

采购合同（合同主要条款及格式）

项目名称：桂林师范学院 2026 年校园信息化平台升级及安全防护建设项目-1/2/3

项目编号：GXZC2026-J1-002261-GLSZ

甲方：桂林师范学院（采购人）

乙方：广西苏桂信息科技有限公司（成交供应商）

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等法律、法规规定，按照竞争性谈判文件（以下简称谈判文件）、响应文件规定条款和成交供应商的承诺、甲乙双方签订本采购合同。

第一条 合同标的及合同金额

项号	标的名称	生产厂家、品牌、规格型号	技术参数	数量 ①	单位	单价 (元) ②	单项合计金额 (元) ③=①×②
1	外网防火墙升级授权	深信服科技股份有限公司、深信服、AF-3120-EU	详见附件 1	1	项	23,100	23,100
2	内网防火墙软件升级授权	深信服科技股份有限公司、深信服、AF-3120-EU	详见附件 1	1	项	23,100	23,100
3	上网行为管理软件升级授权	深信服科技股份有限公司、深信服、AC-1000-L444-HX	详见附件 1	1	项	38,000	38,000
4	EDR 终端安全平台软件升级授权 1	深信服科技股份有限公司、深信服、终端安全管理系统（EDR）	详见附件 1	1	项	2,400	2,400
5	EDR 终端安全平台软件升级授权 2	深信服科技股份有限公司、深信服、终端安全管理系统（EDR）	详见附件 1	1	项	2,600	2,600
6	安全探针软件升级授权	深信服科技股份有限公司、深信服、STA-100-B2200	详见附件 1	1	项	16,600	16,600
7	态势感知平台软件升级授权	深信服科技股份有限公司、深信服、SIP-1000-B400	详见附件 1	1	项	39,000	39,000

8	NIPS 防入侵软件升级授权	深信服科技股份有限公司、深信服、NIPS-2000-B2100	详见附件 1	1	项	15,800	15,800
9	WEB 应用防火墙软件升级授权	深信服科技股份有限公司、深信服、WAF-2000-B2100	详见附件 1	1	项	18,700	18,700
10	零信任	深信服科技股份有限公司、深信服、aTrust-1000-B1030M	详见附件 1	1	台	51,300	51,300
11	漏洞扫描软件升级授权	奇安信科技集团股份有限公司、奇安信、S5000-W020P	详见附件 1	1	项	25,500	25,500
合 计							256100.00

根据《成交通知书》的成交内容，合同的总金额为：人民币（大写）贰拾伍万陆仟壹佰元整（¥：（小写）256100.00 元）。

第二条 质量保证

1. 乙方应按响应文件承诺的货物规格型号、技术参数、质量标准等向甲方提供未经使用的全新原装产品，且在正常安装使用和保养条件下，其使用寿命期内各项指标均达到质量标准。

2. 乙方提供货物的质量保证期为按“采购需求”规定执行（厂家规定质保期超过一年的，按厂家规定，“采购需求”有规定的，按规定执行）。在质保期内因货物本身的质量问题发生故障，乙方应负责免费修理和更换零部件。对达不到技术要求者，根据实际情况，经双方协商，可按以下第（1）款办法处理：

（1）更换：由乙方承担所有发生的全部费用。

（2）贬值处理：由甲乙双方协议定价。

（3）退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、贷款利息及银行手续费等）。

第三条 权利保证

1. 乙方应保证所提供货物在使用时不会侵犯任何第三方的专利权、商标权、工业设计权或其他权利。

2. 乙方应按竞争性谈判文件规定的时间向甲方提供使用货物的有关技术资料。

3. 乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、质押、查封等产权瑕疵。

第四条 货物包装、运输

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用中文说明书（货物属于进口产品的，供货时应同时附上中文使用说明书）、质量检验证书、随配附件和工具以及清单一并附于货物内。

本项目货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）。

3. 乙方在货物发运手续办理完毕后二十四小时内或货到甲方四十八小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

第五条 交付

1、交付使用时间：自收到采购人交付通知之日起 30 天内交货并安装调试合格交付使用。

2、服务地点：桂林市采购人指定地点；

3、交付方式：现场交付。

第六条 验收方式

1、货物交付前，采购人现场根据竞争性谈判文件要求及响应文件承诺逐条对应进行核验，核验不合格的，采购人有权终止合同执行并全部退货，同时上报政府采购监督管理部门。采购人依法追偿该成交供应商所造成的损失。

2、采购人如需要原厂原件存档，相关获取成本、沟通协调工作由供应商自行承担。供应商若无法提供原厂原件的，须提供原厂官方可核验电子版、官网查询路径，并出具加盖自身公章的兜底服务承诺，保证原厂同等质保效力，否则不予验收。在保修期内如发现货物有其它潜在缺陷及用户使用后发现存在不符合投标承诺的标准的，采购人有权退货或向成交供应商索赔。

第七条 安装和培训

1. 甲方应提供必要安装条件（如场地、电源、水源等）。

2. 乙方负责甲方有关人员的培训。培训时间、地点：采购人指定地点。

第八条 服务要求及免费保修期

分标 3:

1、质量保证与免费质保期

基本要求：投标人应严格遵守《中华人民共和国消费者权益保护法》及国家“三包”规定，提供包括包修、包换、包退在内的全方位售后服务。

免费质保期：本项目所有货物均提供免费上门保修服务，具体期限要求如下：

第十项货物：免费质保期（含软件免费维护与升级服务）3 年；

第十一项：免费质保期（含软件免费维护与升级服务）1 年；

其余各项：免费软件免费维护与升级 1 年。

质保期起算：质保期自项目验收合格之日起计算。

质保期内服务内容：在免费质保期内，投标人应免费提供上门维修、配件更换、软件升级及维护等服务。质保期外，投标人应提供终身维修维护服务，但只收取配件成本费。

2、安装调试与培训

免费安装调试：免费提供上门安装、调试服务，直至设备正常运行。

免费操作培训：免费为采购人进行系统操作培训，直至采购单位的技术人员能熟练独立工作并能进行简单的故障排除为止。

3、技术支持服务

提供 7×24 小时的电话技术支持服务，接到采购人报障电话后 2 小时内响应，8 小时内派技术人员到达

采购人指定地点解决问题，所有问题均需在 24 小时内解决。24 小时内无法修复必须立即提供不低于同档次产品配置的备用设备供采购方正常使用。提供终身免费技术支持服务。

4、产品资料与文档配套

提供完整的产品（软件）配套的产品资料，包括系统安装使用手册、系统功能模块说明书、用户使用手册、帮助文档等。

第九条 税费等要求

本合同执行中相关的一切税费均由乙方负担。

第十条 付款方式

1、付款方式：

（一）预付款支付：采购合同签订之日起 10 个工作日内，中标（成交）供应商向采购人开具与合同总价款 30%等额的保函（保函有效期需覆盖项目履约全周期）和发票，采购人收到合规保函并审核无误后，向中标（成交）供应商支付合同总价款 30%的预付款。

（二）结算款支付：项目所有货物完成安装调试、试运行状态正常，经采购人组织验收合格并完成确认手续后 10 个工作日内，采购人向中标（成交）供应商支付剩余合同款项（即合同总价款的 70%）。

（三）开票要求：中标（成交）供应商须按规定开具增值税专用发票，发票信息需真实、完整、合规，项目名称、金额、税号等内容与采购合同、验收资料保持一致，作为财务结算入账的必备凭证。

2、本项目收取履约保证金。

（一）缴纳标准：中标（成交）供应商为中小企业的，按项目中标（成交）金额的 2%收取；其他企业按项目中标（成交）金额的 5%收取。（备注：中小企业认定严格按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）及《中小企业划型标准规定》（工信部联企业〔2011〕300 号）相关规定执行，项目以中标（成交）供应商自行出具的《中小企业声明函》作为认定依据。中标（成交）供应商须对自身企业类型声明的真实性、合法性、有效性承担全部责任，存在虚假声明的，视同违约，采购人将依规追究其相应责任）。

（二）缴纳方式：须通过银行转账、支票、汇票、本票或金融机构、担保机构出具的保函等非现金方式缴纳。采用银行转账等方式的，须转入采购人指定账户。

中标（成交）供应商须在中标通知书发出后、采购合同签订前通过银行转账、支票、汇票、本票或金融机构、担保机构出具的保函等非现金方式缴纳。采用银行转账等方式的，须转入采购人指定账户。未按规定提交履约保证金的，视为自动放弃中标资格。

指定账户信息：

户名：桂林师范学院；

账号：20205101040000787；

开户行：中国农业银行桂林分行营业部；

转账时备注“项目名称（项目编号）+履约保证金”。

（三）退付规定：

(1) 不予退付情形。

中标（成交）供应商未按合同约定全面履行履约义务、存在违约行为，或项目存在未整改完毕的质量问题的，履约保证金不予退还。

(2) 无息退付情形。

中标（成交）供应商全面履行采购合同约定义务、圆满完成项目履约，且项目验收合格、无任何质量遗留问题及纠纷的，可申请无息退还履约保证金。

(3) 退付流程及时限。

项目质保期满验收合格后5个工作日内，中标（成交）供应商可凭质保期满验收合格资料、履约保证金退付申请书、履约保证金缴费凭证（转账回执等），向采购人申请办理退费手续。采购人收到中标（成交）供应商完整、合规的书面退费资料后，15个工作日内完成审核并无息退还履约保证金。

(4) 责任界定。

因中标（成交）供应商自身原因，未按时提交退费申请、提交的退费资料不完整、不合规等，导致保证金无法按期退还的，所有逾期责任及相关风险由中标（成交）供应商自行承担，采购人不承担任何责任。

第十一条 违约责任

1. 乙方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚，乙方应向甲方支付合同金额5%违约金并赔偿甲方经济损失。

2. 乙方提供的货物如果侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任。

3. 因包装、运输引起的货物损坏，按质量不合格处理。

4. 甲方无故延期接收货物、乙方逾期交货的，每天向对方偿付违约货款额3%违约金，但违约金累计不得超过违约货款额5%，超过15天对方有权解除合同，违约方承担因此给对方造成经济损失；甲方延期付货款的，每天向乙方偿付延期货款额1%滞纳金，但滞纳金累计不得超过延期货款额5%。

5. 乙方未按本合同和响应文件中规定的服务承诺提供售后服务的，乙方应按本合同合同金额5%向甲方支付违约金。

6. 乙方提供的货物在质保期内，因设计、工艺或材料的缺陷和其他质量原因造成的问题，由乙方负责。

7. 其他违约行为按违约货款额5%收取违约金并赔偿经济损失。

8. 乙方未按本合同和响应文件中规定的服务承诺提供售后服务的，乙方应按本合同合同金额5%向甲方支付违约金。

9. 乙方提供的货物在质保期内，因设计、工艺或材料的缺陷和其他质量原因造成的问题，由乙方负责。

10. 其他违约行为按违约货款额5%收取违约金并赔偿经济损失。

第十二条 不可抗力事件处理

1. 在合同有效期内，乙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。

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。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十三条 合同争议解决

1. 因服务问题发生争议的, 应邀请国家认可的相关机构进行鉴定。服务符合要求的, 鉴定费由采购人承担; 服务不符合要求的, 鉴定费由成交供应商承担。

2. 因履行本合同引起的或与本合同有关的争议, 甲乙双方应首先通过友好协商解决, 如果协商不能解决, 可向甲方所在地有管辖权的人民法院提起诉讼。

3. 诉讼期间, 本合同继续履行。

第十四条 合同生效及其它

1. 合同经甲乙双方法定代表人、负责人、自然人或相应的授权代表签字并加盖公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的, 需经本级财政部门审批, 并签订书面补充协议报本级财政部门备案, 方可作为主合同不可分割的一部分。

3. 本合同未尽事宜, 遵照《中华人民共和国民法典》有关条文执行。

第十五条 合同的变更、终止与转让

1. 除《中华人民共和国政府采购法》第五十条规定的情形外, 本合同一经签订, 甲乙双方不得擅自变更, 中止或终止。

2. 乙方不得擅自转让(无进口资格的供应商委托进口货物除外)其应履行的合同义务。

第十六条 签订本合同依据

1. 竞争性谈判文件;
2. 乙方提供的响应(或应答)文件;
3. 服务承诺书;
4. 成交通知书。

第十七条 合同文件

本合同所附下列文件是构成本合同不可分割的部分:

1. 竞争性谈判文件;
2. 乙方提供的响应(或应答)文件;
3. 成交通知书;
4. 本合同协议书及有关补充资料。

政府采购合同双方自签订之日起将自动存档于“广西政府采购云平台”平台上。

甲方(公章): 桂林师范学院

乙方(公章, 自然人除外): 广西苏桂信息科技有限公司

法定代表人签字: 李永华

法定代表人(负责人、自然人)签字(属自然人的应在签名

处加盖大拇指指印) 赵瑞常

委托代理人: 李永华

委托代理人: 赵瑞常

电 话: 0773-3975093

电 话:

开户名称:

开户名称: 广西苏桂信息科技有限公司

开户银行:

开户银行: 建行广西壮族自治区分行营业部

银行账号:

银行账号: 4505 0159 4151 0000 2187

日 期: 2026.9.23

日 期: 2026.9.23

附件 1:

项号	标的名称	技术参数
1	外网防火墙升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换； 2. 产品支持 3 种以上的用户认证方式，包含但不限于单点登录、本地账号密码、外部账号密码认证； 3. 产品支持对 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制； 4. 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
2	内网防火墙软件升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换； 2. 产品支持 3 种以上的用户认证方式，包含但不限于单点登录、本地账号密码、外部账号密码认证； 3. 产品支持对 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制； 4. 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
3	上网行为管理软件升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：AC-1000-L444-HX。包含 URL&应用识别规则库授权+设备系统软件升级包。具体功能描述如下： 1. URL 库与应用识别规则库升级服务能够最大程度对常见的恶意网站、非法应用、可疑行为进行识别，并方便用户根据需要，设定合理的规则，杜绝不安全因素的访问，降低网络使用风险； 2. 保障流量管理（带宽限制，带宽保证等）持续有效；

		3. 保障访问应用控制（各类应用程序使用权限管理，URL 访问权限管理，关键字过滤等）持续有效； 4. 保障应用审计（IM 审计，BBS 发帖审计，邮件审计，网页审计等）持续有效；保障产品对互联网新应用做及时有效的风险管控。
4	EDR 终端安全平台软件升级授权 1	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：终端安全管理系统（EDR）。包含终端安全管理系统软件升级授权。具体功能描述如下： 1. 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数； 2. 基于勒索病毒攻击过程，建立勒索立体防护机制，提供 3 层勒索入侵防御-6 级勒索反加密-5 项勒索检测与响应的完整防护体系，展示勒索病毒处置情况； 3. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴； 4. 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率； 5. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。
5	EDR 终端安全平台软件升级授权 2	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：终端安全管理系统（EDR）。包含终端安全管理系统软件升级授权。具体功能描述如下： 1. 支持终端扫描端口的异常扫描检测； 2. 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描； 3. 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率； 4. 支持根据用户性能偏好设置高、中、低 3 种防护级别； 5. 基于勒索病毒攻击过程，建立勒索立体防护机制，提供 3 层勒索入侵防御-6 级勒索反加密-5 项勒索检测与响应的完整防护体系，展示勒索病毒处置情况； 6. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴； 7. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。
6	安全探针软件升级	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：STA-100-B2200。包含安全感知系统探针特征库软件 V2.0 授权。升级后的设备具体功能描述如下：

	授权	1. 支持多种类型弱口令策略可选；支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数； 2. 支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产 IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 3. 支持 IP，IP 组，服务，访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标 IP（组）已开放的服务，白名单策略只允许白名单里的 IP（组）在指定的时间内访问，其他时间或其他 IP 的访问均被视为违规，黑名单策略禁止黑名单里的 IP（组）在指定的时间内访问，否则将被视为违规； 4. 支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。
7	态势感知 平台软件 升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：SIP-1000-B400。包含安全感知系统平台特征库软件 V2.0 授权+设备系统软件升级包。具体功能描述如下： 1. 支持主机类资产识别，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基线异常、操作系统、操作系统详情、主机类型、服务与端口、状态、责任人、EDR 状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP 类型、识别方式、首次发现时间等； 2. 支持跨三层取 MAC 地址，识别资产 MAC 地址，并能够解决不同资产 IP 冲突问题，以及 DHCP 场景 IP 变更的问题； 3. 支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、服务与端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作； 4. 支持挖矿专项检测页面，帮助组织更好的应对日益严峻的挖矿风险，避免数据被窃取，支持本地挖矿检测和云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果日志，支持基于挖矿阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息； 5. 支持自定义分支管理权限，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等。
8	NIPS 防入侵软件升	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：NIPS-2000-B2100。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下：

	级授权	1. 产品内置 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 2. 产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。 3. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。 4. 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
9	WEB 应用防火墙软件升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：WAF-2000-B2100。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 内置超过 4500 多种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 2. 支持 X-Forwarded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。 3. 支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁。 4. 支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。
10	零信任	一、性能参数： 1、规格 1U，单电源，接口 8 千兆电口+2 万兆光口，配置 4 个万兆多模光模块+2 个光纤线-多模-LC-LC-5M； 2、零信任接入授权 100 套。 二、功能参数： 1、为了满足灵活部署的要求，控制中心应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口； 2、为充分利用设备的网络性能，控制中心部署时支持配置聚合网口，并支持将聚合网口作为控制中心的网络部署 IP，聚合网口支持通过哈希或 802.3ad 等标准对闲置网口进行网口绑定，支持通过 ARP 探测机制对聚合网口进行健康检查； 3、为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的策略基线、设备稳定性、设备自安全等进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告； 4、集群故障切换时间优化，被动故障不超过 60S，主动故障 100S 恢复；

	5、通过隧道模式，可以支持基于 TCP、UDP、ICMP 等协议代理访问业务资源，支持发布 IP、IP 范围、IP 段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面； 6、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、Ubuntu 等主流操作系统，针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的地址； 7、当客户端通过 CDN 加速等代理方式接入访问业务系统时，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP； 8、为满足单位多样化安全便捷认证需求，支持以下认证方式：本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议的票据认证、Radius 账号认证、HTTPS 帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证，支持飞书用户或个人微信企业号通过 H5 接入； 9、支持管理员自行配置单位的弱密码库，可配置 10W 行的弱密码； 10、为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告； 11、支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权； 12、零信任系统支持通过票据共享的方式跟统一身份认证系统进行单点登录对接，为了适应多种身份认证系统获取票据的方式，票据共享应支持 OAuth 对接及票据注入模式； 13、支持对客户端的工作台标签、欢迎语标题、接入按钮、办公提示语等信息进行自定义配置； 14、系统运维支持自行修正设备时间或通过 NTP 自动校正设备时间，可自行配置 NTP 服务器地址； 15、支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆
--	---

		破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等； 16、可扩展文件加密功能，“一文一密”即每个文件使用不同的密钥加密，即相同内容的文件加密后的密文也不同； 17、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、中科方德、Ubuntu 等主流操作系统；针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的 IP。
11	漏洞扫描 软件升级 授权	采购内容为软件产品授权。漏洞特征库升级授权，硬件维修服务。

附件 2：履约保证金缴纳证明

中国建设银行网上银行电子回执					
币别：人民币		日期：2026/09/16		凭证号：108654547275	
付款人	全 称	广西苏桂信息科技有限公司	收款人	全 称	桂林师范学院
	账 号	45050159415100002187		账 号	20205101040000787
	开户行	中国建设银行股份有限公司广西壮族 自治区分行营业部		开户行	中国农业银行桂林 分行营业部广西桂 林市
大写金额	伍仟壹佰贰拾贰元整		小写金额	¥5,122.00元	
用 途	桂林师范学院2026年校园信息化平台升级及安全防护建设项目-3（GXZC2026-J1-002261-GLSZ）履约保证金		验证码	18169126482549	
跟单信息	GX4500009181629501				
单据状态	银行已汇出				
制单员：	123456彭维超				
复核员：	999999彭琼				

重要提示：银行受理成功，本回执不作为收、付款方交易确认的最终依据。



银行受理成功，本回执不作为交易确认的最终依据。

附件 3：微型企业声明函

微型企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司参加桂林师范学院的桂林师范学院 2026 年校园信息化平台升级及安全防护建设项目-分标 3采购活动，已中标（成交）。本公司作为中小微企业的具体情况如下：

本公司（广西苏桂信息科技有限公司）属于软件和信息技术服务业行业；从业人员4人，营业收入为180.87万元，资产总额为378.07万元，属于（微型企业）；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本公司对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。



日期：2026 年 9 月 16 日

附件 4：中标（成交）通知书

中标(成交)通知书

广西苏桂信息科技有限公司：

经评定，编号为GXZC2026-J1-002261-GLSZ采购文件中的桂林师范学院2026年校园信息化平台升级及安全防护建设项目-分标3，确定你公司中标（成交），中标(成交)价格为256100元。

自此通知书发出之日起25天内，与采购人签订政府采购合同。合同签订前，需按本项目采购文件和你公司投标（响应）文件等约定拟定合同文本(合同格式见采购文件)，报我机构项目联系人确认。

采购人联系人：惠襄

电话：0773-3975072

代理机构联系人：廖伟杰

电话：0773-5625166



附件 5：初次报价文件

广西苏桂信息科技有限公司

响应文件

2.谈判报价表（格式见附件）（必须提供）；

附件：

谈判报价表

项号	标的名称	生产厂家	品牌	规格型号	数量 ①	单位	单价 ②	单项合 计=数量 ×单价 ③=①× ②	备注
1	外网防火墙升级授权	深信服科技股份有限公司	深信服	AF-3120-EU	1	项	23,100	23,100	
2	内网防火墙软件升级授权	深信服科技股份有限公司	深信服	AF-3120-EU	1	项	23,100	23,100	
3	上网行为管理软件升级授权	深信服科技股份有限公司	深信服	AC-1000-L444-HX	1	项	38,000	38,000	
4	EDR 终端安全平台软件升级授权 1	深信服科技股份有限公司	深信服	终端安全管理系统 (EDR)	1	项	2,400	2,400	
5	EDR 终端安全平台软件升级授权 2	深信服科技股份有限公司	深信服	终端安全管理系统 (EDR)	1	项	2,600	2,600	
6	安全探针软件升级授权	深信服科技股份有限公司	深信服	ST-1000-B2200	1	项	16,600	16,600	
7	态势感知平台软件升级授权	深信服科技股份有限公司	深信服	SIP-1000-B400	1	项	39,000	39,000	
8	NIPS 防入侵软件升级授权	深信服科技股份有限公司	深信服	NIPS-2000-B2100	1	项	15,800	15,800	

9	WEB 应用防火墙 软件升级授权	深信服科 技股份有 限公司	深信服	WAF-2000-B2100	1	项	18,700	18,700	
1 0	零信任	深信服科 技股份有 限公司	深信服	aTrust-1000-8103 0M	1	台	51,800	51,800	
1 1	漏洞扫描软件 升级授权	奇安信科 技集团股 份有限公 司	奇安信	S5000-W020P	1	项	25,500	25,500	
谈判总报价（大写）：贰拾伍万陆仟陆佰元人民币（¥256600.00）									
交付使用期：自收到采购人交付通知之日起 30 天内交货并安装调试合格交付使用。									
免费保修期：【本项目所有货物均提供免费上门保修服务，具体期限要求如下： 第十项货物：免费质保期（含软件免费维护与升级服务）3 年； 第十一项货物：免费质保期（含软件免费维护与升级服务）1 年； 其余各项：免费软件免费维护与升级 1 年。】									
说明：谈判报价指本次招标采购范围内货物价款、货物随配标准附件、包装、运输、装卸、保险、税金、 货到位以及安装、安装所需辅材、调试、检验、售后服务、培训、保修及其他所有成本费用的总和。报价 人综合考虑在报价中。									

供应商（CA 签章，自然人除外）：广西苏桂信息科技有限公司

法定代表人、负责人、自然人或相应的委托代理人签字或加盖 CA 签章（属自然人的应在签名处加盖大拇指指印或个人 CA 签章）：赵巧勇

注：1. 供应商必须就“采购需求”中所有内容作完整唯一报价，根据“采购需求”中的“采购需求（技术参数、性能、配置等要求）”要求逐项对应填报所提供货物的性能指标等承诺（即：谈判报价表），否则，其响应将被拒绝；响应文件只允许有一个报价，有选择的或有条件的报价将不予接受。

2. 供应商应根据所提供的货物如实填写谈判报价表的各项内容，否则，响应文件无效。

3. 谈判报价表须由法定代表人、负责人、自然人或相应的委托代理人签字或个人 CA 签章（属自然人的应在签名处加盖大拇指指印或个人 CA 签章）并加盖供应商 CA 签章（自然人除外）。

4. 如全部或部分产品属于《节能产品政府采购清单》或《环境标志产品政府采购清单》目录范围的，供应商应在本表备注栏内写明各分项货物属于节能（或环境标志）产品政府采购清单第几类第几项序号的产品，以便谈判小组作为优先采购或评审的依据。

当本表由多页构成时，需逐页加盖供应商 CA 签章（属自然人的须逐页签字或加盖个人 CA 签章）。

附件 6：最后报价应答文件

投标报价明细表

投标人全称（公章）：广西苏桂信息科技有限公司

项目编号及分标：桂林师范学院2026年校园信息化平台升级及安全防护建设项目（GSZC2026-JL-002261-GS21-0003）

供应商名称	名称	总价（元）	备注（如有）
广西苏桂信息科技有限公司	桂林师范学院2026年校园信息化平台升级及安全防护建设项目分标3	¥6100	无

附件 7：技术规格和商务响应偏离表

广西苏桂信息科技有限公司

响应文件

3.技术规格偏离表（必须提供）；

附件：

技术规格偏离表

项目编号：GXZC2026-J1-002261-GLSZ

项目名称：桂林师范学院 2026 年校园信息化平台升级及安全防护建设项目-3

项号	标的名称	项目要求及技术要求	响应文件的响应情况	偏离情况说明
1	外网防火墙升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。 具体功能描述如下： 1. 产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换； 2. 产品支持 3 种以上的用户认证方式，包括但不限于单点登录、本地账号密码、外部账号密码认证； 3. 产品支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。 具体功能描述如下： 1. 产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换； 2. 产品支持 3 种以上的用户认证方式，包括但不限于单点登录、本地账号密码、外部账号密码认证； 3. 产品支持对 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制； 4. 产品支持多维度流量控制功能，支持基	无偏离

		4. 产品支持多维度流量控制功能, 支持基于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求; 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求; 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	
2	内网防火墙软件升级授权	采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。 具体功能描述如下: 1. 产品支持 IPSec VPN 智能选路功能, 根据线路质量和应用实现自动链路切换; 2. 产品支持 3 种以上的用户认证方式, 包括但不限于单点登录、本地账号密码、外部账号密码认证; 3. 产品支持对不少于 9000 种应用的识别和控制, 应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制; 4. 产品支持多维度流量控制功能, 支持基于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求; 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: AF-3120-EU。包含云智订阅软件授权+设备系统软件升级包。 具体功能描述如下: 1. 产品支持 IPSec VPN 智能选路功能, 根据线路质量和应用实现自动链路切换; 2. 产品支持 3 种以上的用户认证方式, 包括但不限于单点登录、本地账号密码、外部账号密码认证; 3. 产品支持对 9000 种应用的识别和控制, 应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制; 4. 产品支持多维度流量控制功能, 支持基于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求; 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	无偏离
3	上网行为管理软件升级授权	采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: AC-1000-L444-HX。包含 URL&应用识别规则库授权+设备系统软件升级包。具体功能描述如下: 1. URL 库与应用识别规则库升级服务能够最大程度对常见的恶意网站、非法应用、	采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: AC-1000-L444-HX。包含 URL&应用识别规则库授权+设备系统软件升级包。具体功能描述如下: 1. URL 库与应用识别规则库升级服务能够最大程度对常见的恶意网站、非法应用、	无偏离

	可疑行为进行识别, 并方便用户根据需要, 设定合理的规则, 杜绝不安全因素的访问, 降低网络使用风险; 2. 保障流量管理 (带宽限制, 带宽保证等) 持续有效; 3. 保障访问应用控制 (各类应用程序使用权限管理, URL 访问权限管理, 关键字过滤等) 持续有效; 4. 保障应用审计 (IM 审计, BBS 发帖审计, 邮件审计, 网页审计等) 持续有效; 保障产品对互联网新应用做及时有效的风险管控。	可疑行为进行识别, 并方便用户根据需要, 设定合理的规则, 杜绝不安全因素的访问, 降低网络使用风险; 2. 保障流量管理 (带宽限制, 带宽保证等) 持续有效; 3. 保障访问应用控制 (各类应用程序使用权限管理, URL 访问权限管理, 关键字过滤等) 持续有效; 4. 保障应用审计 (IM 审计, BBS 发帖审计, 邮件审计, 网页审计等) 持续有效; 保障产品对互联网新应用做及时有效的风险管控。	
4	EDR 终端安全平台软件升级授权 1 采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: 终端安全管理系统 (EDR)。包含终端安全管理系统软件升级授权。具体功能描述如下: 1. 提供勒索病毒整体防护体系入口, 直观展示最近七天勒索病毒防护效果, 包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数; 2. 基于勒索病毒攻击过程, 建立勒索立体防护机制, 提供 3 层勒索入侵防御-6 级勒索反加密-5 项勒索检测与响应的完整防护体系, 展示勒索病毒处置情况; 3. 支持客户端的错峰升级, 可根据实际情况控制客户端同时升级的最大数量, 避免大量终端程序同时更新造成网络拥堵或 I/O 风暴; 4. 可通过多维度引擎进行漏斗式检测, 保	采购内容为软件产品授权及升级包。原品牌为: 深信服, 型号: 终端安全管理系统 (EDR)。包含终端安全管理系统软件升级授权。具体功能描述如下: 1. 提供勒索病毒整体防护体系入口, 直观展示最近七天勒索病毒防护效果, 包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数; 2. 基于勒索病毒攻击过程, 建立勒索立体防护机制, 提供 3 层勒索入侵防御-6 级勒索反加密-5 项勒索检测与响应的完整防护体系, 展示勒索病毒处置情况; 3. 支持客户端的错峰升级, 可根据实际情况控制客户端同时升级的最大数量, 避免大量终端程序同时更新造成网络拥堵或 I/O 风暴; 4. 可通过多维度引擎进行漏斗式检测, 保	无偏离

		障查杀效果在低误报率的情况下保持高检出率； 5. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。	障查杀效果在低误报率的情况下保持高检出率； 5. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。	
5	EDR 终端安全平台 软件升级授权 2	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：终端安全管理系统（EDR）。包含终端安全管理系统软件升级授权。具体功能描述如下： 1. 支持终端扫描端口的异常扫描检测； 2. 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描； 3. 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率； 4. 支持根据用户性能偏好设置高、中、低3种防护级别； 5. 基于勒索病毒攻击过程，建立勒索立体防护机制，提供3层勒索入侵防御-6级勒索反加密-5项勒索检测与响应的完整防护体系，展示勒索病毒处置情况； 6. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O 风暴； 7. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：终端安全管理系统（EDR）。包含终端安全管理系统软件升级授权。具体功能描述如下： 1. 支持终端扫描端口的异常扫描检测； 2. 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描； 3. 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率； 4. 支持根据用户性能偏好设置高、中、低3种防护级别； 5. 基于勒索病毒攻击过程，建立勒索立体防护机制，提供3层勒索入侵防御-6级勒索反加密-5项勒索检测与响应的完整防护体系，展示勒索病毒处置情况； 6. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O 风暴； 7. 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到各终端快速响应终端威胁。	无 偏 离
6	安全探针软件	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：STA-100-B2200。	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：STA-100-B2200。	无

	升级授权	包含安全感知系统探针特征库软件 V2.0 授权。升级后的设备具体功能描述如下： 1. 支持多种类型弱口令策略可选；支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数； 2. 支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产 IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 3. 支持 IP、IP 组、服务、访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标 IP（组）已开放的服务，白名单策略只允许白名单里的 IP（组）在指定的时间内访问，其他时间或其他 IP 的访问均被视为违规，黑名单策略禁止黑名单里的 IP（组）在指定的时间内访问，否则将被视为违规； 4. 支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。	包含安全感知系统探针特征库软件 V2.0 授权。升级后的设备具体功能描述如下： 1. 支持多种类型弱口令策略可选；支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数； 2. 支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产 IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 3. 支持 IP、IP 组、服务、访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标 IP（组）已开放的服务，白名单策略只允许白名单里的 IP（组）在指定的时间内访问，其他时间或其他 IP 的访问均被视为违规，黑名单策略禁止黑名单里的 IP（组）在指定的时间内访问，否则将被视为违规； 4. 支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。	偏离
7	态势感知平台软件升级授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：SIP-1000-B400。包含安全感知系统平台特征库软件 V2.0 授权+设备系统软件升级包。具体功能描述如下： 1. 支持主机类资产识别，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：SIP-1000-B400。包含安全感知系统平台特征库软件 V2.0 授权+设备系统软件升级包。具体功能描述如下： 1. 支持主机类资产识别，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基	无偏离

		线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR 状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP 类型、识别方式、首次发现时间等； 2. 支持跨三层取 MAC 地址，识别资产 MAC 地址，并能够解决不同资产 IP 冲突问题，以及 DHCP 场景 IP 变更的问题； 3. 支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、服务与端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作； 4. 支持挖矿专项检测页面，帮助组织更好的应对日益严峻的挖矿风险，避免数据被窃取，支持本地挖矿检测和云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果日志，支持基于挖矿阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息； 5. 支持自定义分支管理权限，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等。	线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR 状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP 类型、识别方式、首次发现时间等； 2. 支持跨三层取 MAC 地址，识别资产 MAC 地址，并能够解决不同资产 IP 冲突问题，以及 DHCP 场景 IP 变更的问题； 3. 支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、服务与端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作； 4. 支持挖矿专项检测页面，帮助组织更好的应对日益严峻的挖矿风险，避免数据被窃取，支持本地挖矿检测和云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果日志，支持基于挖矿阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息； 5. 支持自定义分支管理权限，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等。	
8	NIPS 防入侵	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：NIPS-2000-B2100。	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：NIPS-2000-B2100。	无

软件升级授权	包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 2. 产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。 3. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。 4. 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 产品内置 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 2. 产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。 3. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。 4. 产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 5. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。	偏离
9 WEB 应用防 火墙软 件升级 授权	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：WAF-2000-B2100。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 内置超过 4500 多种 WEB 应用攻击特征，支持对跨站脚本 (XSS) 攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 2. 支持 X-Forwarded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。 3. 支持服务器漏洞扫描功能，并对扫描	采购内容为软件产品授权及升级包。原品牌为：深信服，型号：WAF-2000-B2100。包含云智订阅软件授权+设备系统软件升级包。具体功能描述如下： 1. 内置超过 4500 多种 WEB 应用攻击特征，支持对跨站脚本 (XSS) 攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 2. 支持 X-Forwarded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。 3. 支持服务器漏洞扫描功能，并对扫描	无 偏 离

		源 IP 进行日志记录和联动封锁。 4. 支持 Cookie 攻击防护功能, 并通过日志记录 Cookie 被篡改。	源 IP 进行日志记录和联动封锁。 4. 支持 Cookie 攻击防护功能, 并通过日志记录 Cookie 被篡改。	
10	零信任	一、性能参数: 1、规格≥1U, 单电源, 接口≥8千兆电口+2万兆光口, 配置≥4个万兆多模光模块+2个光纤线-多模-LC-LC-5M; 2、零信任接入授权≥100套。 二、功能参数: 1、为了满足灵活部署的要求, 控制中心应支持 IPV4/IPV6 双栈网络 IP 配置, 可自主选择配置 LAN 口或 WAN 口; 2、为充分利用设备的网络性能, 控制中心部署时支持配置聚合网口, 并支持将聚合网口作为控制中心的网络部署 IP, 聚合网口支持通过哈希或 802.3ad 等标准对闲置网口进行网口绑定, 支持通过 ARP 探测机制对聚合网口进行健康检查; 3、为方便管理员统筹查看管理零信任系统的整体运行状态, 支持对设备自身的策略基线、设备稳定性、设备自安全等进行巡检, 对设备的整体状态进行打分, 统计所有检查的正常项、异常项和告警项, 并输出巡检报告; (需提供产品功能截图, 并加盖投标人公章) 4、集群故障切换时间优化, 被动故障不超过 60S, 主动故障不超过 100S 恢复; 5、通过隧道模式, 可以支持基于 TCP、UDP、ICMP 等协议代理访问业务资源, 支持发布 IP、IP 范围、IP 段、具体域名及	一、性能参数: 1、规格 1U, 单电源, 接口 8 千兆电口+2万兆光口, 配置 4 个万兆多模光模块+2 个光纤线-多模-LC-LC-5M; 2、零信任接入授权 100 套。 二、功能参数: 1、为了满足灵活部署的要求, 控制中心应支持 IPV4/IPV6 双栈网络 IP 配置, 可自主选择配置 LAN 口或 WAN 口; 2、为充分利用设备的网络性能, 控制中心部署时支持配置聚合网口, 并支持将聚合网口作为控制中心的网络部署 IP, 聚合网口支持通过哈希或 802.3ad 等标准对闲置网口进行网口绑定, 支持通过 ARP 探测机制对聚合网口进行健康检查; 3、为方便管理员统筹查看管理零信任系统的整体运行状态, 支持对设备自身的策略基线、设备稳定性、设备自安全等进行巡检, 对设备的整体状态进行打分, 统计所有检查的正常项、异常项和告警项, 并输出巡检报告; (需提供产品功能截图, 并加盖投标人公章) 4、集群故障切换时间优化, 被动故障不超过 60S, 主动故障 100S 恢复; 5、通过隧道模式, 可以支持基于 TCP、UDP、ICMP 等协议代理访问业务资源, 支持发布 IP、IP 范围、IP 段、具体域名及	无偏离

通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面； 6、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、Ubuntu 等主流操作系统，针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的地址； 7、当客户端通过 CDN 加速等代理方式接入访问业务系统时，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP；（需提供产品功能截图，并加盖投标人公章） 8、为满足单位多样化安全便捷认证需求，支持以下认证方式：本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议的票据认证、Radius 账号认证、HTTPS 帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证，支持飞书用户或个人微信企业号通过 H5 接入； 9、支持管理员自行配置单位的弱密码库，可配置不少于 10W 行的弱密码； 10、为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安	通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面； 6、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、Ubuntu 等主流操作系统，针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的地址； 7、当客户端通过 CDN 加速等代理方式接入访问业务系统时，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP；（需提供产品功能截图，并加盖投标人公章） 8、为满足单位多样化安全便捷认证需求，支持以下认证方式：本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议的票据认证、Radius 账号认证、HTTPS 帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证，支持飞书用户或个人微信企业号通过 H5 接入； 9、支持管理员自行配置单位的弱密码库，可配置 10W 行的弱密码； 10、为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安
--	---

全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告； 11、支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权； 12、零信任系统支持通过票据共享的方式跟统一身份认证系统进行单点登录对接，为了适应多种身份认证系统获取票据的方式，票据共享应至少支持 OAuth 对接及票据注入模式；（需提供产品功能截图，并加盖公章投标人公章） 13、支持对客户端的工作台标签、欢迎语标题、接入按钮、办公提示语等信息进行自定义配置； 14、系统运维支持自行修正设备时间或通过 NTP 自动校正设备时间，可自行配置 NTP 服务器地址； 15、支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等；	全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告； 11、支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权； 12、零信任系统支持通过票据共享的方式跟统一身份认证系统进行单点登录对接，为了适应多种身份认证系统获取票据的方式，票据共享应支持 OAuth 对接及票据注入模式；（需提供产品功能截图，并加盖公章投标人公章） 13、支持对客户端的工作台标签、欢迎语标题、接入按钮、办公提示语等信息进行自定义配置； 14、系统运维支持自行修正设备时间或通过 NTP 自动校正设备时间，可自行配置 NTP 服务器地址； 15、支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等；
---	---

		16、可扩展文件加密功能，“一文一密”即每个文件使用不同的密钥加密，即相同内容的文件加密后的密文也不同；（需提供产品功能截图，并加盖投标人公章） 17、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、中科方德、Ubuntu 等主流操作系统；针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的 IP。	16、可扩展文件加密功能，“一文一密”即每个文件使用不同的密钥加密，即相同内容的文件加密后的密文也不同；（需提供产品功能截图，并加盖投标人公章） 17、支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、中科方德、Ubuntu 等主流操作系统；针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的 IP。	
11	漏洞扫描软件升级授权	采购内容为软件产品授权。漏洞特征库升级授权，硬件维修服务。	采购内容为软件产品授权。漏洞特征库升级授权，硬件维修服务。	无偏离

供应商[公章(CA 签章)，自然人签字或个人 CA 签章]：广西苏桂信息科技有限公司

日期：2026 年 09 月 14 日

注：

1.供应商应对照竞争性谈判文件中“第三章 采购需求”中技术规格需求的内容逐条响应，并在“偏离情况说明”栏注明“正偏离”、“负偏离”或“无偏离”。否则，响应无效。

2.当所提供货物的技术参数性能指标等承诺出现“正偏离”情况时，应详细填写偏离情况说明及提供相应有效的证明材料，否则，谈判小组有权不予认定“正偏离”情况。

3.技术规格偏离表须加盖供应商 CA 签章（自然人签字或加盖个人 CA 签章）。当本表由多页构成时，需逐页加盖供应商 CA 签章（属自然人的须逐页签字或加盖个人 CA 签章）。

4.商务响应表（必须提供）；

附件：

商务响应表

项目编号：GXZC2026-J1-002261-GLSZ

项目名称：桂林师范学院 2026 年校园信息化平台升级及安全防护建设项目-3

项号	竞争性谈判文件的商务要求	响应文件承诺的商务要求	偏离情况说明
售后服务要求	1、质量保证与免费质保期 基本要求：投标人应严格遵守《中华人民共和国消费者权益保护法》及国家“三包”规定，提供包括包修、包换、包退在内的全方位售后服务。 免费质保期：本项目所有货物均提供免费上门服务。 保修服务，具体期限要求如下： 第十项货物：免费质保期（含软件免费维护与升级服务）最短不得少于 3 年； 第十一项：免费质保期（含软件免费维护与升	我公司承诺： 1、质量保证与免费质保期 基本要求：投标人应严格遵守《中华人民共和国消费者权益保护法》及国家“三包”规定，提供包括包修、包换、包退在内的全方位售后服务。 免费质保期：本项目所有货物均提供免费上门服务。 保修服务，具体期限要求如下： 第十项货物：免费质保期（含软件免费维护与升级服务）3 年；	无偏离

级服务) 最短不得少于 1 年; 其余各项: 免费软件免费维护与升级最短不得少于 1 年。 质保期起算: 质保期自项目验收合格之日起计算。 质保期内服务内容: 在免费质保期内, 投标人应免费提供上门维修、配件更换、软件升级及维护等服务。质保期外, 投标人应提供终身维修维护服务, 但只收取配件成本费。 2、安装调试与培训 免费安装调试: 免费提供上门安装、调试服务, 直至设备正常运行。 免费操作培训: 免费为采购人进行系统操作培训, 直至采购单位的技术人员能熟练独立工作并能进行简单的故障排除为止。 3、技术支持服务 需提供 7×24 小时的电话技术支持服务, 接到采购人报障电话后 2 小时内响应, 8 小时内派技术人员到达采购人指定地点解决问题, 所有问题均需在 24 小时内解决。24 小时内无法修复必须立即提供不低于同档次产品配置的备用设备供采购方正常使用。提供终身免费技	第十一项: 免费质保期 (含软件免费维护与升级服务) 1 年; 其余各项: 免费软件免费维护与升级 1 年。 质保期起算: 质保期自项目验收合格之日起计算。 质保期内服务内容: 在免费质保期内, 投标人应免费提供上门维修、配件更换、软件升级及维护等服务。质保期外, 投标人应提供终身维修维护服务, 但只收取配件成本费。 2、安装调试与培训 免费安装调试: 免费提供上门安装、调试服务, 直至设备正常运行。 免费操作培训: 免费为采购人进行系统操作培训, 直至采购单位的技术人员能熟练独立工作并能进行简单的故障排除为止。 3、技术支持服务 提供 7×24 小时的电话技术支持服务, 接到采购人报障电话后 2 小时内响应, 8 小时内派技术人员到达采购人指定地点解决问题, 所有问题均在 24 小时内解决。24 小时内无法修复必须立即提供同档次产品配置的备用设备供采购方正常使用。提供终身免费技术支持服
--	--

	术支持服务。 4、产品资料与文档配套 提供完整的产品（软件）配套的产品资料，包括系统安装使用手册、系统功能模块说明书、用户使用手册、帮助文档等。	务。 4、产品资料与文档配套 提供完整的产品（软件）配套的产品资料，包括系统安装使用手册、系统功能模块说明书、用户使用手册、帮助文档等。	
交付 使用 时间、 地点 及交 付方 式	1、交付使用时间：自收到采购人交付通知之日起 30 天内交货并安装调试合格交付使用。 2、服务地点：桂林市采购人指定地点； 3、交付方式：现场交付。	我公司承诺： 1、交付使用时间：自收到采购人交付通知之日起 30 天内交货并安装调试合格交付使用。 2、服务地点：桂林市采购人指定地点； 3、交付方式：现场交付。	无 偏 离
付款 方式 及履 约保 证金	1、付款方式： （一）预付款支付：采购合同签订之日起 10 个工作日内，中标（成交）供应商向采购人开具与合同总价款 30% 等额的保函（保函有效期需覆盖项目履约全周期）和发票，采购人收到合规保函并审核无误后，向中标（成交）供应商支付合同总价款 30% 的预付款。 （二）结算款支付：项目所有货物完成安装调试、试运行状态正常，经采购人组织验收合格并完成确认手续后 10 个工作日内，采购人向	我公司承诺： 1、付款方式： （一）预付款支付：采购合同签订之日起 10 个工作日内，中标（成交）供应商向采购人开具与合同总价款 30% 等额的保函（保函有效期需覆盖项目履约全周期）和发票，采购人收到合规保函并审核无误后，向中标（成交）供应商支付合同总价款 30% 的预付款。 （二）结算款支付：项目所有货物完成安装调试、试运行状态正常，经采购人组织验收合格	无 偏 离

中标（成交）供应商支付剩余合同款项（即合同总价款的 70%）。 （三）开票要求：中标（成交）供应商须按规定开具增值税专用发票，发票信息需真实、完整、合规，项目名称、金额、税号等内容与采购合同、验收资料保持一致，作为财务结算入账的必备凭证。 2、履约保证金： （一）缴纳标准：中标（成交）供应商为中小企业的，按项目中标（成交）金额的 2%收取；其他企业按项目中标（成交）金额的 5%收取。 （备注：中小企业认定严格按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）及《中小企业划型标准规定》（工信部联企业〔2011〕300 号）相关规定执行，项目以中标（成交）供应商自行出具的《中小企业声明函》作为认定依据。中标（成交）供应商须对自身企业类型声明的真实性、合法性、有效性承担全部责任，存在虚假声明的，视同违约，采购人将依规追究其相应责任）。 （二）缴纳方式：须通过银行转账、支票、汇票、本票或金融机构、担保机构出具的保函等	并完成确认手续后 10 个工作日内，采购人向 中标（成交）供应商支付剩余合同款项（即合同总价款的 70%）。 （三）开票要求：中标（成交）供应商须按规定开具增值税专用发票，发票信息需真实、完整、合规，项目名称、金额、税号等内容与采购合同、验收资料保持一致，作为财务结算入账的必备凭证。 2、履约保证金： （一）缴纳标准：中标（成交）供应商为中小企业的，按项目中标（成交）金额的 2%收取；其他企业按项目中标（成交）金额的 5%收取。 （备注：中小企业认定严格按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）及《中小企业划型标准规定》（工信部联企业〔2011〕300 号）相关规定执行，项目以中标（成交）供应商自行出具的《中小企业声明函》作为认定依据。中标（成交）供应商须对自身企业类型声明的真实性、合法性、有效性承担全部责任，存在虚假声明的，视同违约，采购人将依规追究其相应责任）。 （二）缴纳方式：须通过银行转账、支票、汇
---	---

非现金方式缴纳。采用银行转账等方式的，须转入采购人指定账户。 指定账户信息： 户名：桂林师范学院； 账号：20205101040000787； 开户行：中国农业银行桂林分行营业部； 转账时备注“项目名称（项目编号）+履约保证金”。 （三）退付规定： （1）不予退付情形。 中标（成交）供应商未按合同约定全面履行履约义务、存在违约行为，或项目存在未整改完毕的质量问题的，履约保证金不予退还。 （2）无息退付情形。 待成交供应商履行完合同约定的权利义务事项后不存在争议的，中标（成交）供应商可凭验收合格资料、履约保证金退付申请书、履约保证金缴费凭证（转账回执等），向采购人申请办理退费手续。采购人收到中标（成交）供应商完整、合规的书面退费资料完成审核后，采购人在 5 个工作日内办理履约保证金退还手续。	票、本票或金融机构、担保机构出具的保函等非现金方式缴纳。采用银行转账等方式的，须转入采购人指定账户。 指定账户信息： 户名：桂林师范学院； 账号：20205101040000787； 开户行：中国农业银行桂林分行营业部； 转账时备注“项目名称（项目编号）+履约保证金”。 （三）退付规定： （1）不予退付情形。 中标（成交）供应商未按合同约定全面履行履约义务、存在违约行为，或项目存在未整改完毕的质量问题的，履约保证金不予退还。 （2）无息退付情形。 待成交供应商履行完合同约定的权利义务事项后不存在争议的，中标（成交）供应商可凭验收合格资料、履约保证金退付申请书、履约保证金缴费凭证（转账回执等），向采购人申请办理退费手续。采购人收到中标（成交）供应商完整、合规的书面退费资料完成审核后，采购人在 5 个工作日内办理履约保证金退还手续。
--	--

	(3) 责任界定。 因中标（成交）供应商自身原因，未按时提交退费申请、提交的退费资料不完整、不合规等，导致保证金无法按期退还的，所有逾期责任及相关风险由中标（成交）供应商自行承担，采购人不承担任何责任。	手续。 (3) 责任界定。 因中标（成交）供应商自身原因，未按时提交退费申请、提交的退费资料不完整、不合规等，导致保证金无法按期退还的，所有逾期责任及相关风险由中标（成交）供应商自行承担，采购人不承担任何责任。	
验收标准、要求	1、设备安装前，采购人现场根据竞争性谈判文件要求及响应文件承诺逐条对应进行核验，核验不合格的，采购人有权终止合同执行并全部退货，同时上报政府采购监督管理部门。采购人依法追偿该成交供应商所造成的损失。 2、采购人如需要原厂原件存档，相关获取成本、沟通协调工作由供应商自行承担。供应商若无法提供原厂原件的，须提供原厂官方可核验电子版、官网查询路径，并出具加盖自身公章的兜底服务承诺，保证原厂同等质保效力，否则不予验收。在保修期内如发现货物有其它潜在缺陷及用户使用后发现存在不符合投标承诺的标准的，采购人有权退货或向成交供应商索赔。	我公司承诺： 1、设备安装前，采购人现场根据竞争性谈判文件要求及响应文件承诺逐条对应进行核验，核验不合格的，采购人有权终止合同执行并全部退货，同时上报政府采购监督管理部门。采购人依法追偿该成交供应商所造成的损失。 2、采购人如需要原厂原件存档，相关获取成本、沟通协调工作由供应商自行承担。供应商若无法提供原厂原件的，须提供原厂官方可核验电子版、官网查询路径，并出具加盖自身公章的兜底服务承诺，保证原厂同等质保效力，否则不予验收。在保修期内如发现货物有其它潜在缺陷及用户使用后发现存在不符合投标承诺的标准的，采购人有权退货或向成交供应商索赔。	无偏离

报价要求	本项目实行费用包干制, 竞谈报价应包括但不 限于: 完成采购货物实施所需的费用 (包含采购范围内的货物及服务价格、升级、培训、技术支持、售后服务、安装调试等)、和各项税金等完成本项目所产生的全部费用。供应商在报价时应考虑各方面因素、各种风险和自己的承受能力, 报价中应包含全部内容, 成交后采购人不再另行支付额外费用。	我公司承诺: 本项目实行费用包干制, 竞谈报价应包括但不 限于: 完成采购货物实施所需的费用 (包含采购范围内的货物及服务价格、升级、培训、技术支持、售后服务、安装调试等)、和各项税金等完成本项目所产生的全部费用。供应商在报价时应考虑各方面因素、各种风险和自己的承受能力, 报价中应包含全部内容, 成交后采购人不再另行支付额外费用。	无 偏 离
核心产品	核心产品: 第 10 项货物 “零信任”	我公司承诺: 核心产品: 第 10 项货物 “零信任”	无 偏 离
其他要求	1、本分标的采购预算金额为人民币 (大写): 人民币贰拾伍万捌仟伍佰元整 (¥258500.00 元), 最后报价超出采购预算金额的将被视为响应文件无效。 2、本表中技术规格需求所有条款及商务要求均为实质性要求, 投标时必须响应, 若有任意一项负偏离, 作响应文件无效处理。 3、本项目涉及的货物不接受进口产品 (即通过中国海关报关验放进入中国境内且产自关境外的产品) 参与竞谈, 若有此类产品参与竞	我公司承诺: 1、本分标的采购预算金额为人民币 (大写): 人民币贰拾伍万捌仟伍佰元整 (¥258500.00 元), 我公司本次报价金额为人民币 (大写): 人民币贰拾伍万陆仟陆佰元整 (¥256600.00 元), 没有超出最高限价。最后报价超出采购预算金额的将被视为响应文件无效。 2、本表中技术规格需求所有条款及商务要求均为实质性要求, 我公司投标时将完全响应, 若有任意一项负偏离, 作响应文件无效处理。	无 偏 离

	谈的，按响应文件无效处理。 4、本项目所属行业：软件和信息技术服务业	3、本项目所提供的产品均不属于进口产品 (即通过中国海关报关验放进入中国境内且 产自关境外的产品)参与竞谈，若有此类产品 参与竞谈的，按响应文件无效处理。 4、本项目所属行业：软件和信息技术服务业	
--	---------------------------------------	--	--

供应商（公章(CA 签章)，自然人签字或个人 CA 签章）：广西苏桂信息科技有限公司

日期：2026 年 09 月 14 日

注：1.“商务响应表”各项内容必须如实填写。

2.当本表由多页构成时，需逐页加盖供应商公章（CA 签章）（属自然人的须逐页签字或个人 CA 签章）。

3.供应商应对照竞争性谈判文件中“第三章 采购需求”中的“商务要求”的内容逐条响应，并在“偏离情况说明”栏注明“正偏离”、“负偏离”或“无偏离”。否则，响应无效。

5.供应商的售后服务承诺书（必须包含售后服务要求的全部内容）（格式见附件）（必须提供）；

附件：

服务承诺书

一、售后服务总则

本方案针对“桂林师范学院 2026 年校园信息化平台升级及安全防护建设项目”，严格遵循国家产品“三包”规定及采购方要求，以“快速响应、高效解决、持续保障”为核心，提供全方位、专业化的售后服务，确保项目系统稳定运行，最大限度满足采购方业务需求。

二、售后服务核心承诺

1、质量保证与免费质保期

基本要求：投标人应严格遵守《中华人民共和国消费者权益保护法》及国家“三包”规定，提供包括包修、包换、包退在内的全方位售后服务。

免费质保期：本项目所有货物均提供免费上门保修服务，具体期限要求如下：

第十项货物：免费质保期（含软件免费维护与升级服务）3 年；

第十一项：免费质保期（含软件免费维护与升级服务）1 年；

其余各项：免费软件免费维护与升级 1 年。

质保期起算：质保期自项目验收合格之日起计算。

质保期内服务内容：在免费质保期内，投标人应免费提供上门维修、配件更换、软件升级及维护等服务。质保期外，投标人应提供终身维修维护服务，但只收取配件成本费。

2、安装调试与培训

免费安装调试：免费提供上门安装、调试服务，直至设备正常运行。

免费操作培训：免费为采购人进行系统操作培训，直至采购单位的技术人员能熟练独立工作并能进行

简单的故障排除为止。

3、技术支持服务

提供 7×24 小时的电话技术支持服务，接到采购人报障电话后 2 小时内响应，8 小时内派技术人员到达采购人指定地点解决问题，所有问题均在 24 小时内解决。24 小时内无法修复必须立即提供不低于同档次产品配置的备用设备供采购方正常使用。提供终身免费技术支持服务。

4、产品资料与文档配套

提供完整的产品（软件）配套的产品资料，包括系统安装使用手册、系统功能模块说明书、用户使用手册、帮助文档等。

三、售后服务配置

1. 为采购方指定 1 名售后技术负责人作为对接人，负责日常沟通、需求协调及服务跟踪。
2. 确保 7×24 小时响应机制落地，节假日及突发情况提前做好人员备份安排。

四、具体售后服务内容与方案

（一）故障出现解决方案

1. 故障分级标准

- 一级故障（紧急）：系统瘫痪、核心功能失效、网络安全漏洞风险等影响采购方业务正常运行的故障。

- 二级故障（严重）：非核心功能异常，但影响部分业务效率或存在潜在风险的故障。

- 三级故障（一般）：不影响业务运行，仅需优化调整或咨询解答的问题。

2. 故障处理流程

- 接收报障：通过 7×24 小时服务热线、企业微信/邮件等多渠道接收采购方报障，记录故障现象、发生时间、影响范围等关键信息。

- 初步诊断：1 小时内完成故障分级，一级故障立即启动应急响应，远程指导采购方采取临时止损措施；

二、三级故障同步提供初步排查建议。

- 现场处置：一级故障 8 小时内到场，优先采用“替换法”“应急配置”等方式快速恢复系统；二级故障 6 小时内到场，24 小时内解决；三级故障可根据采购方需求选择远程或现场处理，48 小时内闭环。

- 备用设备提供：若故障设备需返厂维修或 24 小时内无法修复，立即启动备用设备调配流程，8 小时内将备用设备送达采购方指定地点并完成安装调试。

- 故障复盘：故障解决后 3 个工作日内，提交《故障处理报告》，说明故障原因、处理过程、优化建议，避免同类问题重复发生。

(二) 定期维护方案

1. 维护周期与内容

- 月度维护（远程）：通过远程登录系统，检查设备运行状态、软件日志、系统稳定性、安全补丁更新情况，排查潜在风险，提供优化建议。

- 季度维护（现场）：技术人员到场对设备进行全面检测（含硬件老化检查、散热系统清理）、软件版本升级（质保期内免费）、数据备份与恢复测试、系统性能调优，同步收集采购方使用反馈。

- 年度维护（现场）：开展全面系统巡检，包括设备硬件深度检测、软件功能完整性验证、数据安全审计，出具《年度维护报告》，制定下一年度维护计划。

2. 维护保障措施

- 建立维护档案，详细记录每次维护的时间、内容、结果及采购方反馈，实现全生命周期可追溯。
- 维护前提前 3 个工作日与采购方沟通，确认维护时间（避开业务高峰期），减少对正常工作的影响。
- 维护过程中严格遵守采购方数据安全管理规定，不得泄露任何敏感信息，维护后需经采购方技术人员确认签字。

(三) 免费技术培训方案

1. 培训目标：确保采购方技术人员能熟练独立操作系统、完成日常维护及简单故障排除，掌握核心操作要

点。

2. 培训对象：采购方技术运维人员、相关业务操作人员（人数根据采购方需求确定）。

3. 培训形式与时间

- 现场集中培训：系统安装调试合格后 1 周内，开展 2 天集中培训（每天 6 小时），采用“理论讲解+实操演示+案例分析”相结合的方式。

- 一对一实操指导：集中培训后 1 个月内，提供 2 次上门一对一指导，针对性解决采购方人员操作疑问。

- 远程补充培训：质保期内根据采购方需求，提供不限次数远程培训支持，可按需定制专项培训内容。

4. 培训内容

- 基础模块：设备硬件认知、软件安装与卸载、系统界面操作、基础配置修改。
- 核心模块：系统适配要点、网络安全设备功能应用、数据备份与恢复、日常维护流程。
- 故障处理模块：常见故障排查方法、故障报警信息解读、简单故障自主解决案例。
- 资料支持：提供培训课件、操作视频教程、FAQ 手册，方便采购方人员课后复习。

（四）免费保修期外维修方案

1. 维修流程：采购方提出维修需求后，2 小时内响应，确认故障情况；如需现场维修，8 小时内到场检测，明确维修方案及配件费用，经采购方确认后实施维修；如需返厂维修，提供免费上门取送设备服务，维修周期不超过 7 个工作日（特殊配件除外，需提前告知采购方）。

2. 费用标准：仅收取元器件或配件成本费，无人工维修费、服务费，配件价格透明，提供正规发票及配件合格证明。

3. 维修保障：维修后的设备/配件提供 6 个月质保期，质保期内出现同类故障免费再次维修；终身提供维修技术支持，定期告知设备升级换代信息及优化建议。

（五）售后服务措施

1. 多渠道响应机制：开通7×24小时服务热线、专属企业微信/邮箱、在线客服平台，确保采购方可通过多种方式快速联系售后团队。
2. 快速调配机制：在采购方所在城市或周边区域储备常用配件及备用设备，建立配件供应商应急联动机制，确保配件快速采购与调配。
3. 服务质量监督：建立售后服务评价体系，每次服务完成后，通过电话、问卷等方式收集采购方满意度评价，对服务质量不达标的情况及时整改。
4. 定期沟通机制：每季度与采购方召开1次服务沟通会，汇报设备运行情况、维护工作开展情况，听取采购方需求及建议，持续优化服务方案。
5. 应急预案：针对自然灾害、重大系统故障等突发事件，制定专项应急预案，明确应急响应流程、人员分工、资源调配方案，确保快速应对。

(六) 安装要求及方案

1. 安装前期准备

- 现场勘察：安装前3个工作日，技术团队到场勘察安装环境，确认电源、网络、场地空间等是否符合设备安装要求，如需整改，提供书面整改建议。
- 设备检查：送货上门后，与采购方共同核对设备型号、数量、配件是否齐全，外观是否完好，确认无误后签署《设备验收单》。
- 资料准备：提前整理好安装所需的系统安装包、驱动程序、配置文件等，确保安装工作顺利开展。

2. 安装实施流程

- 设备部署：按照设计方案及行业规范，完成网络安全设备的固定安装、接线（电源、网络线），确保安装牢固、接线规范。
- 系统安装：安装系统及相关软件，进行基础配置（网络参数、安全策略、用户权限等），确保系统与采购方现有IT环境兼容。

- 调试测试：开展功能测试（核心功能、接口兼容性、数据传输稳定性）、压力测试（模拟高负载场景）、安全测试（漏洞扫描、防护能力验证），测试合格后填写《安装调试报告》。
- 交付验收：向采购方移交设备及相关资料，演示系统操作流程，解答采购方疑问，采购方验收合格后签署《项目验收单》。

3. 安装质量要求

- 安装过程严格遵守国家相关技术标准及设备厂商规范，确保设备运行稳定、安全可靠。
- 安装完成后，清理现场环境，确保无杂物遗留，设备周边环境符合散热、安全要求。
- 提供 1 个月安装后跟踪服务，密切关注系统运行状态，及时解决安装后出现的各类问题。

五、售后服务保障体系

1. 技术保障：售后团队成员均接受专业培训及考核，具备丰富的网络安全设备运维经验，确保技术服务专业性。
2. 资源保障：建立配件及备用设备储备库，与设备厂商、配件供应商签订应急供应协议，确保维修及备用资源快速到位。
3. 制度保障：制定《售后服务管理制度》《故障处理流程规范》《定期维护工作细则》等一系列制度，规范服务流程，确保服务质量。
4. 责任保障：明确售后团队各岗位责任，建立服务追责机制，对未按规定响应、处理故障的情况进行内部考核，确保服务承诺落实到位。

供应商[公章(CA 签章)，自然人签字或个人 CA 签章]：广西苏桂信息科技有限公司

日 期：2026 年 09 月 14 日