30分。 2、每有1个市级高危有效通报扣20分，每有1个市级中高危网络安全事件通报扣10分，最多扣30分。 安全事件通报： 1、每有1个省级及以上高危有效通报扣30分，每有1个省级及以上中高危有效通报扣20分，最多扣30分。 2、每有1个市级高危有效通报扣30分，每有1个市级中高危网络安全事件通报扣15分，最多扣30分。 高危网络安全事件：造成重要网络和信息系统遭受特别严重的系统损失，系统大面积瘫痪，丧失业务处理能力的； 中高危网络安全事件：重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响的。	30
项目进度	1、根据甲方进度要求及时完成安全服务技术手段部署并维护其正常运行。 2、按甲方进度要求及时开展安全服务工作。 3、及时支持甲方安全事件处置，及时跟踪安全问题/漏洞复核进度。 4、按照甲方统一进度要求，按时提供各类服务	每有一项未满足进度扣2分，最多扣20分	20

	成果文档。		
文档质量	1、按甲方进度要求出具统一格式的相关成果文档。 2、文档中若包含安全问题/漏洞，应提供对应的举证、描述及处置建议等信息。	每有一份文档未满足质量要求扣1分，最多扣10分	10
月度综合评分合计			100

1.4 履行时间（期限）：合同签订至履约结束。

1.5 履行地点：南京市建邺区城市数字治理中心。

1.6 履行方式：

1.6.1、信息系统安全运维成果物要求

项目实施过程中产生建设方案、工作记录、工作结论等一切工作成果产权均归甲方所有。

1.6.2、信息系统安全运维工作承诺要求

乙方承诺全权负责甲方信息系统的安全保障工作，在项目合同履行期内，出现的相关信息系统安全事件，乙方负责全面处理并承担由此引发的所有责任。在安全事件处理中产生的所有费用均由乙方承担。

1.6.3、项目团队及人员要求

（1）乙方须为本项目建立技术支撑团队，负责本项目的总体规划、各项工作计划及内容制定、技术实施及故障处置。

（2）乙方安排至少2名安全工程师现场服务，现场服务期同合同期。现场人员须熟练掌握上述软硬件清单运维经验，能够及时处理设备相关的硬件和软件问题。

（3）提供现场服务的安全工程师须具备网络安全领域或安全咨询领域相关证书。对南京市建邺区新一代电子政务外网进行安全运维、漏洞闭环、风险评估、资产管理、网络安全研判分析，为网络软硬件平台建设提供安全咨询，提供网络安全建设中涉及到的决策、管理及运行操作问题的专业咨询，配合进行可行性研究、方案制定、产品选型等准备工作；按需组织网络与信息安全培训，协助南京市建邺区新一代电子政务外网网络安全管理单位开展网络安全管理工作。在重点时期前对现有网络运行的系统开展安全检查工作，对发现的问题进行相应安全整改，在重点时期之前做好安全加固及防护，保障系统安全稳定运行。根据网络安全保障防护的需要，派驻相关的安全服务专家进行5*8小时的现场驻守服务。

（4）项目组成员必须与响应文件中的拟派出人员保持一致，如有人员调整，应当提前5个工作日向甲方提交书面申请和人员证书（证书等级须高于或等于被更换人员），须保证更换人员服务能力高于或

等于被更换人员且满足项目需求，经甲方批准同意后方可调整。（注：如供应商提供人员能力不能满足需要，采购人有权要求更换，供应商应在48小时内做出响应）

1.6.4、项目实施人员管理要求

严格遵守《中华人民共和国网络安全法》及国家、省、市相关网络安全、保密规定，在规定的区域开展职责范围的工作，不得进入与之无关的工作区域；不得在机房设备上建立与工作无关的网站、网页和服务；不得在设备中传输、粘贴有害信息或与工作无关的信息；不得擅自对设备进行扫描、探测和入侵信息系统；不得对工作信息和资源越权访问、违规使用；不得私自允许他人接触和使用机房设备；严禁将工作用设备和文件带离机房；未经采购人同意，严禁以任何方式和介质拷贝服务器上的任何信息及项目中涉及的信息；对工作中接触到的信息做到保密；不准擅自摘抄、下载、复制、拍摄、提供、销毁或私自留存相关文件、资料（含电子文档）；严禁违反“一机两用”规定；不得在私人交往中谈论相关工作；不得有其他任何危害信息安全的行为。

1.6.5、网络安全及保密要求

（1）乙方应严格执行《中华人民共和国网络安全法》及国家、省、市相关网络安全、保密规定，乙方应按照网络安全等级保护三级要求、网络安全等级保护2.0标准，加强项目驻场及后台实施人员管理。乙方因本项目人员、技术、管理等原因直接或间接产生的各类网络安全事件，乙方承担法律、经济及社会责任，并向甲方承担违约责任。

（2）乙方须对参加项目的人员开展网络安全、保密教育以及人员背景审查，项目实施人员应按照甲方人员管理要求，在监理单位处备案并签订保密协议后进入项目组工作。

（3）凡以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密，将追究当事人及乙方的责任。

（4）项目结束后，乙方在本项目服务期内产生的所有资料（包括纸质、电子类）应全部移交给甲方。

1.6.6、维保服务要求

（1）服务期内，本合同项目所有技术和服 务发生任何非人为故障，由乙方负责系统恢复。故障报修的响应时间为即时，到达现场的时间为1小时，小型故障恢复时间为4个小时，严重故障恢复时间为24小时内，并提供及时有效的解决方案。

（2）服务期内，对甲方提出的合理服务要求，乙方必须及时响应。如响应不及时或服务不满足采购人要求，采购人有权自行处理，相关费用由乙方负责。

（3）所有的服务方式均为乙方上门保修，即由乙方派员到系统使用现场进行故障恢复，由此产生的一切费用均由乙方承担。

(4) 安全软件和硬件设备质保自安全服务相关技术手段在建邺区完成部署并具备安全服务能力, 获得甲方确认起一次性续期至少1年, 另按需进行备机和备品配件应急保障, 确保各项安全设备、软件、人员持续服务不中断。

1.6.7、服务保障和自罚承诺

(1) 如果发生因乙方安全措施不力造成的事故责任、或者其他工作失误, 由此所产生的一切责任由乙方承担。

(2) 如因乙方投入人员过少原因, 造成无法在承诺工期内完成服务, 由此产生的一切责任由乙方承担。

1.6.8、培训要求

乙方按照甲方要求提供详细明确的培训课程内容(包括软件使用、项目实施内容所包含技术的应用、采购人要求的培训内容等)、人数和时间安排。

1.6.9、应急响应要求

按照甲方要求提供信息安全后援应急支撑服务, 30分钟内响应, 1小时内到达现场, 配合采购人排除故障, 保证系统最短时间恢复正常运行。

1.6.10、项目实施要求

(1) 项目文档: 成交供应商必须按国家、省、市行业标准规范及本项目相关工作要求, 提交技术文档和验收文档。

(2) 项目版权: 乙方必须保证本项目成果及所使用到资源的版权合法性, 本项目成果及实施过程中一切产出物所有权及版权归甲方所有。

(3) 项目保密: 乙方严格规范执行各项保密制度, 对采购人各类信息进行保密管理, 杜绝任何泄密事件的发生。

(4) 乙方提供的服务完全符合磋商文件的要求, 在响应文件中提供的服务承诺及方案是真实的, 一旦由甲方发现服务与响应文件说明不符, 甲方有权立即解除与供应商的合同。

(5) 成交供应商应遵守国家、省、市及甲方相关廉政管理规定。

1.6.11、质量保证要求

(1) 包含与项目需求相关的备件(含软、硬件)需在合同签订前一周内备齐, 备件配置不低于现在用设备规格, 并存放于采购人指定地点, 由甲方对备件进行核验, 核验合格并经测试对现网无影响后方可签订合同, 否则, 甲方有权追究责任。

(2) 乙方在项目服务前, 须详细分析在本次项目服务过程中存在的可能影响现有系统安全性与稳定性的风险, 并采取必要的风险控制措施。任何由乙方在项目服务工作中对甲方造成的负面影响, 其后

果都须由乙方承担。

(3) 甲方将在服务过程中对乙方的服务质量进行考核。甲方应根据项目的工作计划，对阶段性工作成果进行审核，并向甲方提交阶段性工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

1.6.12、安全责任

项目服务期内，如发生信息安全事件，造成损失和重大影响的，由乙方承担法律责任、赔偿损失。

二、合同金额

2.1 本合同金额为（大写）：柒拾柒万陆仟圆（776000.00元）人民币。

本合同总价款包含以下内容：

- (1) 完成本服务项目发生的所有含税费用；
- (2) 支付给员工的工资和国家强制缴纳的各种社会保障资金；
- (3) 乙方应当提供的伴随服务/售后服务费用；
- (4) 乙方认为需要的其他费用。

本合同最终结算价款按照服务考核情况确定。

三、技术资料

3.1 乙方应按采购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、权利保证

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

6.1 本项目乙方无需缴纳履约保证金。

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 合同款项的支付方式及进度安排

8.1.1、合同签订后，甲方向乙方支付合同总价的10%，安全服务相关技术手段在南京市建邺区新一代电子政务外网完成部署并具备安全能力并经甲方确认后，甲方向乙方支付合同总价的30%。

8.1.2、服务开始时间从安全服务相关技术手段在南京市建邺区新一代电子政务外网完成部署并具备安全能力后开始计算，服务期满后一次性支付相应考评款。服务开始后，每月进行服务考核，根据考核结果计算每月的服务质量考评款（每月服务质量考评款最高为合同总价的 5%）。考评条件如下：（1）全月考核总得分小于 80，扣除 100%的服务质量考评款；（2） $80 \leq$ 全月考核总得分 <90 ，扣除 50%的服务质量考评款；（6）全月考核总得分 ≥ 90 ，支付全部的服务质量考评款。

8.1.3、乙方提供付款申请时，须一并提供以下资料：（1）乙方签发，并载明付款金额的付款通知一份；（2）乙方提供的并经甲方书面确认的技术服务单（即书面服务总结报告及考核得分）；（3）乙方开具给甲方支付金额的正式增值税专用发票。注：满足合同约定支付条件的，甲方收到乙方发票后 10 个工作日内，将资金支付到合同约定的乙方账户。

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 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

10.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时，甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

10.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

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 甲方未按合同规定的期限向乙方支付服务款的，每逾期 1 天甲方向乙方偿付欠款总额的 5‰ 滞纳金，但累计滞纳金总额不超过欠款总额的 5% 。

11.3 乙方逾期提供服务的，乙方应按合同价款总额的5‰向甲方支付违约金，但累计违约金总额不超过合同价款总额的 5%，由甲方从待付合同款项中扣除。逾期超过约定日期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 乙方所提供服务标准不符合合同规定及采购文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

11.5 若因乙方过错行为（包括但不限于技术缺陷、服务疏漏、管理失职等）导致甲方在省级、市级或上级主管部门组织的网络安全检查、审计、评估活动中被认定为不合格，或因网络安全问题遭受书面通报批评、行政处罚、媒体曝光等负面结果，均视为乙方违约情形。每发生一次本条款下的违约情形，乙方应向甲方支付违约金，违约金金额为合同价款总额的5%。如多次出现，甲方可单方面终止。

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。

十四、合同生效及其它

14.1 合同经双方法定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《中华人民共和国民法典》《中华人民共和国政府采购法》有关条文执行。

14.3 本合同正本一式肆份，具有同等法律效力，甲方、乙方各执贰份。

甲方：

乙方：

地址：

地址：南京市建邺区永初路8号阿里中心T4栋1208室

法定代表人：

法定代表人：

签订日期：

2026年2月13日

陈伟

附件

附件一 报价表

报价一览表

报价表

项目名称：智慧建邺网络信息系统安全运维服务项目			
项目编号：SZC320105-SJGC-C2025-0013			
序号	名称	报价（万元）	其中，小、微型企业 报价（万元）
1	智慧建邺网络信息系统安全运维服务项目	77.6	77.6
	合计：	77.6	77.6
总价（人民币，大写）		柒拾柒万陆仟陆	
供应商是否属于小微企业		是 ☒ 否 ☐	

供应商名称：南京大数据安全技术有限公司（加盖公章或电子章）

注：在“供应商是否属于小和微型企业”栏后“是”或“否”上打“√”。

分项报价表

项目名称:		智慧建邺网络信息系统安全运维服务项目						项目编号:		JSZC-320105-SJGC-C2025-0013		
序号	名称	品牌	型号	产地	承接单位	所属行业	类型	最高限价(元)	单价(元)	数量	小计(元)	
1	安全识别-基线核查服务	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	18000	1	18000	
2	安全识别-安全威胁分析技术服务(互联网区)	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	60000	1	60000	
3	安全识别-安全威胁分析技术服务(公共区)	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	60000	1	60000	
4	安全保护-服务器主机防病毒	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	50000	1	50000	
5	安全保护-云WAF安全防护	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	30000	1	30000	
6	安全保护-本地WAF安全防护	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	50000	2	100000	
7	安全保护-DNS云解析及防护	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	10000	1	10000	
8	安全保护-蜜罐防护	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	10000	1	10000	
9	安全保护-安全堡垒机	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	50000	1	50000	
10	安全检测-安全漏洞扫描	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	10000	1	10000	
11	安全检测-安全渗透测试	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	20000	1	20000	
12	安全检测-违规外联安全检测	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	50000	1	50000	

13	安全检测-日志管理	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	48000	1	48000
14	安全响应与恢复-安全威胁监测综合分析	大数据安全	/	南京市	南京大数据安全技术有限公司	信息技术服务业	服务	/	260000	1	260000

附件二 服务一览表

项目名称	智慧建邺网络信息系统 安全运维服务项目	项目编号	JSZC-320105-SJGC-C2025-0013
服务企业 名称	南京大数据安全技术有 限公司	服务企业地址	南京市建邺区永初路8号阿里中心T4栋1208室

1 安全识别-基线核查服务

序号	考核要求	功能、性能、 配置要求	详细参数
1	★实质性 要求	基线核查服务 范围	南京市建邺区新一代电子政务外网（公共网络区、互联网 网络区）
		基线核查服务 频次	基线核查频次为1月1次，全年12次。
		基线核查服务 形式	现场核查
		基线核查服务 内容要求	1) 安全基线核查： 安全服务供应商依据法律法规和业务环境，协助制定系统安全配置基线规范。再根据上述规范，采用自动工具检查（安全服务供应商提供）加人工审核的方式，对系统进行基线核查，检出信息系统与相关IT设备配置的不合规部分。检查内容包括但不限于：服务和应用程序设置、操作系统组件的配置、账号和权限分配、管理规则等。 通过安全基线核查服务，对“南京市建邺区新一代电子政务外网”所涉及的操作系统，Web服务和应用中间件，数据库，网络和安全设备、网络边界等安全配置规范进行梳理和优化，制定符合行业监管要求且为最佳实践的安全基线标准，使得在后期的信息安全体系建设中，都依照该安全基线进行最佳部署，从根本上解决一些不符合规范的配置问题。 2) 配置审查： 按照项目进度统一要求，对指定信息系统进行专家人工安全审核，发现信息系统配置中存在的安全弱点。 通过分析安全审核结果，对指定信息系统的安全威胁、技术脆弱性等风险构成因素进行综合分析和评定，并提供针对性的改进建议及协助加固。 另外应重点关注暴露面压降问题，对基线合规检测结果进行分析，对暴露面压降提出具体实施措施。 3) 基线自动化核查工具：

			安全服务供应商提供基线自动化核查工具。基线自动化核查工具应采用成熟稳定的EDR方案，并部署在南京市建邺区新一代电子政务外网网络内，EDR终端支持部署安装在信创操作系统环境。
		基线核查服务 产品要求	服务端适应公有云、私有云及混合云架构，采用自适应安全及端点检测及响应（EDR）的解决方案
			主机端具有独立的自助安装界面，linux支持自动生成下载和安装命令，windows支持自动生成安全包下载安装 1) 采用轻量级Agent，大大减轻Agent对于主机性能的影响，并支持动态地升级和更新； 2) Agent要求具备“自退出”设置
			支持Windows 2003、Windows 2008、Windows 2012、Windows 2016、Windows 2019、Oracle、Red Hat、SUSE、CentOS、Ubuntu、Debian、Fedora、OpenSuse、amazon、BC-linux、中标麒麟、中科红旗、银河麒麟等操作系统
		资产管理	(1) 资产识别： 资产采集应该具备完善的颗粒度采集：通过从主机、Web站点、Web容器、Web应用、Web应用框架、账号、计划任务、端口、数据库、进程、第三方组件、环境变量、Jar包、系统安装包、软件应用、内核模块等多个维度进行统一的管理和清点资产概况； (2) 主机： 1) 支持采集已安装轻代理主机中的各类信息，支持采集主机内外网IP、主机名、操作系统、系统内核、业务角色、安装时间等信息； 2) 支持主机自定义分组管理、支持主机资产价值自定义管理； 3) 支持通过主机分组、体检分数、主机状态、操作系统、业务角色、资产价值、安装时间等过滤筛选； (3) 端口： 支持探测主机上对内端口及对外端口，可采集端口对应的服务及端口协议信息； (4) 网站： 支持探测主机上的网站信息，可采集网站域名、网站安装路径、网站运行状态及网站相关的web容器等信息； (5) Web容器： 支持采集主机上的Web容器信息，可采集Web容器的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、

		插件路径、数据路径、进程二进制路径、启动参数等信息；支持Web容器有Apache、IIS、JBoss、Nginx、Tomcat、Weblogic等； (6) 第三方组件： 支持采集主机上的第三方组件信息，可采集第三方组件的版本、安装路径、相关网站等信息；支持的第三方组件有CKEditor、DedeCMS、Discuz、PHP、PHPMyAdmin、Struts2、WordPress、Zabbix等； (7) 数据库： 支持采集主机上的数据库信息，可采集数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等；支持的数据有Hadoop、Memcached、MySQL、Redis等。支持主机及对应数据库双维度查看； (8) Web框架： 1) 支持识别出所有Web站点中使用的框架，并且识别出框架版本、使用该web框架的web应用的路径等信息； 进程： 2) 支持采集主机上的进程信息，可采集进程的路径、版本、hash值等；支持进程白名单设置、业务进程设置等；可通过运行状态、进程标签、进程权限、是否系统进程、是否自启动、是否包管理安装、是否服务进程等多个维度进行进程信息的筛选； (9) 账号： 支持采集主机上的账号信息，可采集账号的用户名、是否Root权限、Shell、状态、上次登录时间、可否交互登录、登录方式、所属用户组、UID、密码过期时间、上次密码修改时间、终端、IP、用户主目录、上次密码修改时间、是否可交互登录等信息。
	安全体检	支持即时体检及定时体检两种体检模式，即时体检即检测命令下发后立即执行体检命令；定时体检用户设置扫描周期、扫描时间段后系统会按照设置规则定时执行体检命令； 支持批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发。并且支持定时体检策略与即时体检策略两种类型；
	风险管理	漏洞风险： (1) 支持发现主机自身的脆弱性，并形成了自有的漏洞知识库体系：

		Windows漏洞通过订阅微软漏洞更新，当发现主机存在漏洞时推送微软官方补丁信息，支持漏洞修复、忽略；Linux漏洞通过检测主机上的软件版本信息，与CVE官方漏洞库进行匹配，检测出存在漏洞软件并推送漏洞信息，支持漏洞忽略； （2）支持对人为原因造成的风险因素如弱口令（操作系统弱口令、数据库弱口令等）、高危账号（高权限账号、空密码账号、用户名和密码相同的账号）、配置缺陷（操作系统配置缺陷、Web容器配置缺陷、数据库配置缺陷等）进行管理； （3）支持显示当前主机上的漏洞风险情况，同时提供修复方案供用户进行参考； （4）支持从云端下载漏洞策略库在本地执行检测； （5）支持对存在漏洞风险的主机上报应用软件的名称、版本号、路径、发现时间； （6）支持对检测出的各类漏洞风险进行风险等级评估。 漏洞检测： （1）支持自动扫描主机操作系统的系统漏洞，并提供补丁官方下载链接； （2）支持安全建议、漏洞介绍、影响版本、CVE漏洞描述及漏洞修复； （3）Windows 支持漏洞修复； （4）Linux包括rootkit漏洞、Linux核心库漏洞、Linux CVE漏洞等。 应急漏洞： 具备丰富的应急漏洞库，针对新爆发的高危漏洞，支持实时发起检测任务对全网主机资产进行高危漏洞检测，确认是否有资产受到影响。并提供详细漏洞描述、修复建议、修复影响，指导下一步漏洞应急处置工作。 网站漏洞： 支持检测Discuz远程代码执行漏洞、DedeCMS注入漏洞、WordPress IP验证不当漏洞，支持漏洞忽略、修复操作； 弱口令： 可识别操作系统弱口令、数据库弱口令、应用弱口令，应包括：ssh、RDP、MySQL、FTP、Redis、MongoDB、Memcached、ElasticSearch、PostgreSQL、Samba、VSFTP、ProFTP，支持弱口令忽略操作； 高危账号： 可识别高权限账号、空密码账号、用户名和密码相同
--	--	--

			的账号，支持高危账号忽略、禁用、信任； 可对系统中的影子账号、空密码账号、可疑高权限账号、可sudo账号、是否限制su成root账号检测和告警； 配置缺陷： (1) 具备操作系统、Web容器、数据库、及其他应用的配置缺陷检测能力，支持Windows2003、Windows2008、Windows2012、Windows2016等各种Windows系统配置缺陷检测； (2) 支持Memcached、CentOS、Ubuntu、Debian、OpenSUSE、RedHat等Linux操作系统配置缺陷检测； (3) 支持IIS、Apache、Nginx、Tomcat、Weblogic、Tengine、JBoss等各类Web容器配置缺陷检测； (4) 支持Redis、Mongodb、Memcached、ElasticSearch、PostgreSQL、Oracle等数据库配置缺陷检测； (5) 支持FTP、SNMP、Samba等应用的配置缺陷检测。
		安全防护（基线安全加固）	安全防护： 支持端口安全防护、防护控制、暴力破解防护、扫描防护、病毒防护、IP黑白名单设置、进程行为控制，可通过对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件； 端口安全： 支持端口安全规则设置，可选宽松模式及严格模式，宽松模式下开放所有端口，只关闭规则中的端口；严格模式下关闭所有端口，只开放规则中的端口。支持TCP、UDP、ICMP、IGMP6、IGMP五种协议； 访问控制： 支持文件保护及注册表保护，支持记录并拦截模式及记录不拦截两种模式，可选系统防护规则或自定义防护规则，系统防护规则提供高、中、低三种防护等级； 支持关键位置文件的保护：能够禁止对指定位置文件的操作，包括文件删除、读取等行为。 暴力破解防护： 提供全方位的暴力破解防护功能，支持FTP防暴力破解、远程桌面防暴力破解、MySQL数据库防暴力破解等暴力破解防护功能，支持记录并拦截、记录不拦截两种模式； 扫描防护： 支持扫描攻击防护，能有效地防止入侵扫描，可选记录并拦截、记录不拦截两种模式； 病毒木马防护： 支持多引擎技术识别并查杀最新病毒，应至少包含四

			种查杀引擎；支持轻巧、中度、严格三种防护等级； IP黑白名单： 支持白名单及黑名单设置，支持黑白名单批量导出及导入；黑名单下可设置记录并拦截、记录不拦截两种模式； 进程行为控制： 支持进程行为控制，能够有效地监测非法进程操作； 进程白名单： 通过自学习或添加进程白名单，对非白名单进程的启动进行告警，非白名单进程支持记录或拦截模式； 账号保护： 支持账号保护优化，针对帐号提权、账号克隆等账号异常创建操作进行有效禁止；主动发现账号，锁定账号，防止用户私自新建账号； 远程登录保护： 支持远程登录保护：通过阻止未授权用户的远程登录，为服务器提供实时、主动的远程登录保护功能。
		合规基线	提供常用的linux及windows系统基线模板，支持基线检查及部分基线自动优化，支持用户自定义基线模板。
		服务成果	开始时提供《安全配置基线规范》；每次核查审查后提交基线不合规问题清单和暴露面压降建议清单。

2 安全识别-安全威胁分析技术服务

序号	考核要求	功能、性能、配置要求	详细参数
1	★实质性要求	安全威胁分析范围、频次、服务形式	采用现场或远程专家人工分析，态势感知系统对南京市建邺区新一代电子政务外网内外网进行安全威胁实时分析。
		安全威胁内容要求	在南京市建邺区新一代电子政务外网出口节点旁路部署态势感知设备，中标供应商提供态势感知设备。 安全态势感知设备能力应不低于如下要求： 1) Web 应用攻击检测： 具备 Webshell 检测能力，并能识别出不同攻击手段，包括但不限于B374k、中国菜刀、PHP 后门上传、Asp shell、冰蝎、冰蝎 3.0、Jsp、一句话木马、蚁剑等，并具有机器学习检测 Webshell 能力。具备 SQL 注入攻击检测能力，并能识别出不同攻击手段，包括但不限于泛微 OA、用友 OA、通达 OA、启莱 OA、致远 OA 等，并具有机器学习检测 SQL 注入能力。具备XSS注入攻击检测能力，并具有机器学习检测能力。支持检测其他类型 web 攻击，包括但不限于敏感文件访问、XXE 注入、文件包含漏洞、CSRF 跨站

		请求伪造、路径穿越攻击、文件下载攻击、web 远程代码执行、web 爬虫探测、web 扫描。 2) 隐蔽隧道检测: 具备 DNS 隐蔽隧道检测能力,并具有机器学习检测能力。具备 ICMP 隐蔽隧道检测能力,并具有机器学习检测能力。具备 HTTP 隐蔽隧道检测能力,并能识别出不同攻击手段,包括但不限于reDuh、abptts、CobaltStrike、Tunna、ReGeorg、Firepass,并具有机器学习检测能力。具备 DGA 域名检测能力,并能识别出不同攻击手段,包括但不限于speech、enviserv、mirar、kraken、pykspace_v2、ranbyus、Murofet、symmi,并具有机器学习检测能力。 3) 恶意文件检测: 具备僵木蠕文件检测能力。具备加壳文件检测能力,并能识别出加壳方法。具备 APT 文件检测能力,并能识别出具体APT家族。内置沙箱支持多平台动态检测能力,包括 Windows 7,Windows 10, Windows Server 2016,Windows Server 2008, Linux, Android, 支持系统根据样本类型自动选取匹配的虚拟机环境分析样本,支持显示沙箱内样本运行。支持基因图谱检测能力,支持通过机器学习方式检测变种文件,提供高级病毒检测能力。进程行为检测:支持文件进程行为检测,可视化展示文件在沙箱内的进程行为,包括创建进程、进程行为、释放进程等。文件静态信息检测:支持显示文件静态信息,包括文件头、PE 节表信息、PE 资源信息、PE 导入表信息等。杀毒引擎检测:支持内置不少于 3 个杀毒引擎,支持启发式检测。 4) 加密、暗网流量检测: 具备恶意加密流量检测能力,并能识别出不同攻击手段,包括但不限于 IcedID、TrickBot、PandaZeuS、CobaltStrike等恶意家族。具备暗网流量检测能力,支持基于机器学习方法检测暗网流量并与威胁情报、特征检测交叉验证。 5) 木马、蠕虫通信检测: 具备蠕虫检测能力。具备木马检测能力,包括但不限于窃密木马、远控木马、银行木马、后门木马等。具备勒索软件检测能力。具备间谍软件检测能力。 6) 网络异常行为检测: (1) 具备密码暴力破解能力,包括但不限于SSH、SMB、HTTP、FTP、MYSQL 等。 (2) 具备透工具识别能力,包括但不限于 CobaltStrike、PowerShell Empire C2、Netsparker 等。 7) 漏洞攻击检测:
--	--	---

		具备 IE 漏洞攻击检测能力；具备微软漏洞攻击检测能力；具备 TFTP 漏洞攻击检测能力；具备 Apache 漏洞攻击检测能力；具备多种基于 CVE 漏洞攻击检测能力。 8) 威胁情报检测： 支持IP、URL、域名类型情报。支持 APT检测能力。支持文件 Hash 情报检测能力。 9) 协议解析： 能够解析并存储HTTP、FTP、SMTP、POP3、SMB、SSH、DNS、MYSQL、TELNET、RDP、ICMP、IEC60870-5-104、IEC61850-MMS、IEC61850-GOOSE、IEC61850-SV、GTP等协议。支持还原exe、pdf、xls、ppt、py、zip、jpeg、rar等文件类型。支持通过如下协议进行文件还原，包括但不限于HTTP、FTP、SMTP、POP3、IMAP、IEC61850-MMS、IEC60870-5-104等。支持HTTPS流量解析。 10) 数据展示及策略配置： 大屏展示：支持综合安全态势展示、支持资产态势展示、支持攻击者态势展示、支持外联风险态势展示、支持横向威胁态势展示、支持威胁事件态势展示、支持安全金字塔展示。 溯源取证： 支持告警高亮显示功能，关键证据高亮显示，以便展示关键威胁信息。 具备威胁的研判和取证能力，无需借助第三方软件，可通过产品直接在线解包并查看原始包信息内容，支持下载事件相关的 PCAP 包。 攻击结果分析：支持从多个维度捕获并分析攻击链，自动化完成对攻击结果进行判定，包括成功、尝试、疑似。 威胁分析： (1) 支持以攻击者/受害者视角查看威胁事件，包括但不限于攻击者 IP、受害者 IP、是否属于资产、攻击手段、攻击结果、攻击阶段、攻击起止时间、攻击事件数量等。 (2) 攻击链分析：支持通过流量的监控分析，自动化形成攻击链，识别攻击阶段，能够从攻击链阶段的扫描探测、尝试攻击、漏洞利用、木马下载、远程控制、横向渗透、行动收割等阶段识别对应的攻击方式。 (3) 支持保存检索参数，方便分析人员保存历史分析场景，用于快速聚焦关注的威胁事件。 (4) 支持告警威胁情报联动，可对恶意 IP，恶意域名，恶意 URL，恶意文件进行情报匹配与分析，威胁情报展示内容至少包含：威胁 IOC、情报类型、攻击类型、情
--	--	--

		报家族等。 (5) 支持对攻击源 IP/目的 IP 进行关联与溯源，并对所有攻击行为以时间轴的方式进行展示。 离线威胁分析： (1) 支持流量包上传功能，支持pcap、cap、pcapng三种格式。 (2) 支持文件上传功能，支持rar、zip、doc、docx、pdf等文件格式。支持上传文件和所提供的 URL 中的文件检测；支持前台批量上传待检测文件；支持检测结果的直接跳转。 (3) 支持离线回放大量pcap文件，自动获取ftp 服务器和文件共享服务器文件数据，并上传至设备本地沙箱进行文件动态检测。 策略管理： (1) 支持添加黑名单，可添加IP、域名、URL、文件MD5、邮箱IOC。 (2) 支持添加白名单，可根据源IP、目的IP、域名/URL、威胁名称、XFF、攻击载荷、过期时间进行添加白名单字段。载荷支持正则匹配与精准匹配，可自定义载荷匹配位置，至少包括攻击/异常载荷、HTTP请求头、HTTP 请求体、HTTP响应头、HTTP响应体。 (3) 支持通过邮件、钉钉、企业微信方式发送告警通知。 (4) 支持调整文件检测优先级，可在文件有堆积的情况下，调整文件优先级优先进行检测。 (5) 支持添加自定义规则，允许用户在 web 界面自定义添加检测规则，支持定义相应的威胁等级、确信度、攻击阶段、攻击组织以及攻击工具等基本信息字段。 安全管理： (1) 支持账号锁定功能，设备自身账号支持登录失败次数过多自动锁定功能，可配置登录失败次数限制。 (2) 支持超时退出功能，支持界面超时无操作自动退出，并可配置超时时间。 (3) 支持登陆 IP 限定，可对登陆 IP 白名单配置，进行登陆限制。 资产识别： (1) 支持自动识别内部资产信息，可识别资产状态、资产名称、IP地址、资产组、MAC地址、操作系统、资产权重、设备类型、以及资产软件/服务/账号信息等资产内容。 (2) 支持手动添加内部资产信息，包括资产名称、IP地址、资产权重、设备类型、操作系统、资产组、所有者、
--	--	--

			资产描述等字段。 (3) 支持对资产进行分组管理,可按照资产组网段或者组织资产 IP 划分资产组,对资产进行模块化管理。 (4) 支持配置资产网段,包括网段、设备类型、国家、城市/单位及经纬度等信息。 威胁报告:支持自动化生成威胁分析报告,包括但不限于攻击结果、威胁等级、威胁事件类型、攻击阶段、风险主机展示,支持多种格式报表输出,包括但不限于 word、html、pdf。支持对威胁报告进行加密或添加水印等操作。
		服务成果	态势感知设备安全、稳定、可靠运行,对南京市建邺区新一代电子政务外网网络安全威胁进行实时分析和告警。

3 安全保护-服务器主机防病毒

序号	考核要求	功能、性能、配置要求	详细参数 (不低于以下要求)
1	★实质性要求	服务器主机防病毒要求	(1) 防护范围: 南京市建邺区新一代电子政务外网 (公共网络区、互联网络区) 相关设备及系统,管理主机数量不少于400台。 (2) 防护频次: 实时检测与查杀。 (3) 主机防病毒人工专家服务形式: 采用现场或远程专家人工服务形式。 (4) 服务器主机防病毒要求: 1) 采用主机安全 (EDR) 方案对服务器主机进行防病毒; 2) 应组织一次专项行动,对全量资产进行病毒、木马查杀、清理; 3) 安全服务供应商提供服务器主机防病毒系统平台或工具。服务器主机防病毒系统平台或工具,服务器主机防病毒应采用成熟稳定的EDR方案,并部署在南京市建邺区新一代电子政务外网网络内,EDR终端支持部署安装在信创操作系统环境。
		产品要求	(1) 服务端适应公有云、私有云及混合云架构,采用自适应安全及端点检测及响应 (EDR) 的解决方案; (2) 主机端具有独立的自助安装界面,linux支持自动生成下载和安装命令,windows支持自动生成安全包

			下载安装: 1) 应采用轻量级Agent,降低Agent对于主机性能的影响,并支持动态地升级和更新; 2) Agent要求具备“自退出”设置。 3) 支持Windows 2003、Windows 2008、Windows 2012、Windows 2016、Windows 2019、Oracle、Red Hat、SUSE、CentOS、Ubuntu、Debian、Fedora、OpenSuse、amazon、BC-linux、中标麒麟、中科红旗、银河麒麟等操作系统
		资产管理	(1) 资产识别: 资产采集应该具备完善的颗粒度采集:通过从主机、Web站点、Web容器、Web应用、Web应用框架、账号、计划任务、端口、数据库、进程、第三方组件、环境变量、Jar包、系统安装包、软件应用、内核模块等多个维度进行统一的管理和清点资产概况; (2) 主机: 1) 支持采集已安装轻代理主机中的各类信息,支持采集主机内外网IP、主机名、操作系统、系统内核、业务角色、安装时间等信息;支持主机自定义分组管理、支持主机资产价值自定义管理; 2) 支持通过主机分组、体检分数、主机状态、操作系统、业务角色、资产价值、安装时间等过滤筛选。 (3) 端口: 支持探测主机上对内端口及对外端口,可采集端口对应的服务及端口协议信息。 (4) 网站: 支持探测主机上的网站信息,可采集网站域名、网站安装路径、网站运行状态及网站相关的web容器等信息。 (5) Web容器: 支持采集主机上的Web容器信息,可采集Web容器的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等信息;支持Web容器有Apache、IIS、JBoss、Nginx、Tomcat、Weblogic等。 (6) 第三方组件: 支持采集主机上的第三方组件信息,可采集第三方组件的版本、安装路径、相关网站等信息;支持的第三方组件有CKEditor、DedeCMS、Discuz、PHP、PHPMyAdmin、Struts2、WordPress、Zabbix等 (7) 数据库:

			支持采集主机上的数据库信息，可采集数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等；支持的数据有Hadoop、Memcached、MySQL、Redis等。支持主机及对应数据库双维度查看。 (8) Web应用框架： 支持识别出所有Web站点中使用的框架，并且识别出框架版本、使用该web框架的web应用的路径等信息。 (9) 进程： 支持采集主机上的进程信息，可采集进程的路径、版本、hash值等；支持进程白名单设置、业务进程设置等；可通过运行状态、进程标签、进程权限、是否系统进程、是否自启动、是否包管理安装、是否服务进程等多个维度进行进程信息的筛选。 (10) 账号： 支持采集主机上的账号信息，可采集账号的用户名、是否Root权限、Shell、状态、上次登录时间、可否交互登录、登录方式、所属用户组、UID、密码过期时间、上次密码修改时间、终端、IP、用户主目录、上次密码修改时间、是否可交互登录等信息。
		安全体检	自定义体检： 支持用户自定义安全体检项目，病毒木马检测支持快速扫描、全盘扫描及自定义路径扫描三种方式，网页后门检测支持自定义路径扫描； 定时体检： 支持即时体检及定时体检两种体检模式，即时体检即检测命令下发后立即执行体检命令；定时体检用户设置扫描周期、扫描时间段后系统会按照设置规则定时执行体检命令； 批量体检： 支持批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发。并且支持定时体检策略与即时体检策略两种类型； 体检报告： 支持体检报告生成及导出，体检报告展示体检分数、健康指数，体检结果图表化展示及详细体检问题说明展示，可导出Word格式的体检报告。
		安全监控	(1) 监控要求： 可对主机开启各类监控包括登录监控、完整性监控、

		操作审计、进程监控、资源监控、性能监控。从主机安全角度，全天候监控主机的运行情况，能确保第一时间发现服务器问题，排除故障时间提速10倍，帮助企业快速发现安全风险和性能瓶颈。安全监测监测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中； (2) 登录监控： 监控主机登录情况，可以设置常用地点、常用IP、常用时间段，监控类型有异常地点、异常时间、异常IP和暴力破解登录情况 (3) 完整性监控： 1) 监控文件和目录的完整性情况，包括文件被修改、删除和新增，支持设置文件夹和特定文件监控，支持白名单路径和文件类型；(签订合同时提供功能截图证明) 2) 监控账号是否存在修改账号用户名、修改账号密码、修改账号权限、删除账号和新增账号的操作。(签订合同时提供功能截图证明) (4) 操作审计： 可对Linux当前用户的shell命令并记录命令内容、进程和操作用户和登录IP，可以通过定义的规则进行筛选威胁的命令 (5) 进程监控： 支持监控服务器进程，实时发现可能存在的异常进程；
	入侵威胁管理	(1) 入侵威胁： 支持对恶意进程及软件进行查杀，并提供隔离、信任等操作。 (2) 病毒木马： 支持发现二进制病毒木马信息，包含病毒的类型、hash、路径，并且提供对病毒的隔离、信任和下载，支持显示病毒引擎版本号。 (3) 网页后门： 展示安全体检和实时防护的webshell文件信息，包含webshell的类型、hash、路径，并且提供对webshell文件隔离、信任、下载和查看操作。 (4) 反弹 shell： 支持安全体检和实时防护的反弹 shell 进程、进程运行参数、父进程和父进程运行参数、本地地址和反弹的目的地址。 (5) 异常账号： 支持影子账号、篡改系统账号的检测识别及事件关闭，影子账号支持禁用处理。

			(6) 日志删除： 支持 windows 日志删除的检测识别及事件关闭，支持 windows 日志删除事件告警。 (7) 异常登录： 支持异常登录信息，包括异常地点、异常IP、异常时间和暴力破解登录信息。 (8) 异常进程： 展示安全体检的子进程高于父进程权限进程、隐藏进程和隐藏端口进程信息，进程 hash 等。 (9) 系统命令篡改： 支持安全体检检测到的系统命令被篡改的信息，包括篡改后的 hash，路径、篡改系统命令的危害和建议，并提供隔离和信任操作。 (10) 进程监控： 支持进程行为监控功能，针对 RCE 攻击、漏洞利用、凭证窃取、隐秘隧道等攻击行为能够有效检测，支持对进程基本信息及关键行为信息等多个维度进行采集，包括进程名称、进程文件路径、运行进程所属用户、进程 MD5 值、进程命令行、进程树等，可通过指定进程树上的起始进程、终点进程、以及中间各层级的进程进行规则配置、进程与进程维度之间支持“and”、“or”、“not”等逻辑判断关系。用户可根据实际需要进行进程监控规则创建。 (11) 内存马： 支持定时和即时检测注入Java进程的内存马，包括 Filter、servlet、listener等内存马类型；支持JSP和agent注入两种检测引擎；agent注入支持无源检测和敏感操作检测，敏感操作检测可检测出有源木马。 (12) 告警与响应中心： 展示及处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件，并提供隔离、信任等功能；支持一键搜索主机及告警信息，此处支持搜索的信息包括：主机内外网IP、主机名、主机分组、主机标签、主机操作系统版本、主机备注；风险等级、事件类型、ATT&CK分类、攻击者IP；支持通过主机及告警等相关字段组合成条件进行逻辑关联以完成更复杂的告警数据过滤；支持对告警进行处置操作，包括：点击详情、导出、关闭或取消关闭事件、加入或者取消黑名单、加入白名单、信任或者取消信任、隔离或者取消隔离、禁用或者取消禁用、下载、复测扫描等。
		威胁情报	支持通过本地和云端威胁情报库数据进行匹配，捕

			获潜在的威胁信息，包括IP、C&C域名、hash值。支持情报类型、情报指标、命中次数以及威胁特征
		安全报表	可自定义时间区间分析生成全站攻击趋势、攻击类型分布、资产分布、漏洞风险分布、漏洞发现趋势、入侵威胁分布、入侵威胁发现趋势、新增监控异常分布、监控异常变化趋势等图表；
		服务成果	每周提供服务器主机防病毒处理报告。

4 安全保护-云 WAF 安全防护

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	云WAF 安全防护服务要求	(1) 安全防护范围： 南京市建邺区新一代电子政务外网网络信息系统 Web 服务互联网暴露面均应纳入云 WAF 进行安全防护。在远程云端对攻击流量进行监测和拦截，适用反向代理和域名访问方式的 Web 服务，提供不少于5个域名的防护服务。 (2) 安全防护频次： 对南京市建邺区新一代电子政务外网网络信息系统 Web 服务互联网提供实时安全防护。 (3) 安全防护服务形式：云 WAF 安全防护。
		云 WAF 防御功能要求	云WAF安全防护能力应不低于如下要求： (1) Web防火墙： 可防护 SQL 注入、命令注入、跨站脚本、文件包含、信息探测等常见攻击，防止网站因为漏洞导致被篡改，被拖库，被入侵。 (2) 防火墙策略集控制： 支持子防护策略集打开关闭；子防护策略集如下：政企专用防护策略集，扫描器/爬虫防御策略集，异常 HTTP 请求防御策略集，SQL 注入防护策略，POST 请求 SQL 注入防护策略，Webshell 防护策略，XSS 防护策略，POST 请求 XSS 防护策略，命令/代码执行防护策略，文件包含/注入防护策略，特殊/其他攻击防护策略。 (3) 防护策略屏蔽时间： 可以设置防火墙策略拦截的 IP 的屏蔽时间。 (4) 防火墙策略白名单： 对指定的 Web 防火墙策略不进行拦截。 (5) 智能攻击防御： 可精准识别多种自动化扫描和攻击软件，深度解析编码过的、畸形的恶意代码，并阻断其请求，减少90%以上的恶意攻击。

			(6) WebShell 防护： 可防止黑客上传、访问WebShell（网站后门）。 (7) 后台锁： 禁止非授权 IP 访问网站后台管理地址或重要页面。 (8) 防盗链： 保护网站图片、压缩包等资源文件不被其它站点盗用。 (9) URL 黑白名单： 不经过防护的 URL 地址（URL 白名单）、不允许访问的 URL 地址（URL 黑名单）。 (10) IP 地址黑白名单： 可设置不进行防护的 IP 地址（IP 白名单）、不允许访问的 IP 地址（IP 黑名单）。 (11) HTTP/HTTPS防护： 支持HTTP、HTTPS的业务防护，支持强制跳转 HTTPS。
		云 WAF 服务功能要求	(1) 可视化： 1) 网站概况显示： 提供网站访问情况信息展示，包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按照时间来统计的网站访问量。 2) 安全报告： 查看网站安全状况，包括各种攻击发生次数，攻击 IP、来源（国家）等；可显示对网站的安全评级，如安全、危险等等，可显示历史攻击次数等；可显示 CC 攻击详细情况。可显示攻击情况，包括时间、攻击 URL，攻击者 IP 及归属地，攻击类型等。提供一年内自定义报表功能。 3) 实时攻击显示： 提供实时攻击视图，在视图中实时显示攻击源IP，国家，目标域名，目标所在地等。 (2) 攻击预警： 提供按照攻击阈值设定攻击预警功能。 (3) 服务： 1) 数据下载： (a) 报表下载：默认支持当日、前一天、最近30天和最近一年的报表统计下载。 (b) 日志下载：提供攻击和访问日志自助下载服务。 2) 监管协助： 提供一键关停网站服务功能，用户需要事先在云 WAF 平台上认证手机。 3) 日志审计： 提供云 WAF 用户在平台上的操作日志和登录日志，并提供查询功能。

			4) SSL 节点 提供共享证书节点(sni方式,低版本浏览器会有告警) SSL 证书自助上传功能(pem格式,含证书和私钥)。
		安全报告	(1) 基础客服服务: 客服QQ在线支持、客服电子邮件服务、DNS网站接入。 (2) 在线服务: 5x8小时客服电话支持;5x8小时远程运维和操作、使用技术支持服务;5x8 小时指定客户经理远程技术支持服务。 (3) 人工报表服务: 每月定期提供综合报告分析,基于周期检测结果,输出检测报告,并提供趋势分析及建议,发送到客户指定邮箱。 (4) 人工查看、协助: 每周不定时查看网站防护情况,如有异常及时提醒,并协助与相关主管单位及时沟通解决异常情况。
		重点保障	在重大活动期间,提供相应的重点安全监测和保障。并根据要求提供相应的驻场服务。协助相关安全主管单位及时解决应急事件。
		服务成果	安全事件实时分析与处置;每月提供安全综合分析报告。

5 安全保护-本地 WAF 安全防护

序号	考核要求	功能、性能、配置要求	详细参数 (不低于以下要求)
1	★实质性要求	本地 WAF 安全防护服务要求	(1) 安全防护范围: 南京市建邺区新一代电子政务外网网络信息系统Web服务互联网暴露面均应纳入本地硬件WAF进行安全防护。 (2) 安全防护频次: 南京市建邺区新一代电子政务外网网络信息系统Web服务互联网实时安全防护。 (3) 安全防护服务形式: 本地硬件WAF安全防护。
		本地 WAF 防御功能要求	本地硬件WAF作为本地纵深防御机制重要措施,应与云WAF兼容。为保证本地WAF硬件高可用性,应配置不少于2台(含2台)硬件WAF,并采用负载均衡方式部署,单台硬件WAF安全防护能力应不低于如下要求: (1) 硬件要求: 专用Web硬件防火墙,非防火墙、UTM、IPS设备,标配

		千兆电口≥ 8个，冗余千兆电口≥ 2个，万兆光口≥ 2个，具备独立自主知识产权；冗余电源(至少双电源)；冗余BYPASS模块；支持扩展槽；支持冗余的管理口。 (2) 性能要求： 吞吐量≥ 20 Gbps；每秒最大事务处理数≥ 18万；最大并发数≥ 200万；每秒新建连接数≥ 9万。 (3) 部署模式： 支持透明直连模式、旁路镜像模式、反向代理模式。 (4) 高可用要求： 支持配置信息同步、透明代理支持主/主模式。 (5) 网络协议： 支持IPv4/IPv6协议双栈。 (6) 协议识别和解码： 支持http、https协议流量识别；具备http协议深层解码能力，支持递归解码，解码方式包括：Unicode解码、Base64解码。 (7) 过滤恶意访问请求： 能够抵御通用类型的SQL注入、文件包含、远程命令、WEBSHELL、XSS跨站、代码执行、文件注入等攻击威胁。 (8) 黑白名单设置： 1) 支持自主设置特定IP的WAF拦截要求，并支持自主设置WAF拦截IP白名单； 2) 能够对指定IP进行屏蔽时长设置，以分钟为单位。 3) 能够识别Web攻击者的IP所在地区，如是境外IP，可限制境外IP访问，并支持设定限制时间。 4) 能够按照访问时间（设置夜间模式/自定义）进行防御，允许或者阻止一定时间段内的访问。 (9) 弱口令检测： 支持登录、注册接口弱口令检测。 (10) 拟态防御： 支持模拟不同的动态请求访问交互模式实现拟态防御效果，进而迷惑攻击者使其无法形成实质有效攻击。 (11) 前置防御： 支持浏览器安全检查，对首次访问业务系统的客户端浏览器进行全方位安全检查。 (12) 自定义策略： 可以自定义的策略至少包括：扫描器/爬虫防御，异常HTTP请求防御，SQL注入防护，POST请求SQL注入防护，Webshell防护，XSS防护，POST请求XSS防护，命令/代码执行防护，文件包含/注入防护等。 (13) 协同防御：
--	--	---

			当网站部分站点遭受攻击时，能够防御攻击者对其他域名或站点的攻击，具备一定的协同防御能力。
		本地 WAF 服务功能要求	(1) 管理页防护： 1) 能够定义给定的URL作为网站后台管理页面，允许特定IP进行访问，同时可以对URL访问进行限速。 2) 能够缓存特定页面，在网站出现故障时进行展现，保障网站持续在线。 3) 能够支持端口设置功能，进行支持配置80、443端口以外的端口及端口转发策略。 4) 通过https方式提供Web配置管理界面，保证自身安全性。 (2) 可视化： 1) 提供查看网站安全状况，包括各种攻击发生次数，攻击IP、来源（国家）等； 2) 实时获取网络攻击行为，实时发现、分析、报警；展示内容包括攻击的具体来源、IP地址、所属国家（地区）并标示攻击类型。 (3) 系统管理： 1) 支持多等级权限账号系统，支持基于不同功能组合的账号角色； 2) 显示实时网络接口状态，引擎状态、系统CPU、内存及磁盘使用率。
		服务成果	安全事件实时分析与处置；每月提供安全综合分析报告。
2	非实质性要求	不低于以下要求： (1) 本地硬件WAF均应支持语义分析自定义语义引擎白名单功能，支持通过规则、URL参数、IP地址、Webshell上传防护、XXE、SQL、PHP反序列化、PHP代码注入、命令注入、XSS、后门扫描方式精细化排除。 (2) 本地硬件WAF均应支持业务学习参数防护：支持参数防护，支持主动防护，学习访问HTTP的请求参数，总结出参数的路径、变量名、变量类型、长度范围、支持自定义参数防护。	

6 安全保护-DNS 云解析及防护

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	DNS云解析及防护服务要求	(1) DNS云解析及防护范围 南京市建邺区新一代电子政务外网网络信息系统Web

			服务互联网暴露面均应纳入。 (2) DNS云解析及防护频次 DNS云解析及防护平台实时防护。 (3) DNS云解析及防护服务形式 DNS云解析及防护平台实时服务。 (4) DNS 云解析及防护内容要求 DNS云解析及防护服务许可1年，满足南京市建邺区新一代电子政务外网所有域名的解析及防护需求。 (5) 具体功能、性能、规格要求不低于如下要求： 1) 可用性SLA： 100%月度可用性。 2) DNS 节点： 中国及境外 DNS 节点≥ 10个。 3) TTL值： 1秒。支持智能解析。 4) 线路类型切换： 支持运营商线路与地域线路切换。 5) URL转发： 不低于10条（含10条）。 6) 负载均衡： 不低于100条（含100条）。支持宕机自动切换，支持多节点访问。 7) 解析记录： 支持A、CNAME、AAAA记录。 8) 解析记录备份： 支持最短周期按天备份。 9) DNS攻击安全防御： 针对云解析 DNS 实例已绑定的域名，提供针对域名的DNS 攻击防御，每个域名的攻击防御能力超过亿次，保障DNS 在洪水 QPS 攻击下正常解析。
		服务成果	DNS云解析及防护服务生效。

7 安全保护-蜜罐防护

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	蜜罐防护服务要求	(1) 防护范围： 覆盖建邺区核心业务系统，包括但不限于协同OA系统、移动政务平台、钉钉云枢、智慧食堂系统等业务。可根据实际防护需求，添加防护范围。 (2) 防护频次：

			实时监测与诱捕 (3) 服务形式: 通过高仿真沙箱与蜜罐技术构建更为主动的安全防御体系,保障建邺区核心业务系统安全运行。 可通过告警短信等方式实时通知安全管理员,争取应急响应时间,从而降低信息资产受损的风险。
		蜜罐防御功能要求	(1) 业务仿真: 1) 默认仿真蜜罐: 支持至少10种可自定义logo和公司名称的仿真蜜罐,仿真蜜罐类型包括但不限于:“齐治堡垒机、启明堡垒机、深信服VPN、泛微OA、通达OA、u8crm、wiki、mailcow、bbs论坛、订单管理系统”。 2) 完全仿真蜜罐: 支持通过反向代理的方式,接入用户自身搭建的应用系统,生成完全仿真蜜罐(签订合同时,提供由厂商盖章确认的产品界面截图证明)。 3) 钓鱼邮件演练: 可在平台中统计打开钓鱼邮件的账号、点击连接的账号、提交敏感数据的账号等数据,统计维度包括账号名称、访问ip、提交敏感数据内容、访问时间等。 (2) 攻击吸引: 引流防御:可将访问真实业务系统的流量引流到仿真蜜罐,使攻击无法命中真实业务系统。 (3) 威胁感知: 1) 入侵攻击链检测: 参考MITRE ATT&CK,还原黑客攻击入侵蜜罐的过程,形成黑客攻击链,包含:“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远程控制程序、利用蜜罐进行跳板攻击”等入侵过程。 2) 还原攻击数据包: 支持还原攻击者的网络数据包,包括icmp、tcp、udp等协议的攻击包,可查看攻击者发起的具体攻击请求数据,比如SQL注入、XSS攻击的http请求头部信息。 3) 时间轴告警: 支持时间轴告警分析:可根据基于告警时间/攻击类型/地理位置等对攻击行为进行筛查,其中攻击类型可分类为:“可疑访问、尝试登陆、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登陆成功、命令执行、可疑文件、恶意文件、跳板攻击”等类型。 (4) 溯源反制: 1) 攻击者社交信息溯源:

			支持记录攻击者的“黑客社交画像”信息，包括社交账号、昵称、头像等信息，比如溯源百度等不同类型的社交账号。 2) 攻击者指纹溯源： 设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型、mac地址、设备厂商、屏幕分辨率，浏览器历史记录、计算机名、显卡成像参数、CPU等硬件信息。 位置信息溯源至少包括：真实攻击IP（攻击者拨VPN也可获得真实攻击IP）、代理转发前的IP地址、IP地理位置、经纬度。 3) 威慑反制： 可灵活指定对某个攻击源IP地址发起威慑反制，比如灌输国家网络安全法、告知已获得相关溯源信息，发挥互联网攻击监测诱饵威慑作用，使攻击者放弃后续的攻击行为。 4) 拒绝服务反制： 可使攻击者浏览器拒绝服务，可灵活指定对某个攻击源IP地址发起拒绝服务反制。 5) 木马诱骗反制： 可使攻击者下载某个文件时，替换成木马文件，诱骗攻击者下载安装；可在web管理界面上灵活指定对某个攻击源IP地址发起木马远控反制。 6) 漏洞攻击反制： 支持一键扫描攻击源IP地址，探测攻击者主机的开放端口信息、弱口令、漏洞等。
		蜜罐服务功能要求	(1) 职责分离： 提供超级管理员、管理员、普通用户、审计员角色权限。支持生成html、doc、pdf、excel等格式的分析报告。 (2) 可视化： 支持大盘展示受攻击资产、探测与入侵事件统计、受攻击沙箱等。 (3) 告警推送： 支持至少四种方式的告警推送，包括但不限于：邮件、钉钉、企业微信、飞书。 (4) 联动防御： 可搭配组件实现与第三方品牌防火墙进行联动实现自动封禁IP。
		服务成果	每月提供安全攻击事件分析报告。

8 安全保护-安全堡垒机

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	安全堡垒机防护服务要求	(1) 安全防护范围： 南京市建邺区新一代电子政务外网服务器主机应纳入安全堡垒机防护。 (2) 防护频率： 安全堡垒机实时防护。 (3) 防护内容要求： 软件堡垒机授权1年1套，形态为安全堡垒机信创版本软件，支持纳管主机数量不低于1000台。
		安全堡垒机防御功能要求	(1) 部署环境： 堡垒机信创版本，支持部署南京市建邺区新一代电子政务外网阿里云平台，支持部署在国产信创操作系统（包括但不限于龙蜥、麒麟等），支持纳管主机数量不低于1000台，支持纳管信创主机、经检测认证的国密密码产品且安全等级为2级及以上 (2) 角色管理： 1) 默认支持超级管理员、配置管理员、审计管理员、自动化管理员及操作员等角色。 2) 根据工作实际需要，能够支持自定义用户角色名称，并且可以将超级管理员、配置管理员、审计管理员、自动化管理员及操作员角色具备的权限进行组合后赋予这个角色。 (3) 身份认证： 1) 支持本地密码、AD/LDAP、RAOIUS、动态令牌、手机令牌、USBKey、短信、X.509等认证方式，并且可以将两种认证方式自定义组合为全新的认证方式（如本地密码+手机令牌）。 2) 支持AD账号的定期自动化同步，当AD域中的账号有变更时，会被自动同步的系统中，并加入预定义的用户分组。 (3) 账号安全： 1) 支持基于时间、IP地址、MAC地址进行用户登录控制。 2) 具有防暴力猜测功能，支持密码错误锁定、客户端锁定（基于同一客户端不同账号登录失败次数），可以设置锁定时长。 (4) 资源类型：

			支持对windows、linux、unix、龙蜥、麒麟、网络及安全设备、数据库以及各类B/S应用的管理。支持信创服务器、网络设备、安全设备、数据库、及各类B/S应用的管理。 (5) IPv6管理： 产品支持IPv6设置；支持管理IPv6资产。 (6) 访问权限： 1) 支持以用户（用户组）、目标设备（设备组、程序）、系统账号、服务等维度灵活设置访问策略。 2) 支持动态权限管控，管理员可基于用户、资产、协议和账号来创建弹性动态权限规则，只要满足相关属性的用户、资产、协议和账号即会被自动赋予对应访问权限。 (7) 权限查看： 支持按用户展示可管理资产、按资产展示有权限访问的用户账号。 (8) 密码管理： 支持系统账号密码触发式校验功能，对托管的口令进行验证。支持自动改密功能，管理员可自定义密码策略、改密周期、密码备份方式。 如需要临时使用被管理设备的密码，可以通过密码申请工单申请，填写需要使用密码的开始、结束时间，支持通过密码分段将密码分为2段分别发送给不同的管理员用户。 (9) 资源访问： 1) 支持批量启动功能，可一次性登录选择好的多个目标设备。 2) 支持设备收藏功能，用户可以对经常需要访问的目标设备做一键收藏，以便于下次可以直接在收藏夹中找到。 3) 支持基于云盘模式的文件向linux系统传输和下载文件：用户将文件暂存在系统上，再经由系统，一键上传到目标系统或者一键下载到用户本地。 4) 支持对传输文件的大小进行配额限制。
		安全堡垒机服务功能要求	(1) 图形审计： 1) 能够实时显示在线会话、在线字符会话、在线图形会话、在线数据库会话数量，能够直接点击查看审计会话。 2) 能够实时显示在线资产和在线用户数量，能够直接点击查看在线资产和用户信息。 3) windows系统在登录前，能够查看目前在线运维会话数量。

			4) 支持开启或者关闭键盘记录。 5) 支持图形会话无操作超时自动切断会话，可以设置超时时间。 6) 支持设置某个图形会话操作的最大持续时间，超时自动切断会话。 (2) 字符审计： 1) 确保对各种非常规指令操作的100%识别，特别是TAB补全、长命令的行内编辑、上下箭头等操作。 (3) 数据库审计 由于实际业务中数据库操作比较频繁，需要根据任意sql语句中的内容为关键字进行会话查询，查询结果可直接定位到相关操作画面。 (4) 审计分析： 1) 支持运维数据风险直观展示，能够以topN方式展示TOP资产、TOP用户和TOP敏感操作。 2) 支持以1M-10M大小对图形会话进行切片展示功能，管理员点击任意切片，即可直接定位到对应操作片段。 (5) 系统维护： 1) 支持在WEB页面查看所有进程状态，能够显示每个进程的内存占用及CPU使用率。 2) 可以在全局模式下设置会话占用系统资源限制，如图形会话、字符会话、数据库会话占用系统CPU、内存负载限制；也可以按照单会话，设置普通用户和VIP用户对CPU、内存负载限制。 3) 支持选择天数后一键采集系统日志。 (6) 质保要求： 供应商须承诺如中标，须提供1年原厂质保服务。(注：须提供承诺函并加盖公章，承诺函格式自拟)
2	非实质性要求	安全堡垒机功能	(1) 堡垒机应支持权限查看： 支持按用户展示可管理资产、按资产展示有权限访问的用户账号。 (2) 新增部署堡垒机应支持数据库审计： 由于实际业务中数据库操作比较频繁，需要根据任意sql语句中的内容为关键字进行会话查询，查询结果可直接定位到相关操作画面。

9 安全检测-安全漏洞扫描

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	安全漏洞扫描服务要求	(1) 扫描范围 南京市建邺区新一代电子政务外网（公共网络区、互联网络区）相关设备及系统 (2) 扫描频次 一年六次，每2月一次。 (3) 漏洞扫描服务形式 现场安全漏洞扫描。 (4) 扫描要求 中标供应商自带漏扫设备进行主机、数据库、web 系统安全扫描，漏扫设备应满足：漏扫设备漏洞库应包含 CVE、CNNVD、CNVD 等类型的漏洞库漏洞；漏扫设备具备服务器、网络设备、数据库、中间件、web应用扫描能力；漏扫设备具备并发扫描能力；漏扫设备支持国产 OS、国产数据库、国产中间安全漏洞扫描；漏洞扫描设备支持导出漏洞扫描报告。 1) 主机安全扫描：通过专业扫描工具对指定主机系统进行技术脆弱性扫描(含端口、弱口令扫描等)，发现主机系统中存在的安全弱点。 2) 数据库安全扫描：通过专业扫描工具（安全服务提供商提供漏扫工具）对指定数据库进行技术脆弱性扫描，发现数据库中存在的弱点。 3) Web系统安全扫描：通过专业扫描工具（安全服务提供商提供漏扫工具）对指定Web系统进行技术脆弱性扫描，发现Web系统中存在的安全弱点。 通过分析上述安全扫描结果，对指定信息系统的威胁、技术脆弱性等风险构成因素进行综合分析和评定，并提供针对性的整改建议及协助加固。
		服务成果	每次扫描分类提供《漏洞扫描评估报告》。

10 安全检测-安全渗透测试

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	安全渗透测试服务要求	(1) 扫描范围： 南京市建邺区新一代电子政务外网（公共网络区、互联网络区）相关设备及系统。 (2) 扫描频次：

			一年四次，每3月一次。 另可根据实际需求，按需不限次数渗透测试。 (3) 漏洞扫描服务形式： 南京市建邺区新一代电子政务外网管理单位指定现场或远程安全渗透测试。 (4) 扫描要求： 对南京市建邺区新一代电子政务外网网络平台、网站群和重要信息系统进行渗透测试，通过对系统的弱点、技术缺陷或漏洞的主动分析，对信息系统进行模拟攻击测试，分析系统的安全风险和应对措施。通过渗透测试、安全修复、回归性测试进行网络平台、网站群和重要信息系统安全漏洞的闭环管理，从而提高上述平台系统的安全性，降低出现安全事件的风险。
		服务成果	每次渗透测试分类提供《渗透测试报告》，提供解决建议及协助加固。

11 安全检测-日志管理

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	日志管理服务要求	(1) 日志管理范围： 南京市建邺区新一代电子政务外网内所有跨边界流量日志均应纳入集中式日志管理平台进行统一采集和管理。 (2) 日志管理频次： 南京市建邺区新一代电子政务外网跨边界流量日志实行实时采集、实时存储。 (3) 日志管理服务形式： 通过集中式日志管理平台提供统一的日志采集、存储、分析和管理服务。
		日志管理服务功能要求	(1) 硬件指标： 6个千兆电口，2个扩展插槽，1个Console接口，2TB硬盘。 (2) 性能指标： 综合日志处理性能2600EPS，日志采集处理均值7000EPS，不低于35个日志源授权，提供一年以上的硬件维保服务和软件升级维护服务

12 安全检测-违规外联安全检测

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	违规外联安全服务要求	(1) 违规外联服务范围： 南京市建邺区新一代电子政务外网 (2) 防护频次： 实时监测 (3) 服务形式： 为有效防范政务外网违规外联行为，确保建邺区数治中心的公共区网络安全，部署一套违规外联防控系统。对政务外网公共区的所有连接进行实时监控，自动识别私接网线、无线网卡及非法远程桌面操作等违规行为。
		违规外联安全服务功能要求	(1) 硬件规格： 软硬一体国产化设备，配置不低于6个（含6个）千兆电口。内存不低于16GB。 (2) 部署模式： 支持旁路部署，接入交换机trunk流量。 (3) 安全防护： 1) 支持端口汇聚或独立网段工作模式； 2) 支持多节点性能监控、状态监控、升级管理、一键登录等的统一管理。 3) 支持多节点数据采集汇总展示、数据分析的数据汇聚应用。 4) 支持多节点资产管控策略匹配分析后统一下发。 5) 支持对全网不低于1000个入网资产进行发现、识别，建立监测网络内的资产信息库，实现对资产的在网状态、开放的端口、服务、应用等信息进行全时监测。 6) 支持资产快照采集能力，对入网资产生命周期中信息进行相应的具象展示；（签订合同时提供功能截图证明并加盖公司公章）。 7) 支持采用非侵入式的监控模式，无需部署客户端、改造网络和应用，不间断对全网私自搭建的不受控网络边界进行监控。 支持对私自搭建的连接互联网等外部不受控网络的网络边界和通道进行监控； 8) 支持对私自搭建的连接专网等内部网络的网络边界和通道进行监控。 9) 支持对接网络设备snmp信息，绘测入网资产拓扑图，提供资产的网络链路信息，实现快速资产定位。 10) 支持旁路管控方式对风险资产实现网络访问控制。 11) 支持交换机ACL管控方式对风险资产实现网络访问控制。

			12) 支持发现和定位网内私自接入的二层设备, 如傻瓜交换机、HUB等设备。支持对多级串接傻瓜交换机或HUB设备场景下违规串网外联的管控。
--	--	--	---

13 安全响应与恢复-安全威胁监测综合分析

序号	考核要求	功能、性能、配置要求	详细参数（不低于以下要求）
1	★实质性要求	安全威胁监测综合分析服务要求	(1) 服务范围 南京市建邺区新一代电子政务外网信息资产。 (2) 服务频次: 7*24小时。 (3) 服务地点: 现场驻场。 (4) 服务要求 对南京市建邺区新一代电子政务外网进行安全运维, 南京市建邺区新一代电子政务外网所有安全技术手段的安全告警分析与处置, 南京市建邺区新一代电子政务外网所有安全技术手段每日巡检, 安全事件7*24小时应急响应及恢复, 7*24小时安全值守, 安全威胁监测与预警, 安全事件调查、溯源、影响分析, 安全风险专项排查, 重大活动及重要时期网络安全重点保障组织、协调与实施, 南京市建邺区新一代电子政务外网业务单位安全风险整改协助、复核、闭环跟踪管理, 协助南京市建邺区新一代电子政务外网网络安全管理单位开展网络安全管理工作。 (4) 服务成果 安全巡检日报、设备安全告警事件分析处置日报, 及其他相关工作报告(按需)。
		服务成果	安全巡检日报、设备安全告警事件分析处置日报。

附件三 交付一览表

项目名称		JSZC-320105-SJGC-C2025-0013		项目编号	JSZC-320105-SJGC-C2025-0013
服务企业名称		南京大数据安全技术有限公司		服务企业地址	南京市建邺区永初路8号阿里中心T4栋1208室
序号	服务名称	数量	交付成果		
1	安全识别-基线核查服务	1套	服务期内提供《建邺数治中心信息系统资产清单》《建邺数治中心信息系统风险管理报告》，每季度更新一次。		
2	安全识别-安全威胁分析技术服务(互联网区)	1套	服务期内每日提供《建邺区数治中心安全日报》		
3	安全识别-安全威胁分析技术服务(公共区)	1套	服务期内每日提供《建邺区数治中心安全日报》		
4	安全保护-服务器主机防病毒	1套	服务期内每日提供《建邺区数治中心安全日报》		
5	安全保护-云WAF安全防护	1套	服务期内每日提供《建邺区数治中心安全日报》		
6	安全保护-本地WAF安全防护	2套	服务期内每日提供《建邺区数治中心安全日报》		
7	安全保护-DNS云解析及防护	1套	服务期内每日提供《建邺区数治中心安全日报》		
8	安全保护-蜜罐防护	1套	服务期内每日提供《建邺区数治中心安全日报》		
9	安全保护-安全堡垒机	1套	服务期内每日提供《建邺区数治中心安全日报》		
10	安全检测-安全漏洞扫描	1套	服务期内至少出具6份《建邺区数治中心XXX系统漏扫报告》，每两个月一次		
11	安全检测-安全渗透测试	1套	服务期内至少出具4份《建邺区数治中心XXX系统渗透测试报告》，每三个月一次		
12	安全检测-违规外联安全检测:	1套	服务期内每日提供《建邺区数治中心安全日报》		
13	安全检测-日志管理	1套	服务期内每日提供《建邺区数治中心安全日报》		

14	安全响应与 恢复-安全威 胁监测综合 分析	1套	服务期内按需提供《建邺区数治中心XXXX事件分析调查报告》
----	--------------------------------	----	-------------------------------

附件四 投标（响应）承诺

一、供应商信用承诺函

供应商信用承诺函

致：南京市建邺区城市数字治理中心

江苏苏建工程项目管理咨询有限公司

我公司 南京大数据安全技术有限公司（供应商名称）郑重承诺：

我公司符合下列要求：

- （一）具有独立承担民事责任的能力；
- （二）具有良好的商业信誉和健全的财务会计制度；
- （三）具有履行合同所必需的设备和专业技术能力；
- （四）有依法缴纳税收和社会保障资金的良好记录；
- （五）参加政府采购活动前三年内，在经营活动中没有重大违法记录。

如果我公司成交，将在成交结果公示后七个工作日内向代理机构和采购人提供下列材料核验：

- （1）营业执照副本或事业单位法人登记证书；
- （2）参加本次政府采购活动前一年的经审计的财务报告（包括“四表一注”，法人成立满一年的提供）或参加本次政府采购活动前一年内的银行资信证明（法人或其他组织提供）或其他证明材料；
- （3）履行合同所必需的设备和专业技术能力证明材料；
- （4）参加本次政府采购活动前一年内至少一个月依法缴纳税收和社会保障资金的证明材料。

本公司对上述承诺内容的真实性、合法性、有效性负责，如有虚假，将依法承担相应责任。

供应商名称：南京大数据安全技术有限公司（加盖电子公章）

日期：2025年12月15日



附件五 服务承诺

服务承诺书

为切实保障政务数据安全与服务质量，维护采购人合法权益，本公司作为专注于大数据安全领域的技术服务机构，严格遵循国家法律法规及《南京市政务数据安全实施管理实施细则》要求，现就服务相关事项郑重承诺如下：

一、合规经营承诺

1. 我司严格遵守《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》等国家及地方相关法律法规、行业标准与监管要求，所有服务活动均以合法合规为前提，杜绝任何违法违规处理数据及网络安全服务的行为。

2. 我司具备开展相关服务的完整资质，包括信息安全管理证书ISO/IEC 27001:2022、信息技术服务管理体系认证证书ISO/IEC 20000-1:2018、质量管理体系认证证书GB/T 19001-2016/ISO 9001:2015、环境管理体系认证证书GB/T 24001-2016/ISO 14001:2015、ITSS三级-运行维护、CCRC安全运维三级、CCRC安全集成三级等资质证书，确保服务主体合法、资质齐全、能力达标。

3. 我司承诺服务过程中严格遵循合同约定及行业规范，不超出授权范围开展服务，不擅自收集、使用、存储、传输贵方及相关数据主体的信息，坚守数据处理“合法、正当、必要”原则。

二、数据安全与保密承诺

1. 我司对服务过程中接触、获取的贵方所有数据信息（包括但不限于业务数据、客户信息、技术文档、系统配置、密钥证书等）严格保密。

2. 我司为履行本次服务合同之目的使用贵方数据，未经贵方书面授权，绝不擅自复制、传播、转让、披露或用于其他任何商业或非商业用途。服务结束后，按照贵方要求，对留存的贵方数据进行彻底销毁或返还，不留任何副本。

4. 与所有参与服务的员工签订保密协议，定期开展数据安全与保密培训，提升全员保密意识与操作规范；严禁员工以任何形式泄露、传播、倒卖贵方涉密信息，若发生内部泄密，将依法追究相关人员责任。

5. 若服务涉及数据跨境传输，将严格履行安全评估、备案等法定程序，确保符合国内监管要求；服务终止后，按贵方要求及法定标准彻底销毁或返还所有贵方数据及载体，出具数据销毁/返还确认报告，杜绝数据残留风险。

三、服务质量与技术保障承诺

1. 依托我司拥有平台、专利以及专业的技术团队，为贵方提供高质量的安全服务，包括但不限于安全咨询、系统加固、应急响应、安全运维等，确保服务效果达到合同约定及行业标准。

2. 建立7×24小时服务响应机制，贵方提出服务需求或故障告警后，30分钟内完成响应；需现场支持的，4小时内抵达现场，偏远地区8小时内抵达现场，简单问题当日解决，复杂问题48小时内出具解决方案并同步贵方。

3. 制定完善的数据安全事件应急预案，明确上报路径、处置流程及责任分工；若发生数据安全事件或系统故障，将第一时间启动应急响应，全力处置并溯源分析，及时向贵方通报进展，采取补救措施防止类似事件复发。

4. 定期开展服务复盘与质量评估，每季度向贵方提交服务报告，反馈服务开展情况、风险隐患及优化建议；根据法律法规更新、行业技术迭代及贵方需求变化，及时调整服务方案与防护措施，持续提升服务质量与安全保障能力。

四、监督与责任承担承诺

1. 主动接受贵方及相关监管部门的监督、检查与审计，如实提供服务记录、安全报告、资质文件等相关资料，积极配合核查工作，对发现的问题及时整改。

2. 若我司违反本承诺书及合同约定，导致贵方遭受数据泄露、财产损失、声誉损害等后果，将依法承担全部法律责任，包括但不限于消除影响、赔偿全部损失、接受行政处罚等；若因违约行为导致服务无法继续，我司将按合同约定承担相应的解约责任及赔偿义务。

3. 指定专门部门负责数据安全与服务质量管控，每季度开展内部合规审计与服务质量自查，及时调整管理制度与服务流程，确保始终符合法律法规及本承诺书约定。

五、其他承诺

未经采购人书面同意,不向任何第三方泄露本项目涉及的采购人资料或我方服务细节;若发生违约,立即终止行为并支付违约金,赔偿采购人全部损失。

本合同项下双方权利义务不因合并、分立、重组等情形变更;如因上述情形导致主体变更,权利义务由承接方承继,我方配合完成交接。

保证采购人使用本项目服务时,不会因知识产权瑕疵被第三方主张权利;若出现侵权纠纷,由我方承担全部责任(包括但不限于诉讼费、赔偿金、律师费)。

项目中使用的第三方软件、技术等知识产权,我方确保拥有合法所有权、使用权或分许可权,不侵犯任何第三方权益;若因第三方权利主张导致采购人受损,我方负责解决并全额赔偿。

我司将严格恪守上述承诺,以专业能力、严谨态度履行服务职责,全力保障贵方数据安全与合法权益。

附件六 中标（成交）通知书

成交通知书	
JSZC-320105-SJGC-C2025-0013	
采购人	南京市建邺区城市数字治理中心
项目名称	智慧建邺网络信息系统安全运维服务项目
成交供应商	南京大数据安全技术有限公司
成交金额	(小写): ¥776000.00
	(大写): 柒拾柒万陆仟元整
采购方式	竞争性磋商
服务期限	自安全服务相关技术手段在建邺区完成部署并具备安全服务能力并获得采购人确认起一年。
项目实施地点	采购人指定地点。
江苏苏建工程项目管理咨询有限公司 2025年12月23日	
注: 本书一式叁份, 采购人、成交供应商、代理机构各执壹份	

附件七 项目考核办法

服务开始后，每月进行服务考核，考核总金额为合同总金额的60%。根据考核结果计算每月的服务质量考核款（每月服务质量考核款最高为合同总价的 5%）。
 考评条件如下：（1）全月考核总得分小于 80，扣除 100%的服务质量考核款；
 （2） $80 \leq$ 全月考核总得分 <90 ，扣除 50%的服务质量考核款；（6） $90 \leq$ 全月考核总得分，支付全部的服务质量考核款。

项目考核办法（月度）			
考核周期：项目服务期内按月度进行考核			
评分项	内容	评审标准	分值
服务内容要求	1、制定并提供完善的《安全配置基线规范》，每月开展安全基线核查。 2、在南京市建邺区新一代电子政务外网出口节点旁路部署态势感知设备，并及时处置政务外网公共区、互联网区出口态势感知设备发出的告警信息。 3、在南京市建邺区新一代电子政务外网互联网侧部署高仿真业务蜜罐，并及时处置蜜罐设备的告警信息。 4、开展网络安全规划、网络安全建设方案咨询、网络安全管理咨询工作，根据需求输出《现状调研报告》、《网络信息安全发展规划》、《网络安全相关管理制度》等文档。 5、在指定设备上部署主机安全（EDR）agent，及时处置入侵风险并至少组织一次全量的病毒、木马查杀工作。 6、将南京市建邺区新一代电子政务外网互联网web服务纳入云 WAF 保护范围之内。 7、南京市建邺区新一代电子政务外网网络中部署本地WAF，将南京市建邺区新一代电子政务外网网络信息系统 Web 服务互联网暴露面纳入本地硬件 WAF 进行安全防护范围。 8、购买云解析DNS及防护服务许可1年。 9、部署违规外联安全检测设备，并及时处置设备的告警信息。 10、延期南京市建邺区新一代电子政务外网现网云平台堡垒机维保服务1年。 11、每两个月进行一次全量的漏洞扫描工作，提供总计6份《漏洞扫描评估报告》，并协助整改。 12、每三个月进行一次业务系统渗透测试工作，	每有1个点未达到内容要求扣4分，本项最多扣40分。	40

	提供总计4份《渗透测试报告》，并协助整改。 13、专人每日对南京市建邺区新一代电子政务外网所有安全技术手段的安全告警进行分析与处置，协助安全管理并出具《安全运维服务日报》，网络安全事件应急处置。		
安全事件通报	省、市级以上的中高危及以上网络安全事件有效通报数量	本项最高扣30分： 安全漏洞通报： 1、每有1个省级及以上高危有效通报扣20分，每有1个省级及以上中高危有效通报扣15分，最多扣30分。 2、每有1个市级高危有效通报扣20分，每有1个市级中高危网络安全事件通报扣10分，最多扣30分。 安全事件通报： 1、每有1个省级及以上高危有效通报扣30分，每有1个省级及以上中高危有效通报扣20分，最多扣30分。 2、每有1个市级高危有效通报扣30分，每有1个市级中高危网络安全事件通报扣15分，最多扣30分。 高危网络安全事件：造成重要网络和信息系统的特别严重的系统损失，系统大面积瘫痪，丧失业务处理能力的； 中高危网络安全事件：重要网络和信息系统的严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响的。	30
项目进度	1、根据甲方进度要求及时完成安全服务技术手段部署并维护其正常运行。 2、按甲方进度要求及时开展安全服务工作。 3、及时支持甲方安全事件处置，及时跟踪安全问题/漏洞复核进度。 4、按照甲方统一进度要求，按时提供各类服务成果文档。	每有一项未满足进度扣2分，最多扣20分	20
文档质量	1、按甲方进度要求出具统一格式的相关成果文档。 2、文档中若包含安全问题/漏洞，应提供对应的举证、描述及处置建议等信息。	每有一份文档未满足质量要求扣1分，最多扣10分	10
月度综合评分合计			100

附件八 团队人员及社保证明

11.3. 团队人员：

序号	职务	姓名	资格证书	职称
1	技术负责人	刘冬冬	注册渗透测试工程师（CISP）、中级网络工程师	中级
2	工程师	王从飞	注册信息安全工程师（CISP）	
3	工程师	于继武	注册信息安全工程师（CISP）	
4	拟驻场人员	彭凡	注册信息安全工程师（CISP）	
5	工程师	王茂	注册信息安全工程师（CISP）	
6	拟驻场人员	何文杰	注册信息安全工程师（CISP）	
7	工程师	孟子文	注册信息安全工程师（CISP）	

11.3.1. 社保证明

江苏省社会保险权益记录单
(参保单位)



请使用官方江苏智慧人社APP扫描验证

参保单位全称： 南京大数据安全技术有限公司 现参保地： 建邺区
统一社会信用代码： 91320104MAC1NR1G0B 查询时间： 202505-202511

共1页，第1页

单位参保险种		养老保险	工伤保险	失业保险
缴费总人数			30	30
序号	姓名	公民身份号码(社会保障号)	缴费起止年月	缴费月数
1	彭凡	321322199502248833	202505 - 202511	7
2	王从飞	320721199804185414	202505 - 202511	7
3	何文杰	320106200004112013	202505 - 202511	7
4	于继武	320106198804202017	202505 - 202511	7
5	孟子文	320322199610161128	202505 - 202511	7
6	李子熙	440106200011094412	202506 - 202511	6
7	刘冬冬	342522199711283614	202506 - 202511	6
8	王茂	321321199208020014	202505 - 202511	7

- 说明：
- 1. 本权益单涉及单位及参保职工个人信息，单位应妥善保管。
 - 2. 本权益单为打印时参保情况。
 - 3. 本权益单已签具电子印章，不再加盖鲜章。
 - 4. 本权益单记录单出具后有效期内（6个月），如需核对真伪，请使用江苏智慧人社APP，扫描右上方二维码进行验证（可多次验证）。



附件九 甲乙双方商定的其它文件

信息安全保密协议

甲方：南京市建邺区城市数字治理中心

乙方：南京大数据安全技术有限公司

鉴于应用系统实施信息系统风险评估和等级保护测评，需提供相关文档资料，现就文档资料使用所涉及的保密信息达成以下一致：

在本协议中，“保密信息”指：

- 1) 甲方提供给乙方的一切非公开技术和非技术信息，包括网络拓扑结构、业务流程、商业理念、网络安全机制、网络设备、网络方案，以及其他任何乙方无权向第三方泄露的信息。
- 2) 乙方的评估测评流程、评估问卷、文档等，任何甲方无权向第三方泄露的信息。

1. 权利保证：

甲乙双方均保证提供的信息不侵犯任何第三方的知识产权及其它权益。

2. 保密义务：

- 1) 甲乙双方统一严格控制获得的专有信息，保护的等级不能低于对于本方专有信息的保护等级。并且无论如何，对专有信息的保护等级不能低于管理良好的技术企业对自身专有信息的保护等级。

透露的专用信息只能被用于评价系统安全性；

不能将透露的专有信息用于其它任何目的；

除领导和直接参与本项工作的普通职员之外，不能将专有信息透露给其它任何人；

- 2) 无论如何，不能将专有信息的全部或部分进行复制或仿造
- 3) 甲乙双方保证采取所有必要的方法对获得的专有信息进行保密，包括（但不限于）执行和坚持令人满意的作业程序来避免非授权透露、使用或复制专有信息。
- 4) 甲乙双方保证不向任何第三方透露本协议的存在或本协议的任何内容。

5)告知并以适当方式要求参与本项工作之雇员遵守本协议规定,若参与本项工作之雇员违反本协议规定,应承担连带责任。

3. 专有信息的交回:

1)当任何一方以书面形式要求另一方交回专有信息时,应当立即交回所有书面的或其他形式的专有信息以及所有描述和概括该专有信息的文件。

2)没有消息来源方的书面许可,另一方无权处分任何书面的或其他有形专有信息。

4. 乙方只在风险评估和等保测评需要时才使用甲方的保密信息。绝不因与该评估测评项目无关的目的使用保密信息。

5. 乙方承诺将保密信息的使用限制在乙方工作人员范围内。

6. 乙方在本承诺中承担的保密信息的保密义务在下述情况下将被终止:

1)甲方在提供给乙方时已经是公开的信息;

2)甲方在提供给乙方后由于甲方的过错而变成公开信息的信息;

3)甲方在提供给乙方时,乙方已合法获得的信息;

4)乙方通过其他合法途径获得的信息。

7. 从甲方获得所有保密信息,乙方只有使用权,没有所有权、知识产权及解释权。

8. 如果有关权威机构认定本承诺的条文无法履行或者无效,且不是本承诺整体无法履行或者无效,在此情况下,只能修改该条文,并将这种改动解释为在适用法律或适用法庭判决的范围内实现该无法履行或无效条款预定的目标。

9. 对于本协议条款的修改,只有经双方授权的代表书面签署协议后方可生效并对双方具有约束力。

10. 本承诺所要求的或允许的所有通知和报告均以书面为准,且必须由专人送达或经电子邮件、传真或挂号信送达,同时要求对方返送回执,在人员送达、寄送五天后或电子邮件接收并被确认后视为已经送达。通知必须按双方约定地址寄出。

11. 本协议适用中华人民共和国相关法律。

(以下无正文)

甲方公章:



日期: 2016. 2. 13

乙方公章:



日期: 2016. 2. 13



