第五章　用户需求书

一、项目概况

本项目采购的维保服务主要是为学校网络安全体系中重要的网络安全防护设备（VPN、WAF、EDR、漏洞扫描设备）提供软件升级、硬件保修、设备巡检等保障服务，各类安全设备的稳定运行将为学校的信息化服务提供重要的安全保障。

二、建设原则

推进学校智慧校园网络安全保障体系建设，通过采购网络安全防护设备的原厂软、硬件维保服务，保障设备稳定运行，为学校的信息化服务提供重要的安全保障。

三、建设内容

（一）采购服务清单

本期项目旨在采购 VPN、WAF、EDR、漏洞扫描设备的原厂维保服务，具体服务清单如下：

序号	服务内容	数量	单位
1	VPN（深信服 VPN-1000-D600）原厂维保服务	1	项
2	深信服终端检测响应平台（V3.0）原厂维保服务	1	项
3	200 套深信服终端安全软件（V3.0）原厂维保服务	1	项
4	铱迅 WEB 应用防火墙（WAF8930）原厂维保服务	1	项
5	绿盟漏洞扫描系统（NSFOCUS RSAS V6.0）原厂维保服务	1	项

（二）技术参数要求（凡是带★号条款为不可偏离参数，建设文件中未完全满足带★号条款和指标，或非实质性响应有重大偏离的，将导致投标无效。）

1、VPN 原厂维保服务要求

序号	设备名称	采购服务	服 务 要 求
1	深信服 VPN	VPN 原厂维保服务	1、提供 2.5 年硬件整机保修服务，在硬件保修期内，对硬件产品整机给予保修； 2、提供 2.5 年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新； 3、提供 2.5 年售后服务支持，在服务期内，对于用户使用过程中遇到的问题，如用户咨询及远程调试不能解决，需派遣经过技术认证的工程师赶赴现场解决技术问题，为用户进行现场技术支持。并提供每年 4 次固定上门设备巡检服务。 4、需提供原厂售后服务承诺函

2、EDR 原厂维保服务要求

序号	设备名称	采购服务	服 务 要 求
1	深信服终	终端检测	1、提供 3.5 年软件升级服务，在软件升级服务期内，对软

	端检测响应平台	响应平台软件原厂维保服务	件内核进行版本升级及更新； 2、提供 3.5 年售后服务支持，在服务期内，对于用户使用过程中遇到的问题，如用户咨询及远程调试不能解决，需派遣经过技术认证的工程师赶赴现场解决技术问题，为用户进行现场技术支持。并提供每年 4 次固定上门设备巡检服务； 3、需提供原厂售后服务承诺函
2	深信服终端安全软件	200 套终端安全软件原厂维保服务	1、提供 3.5 年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新； 2、提供 3.5 年售后服务支持，在服务期内，对于用户使用过程中遇到的问题，如用户咨询及远程调试不能解决，需派遣经过技术认证的工程师赶赴现场解决技术问题，为用户进行现场技术支持。并提供每年 4 次固定上门设备巡检服务。 3、需提供原厂售后服务承诺函

3、WEB 应用防火墙原厂维保服务要求

序号	设备名称	采购服务	服 务 要 求
1	铱迅 WEB 应用防火墙	WEB 应用防火墙原厂维保服务	1、WEB 应用防护系统固件升级，VLAN 透明解码接入，特征库升级（包含 SQL 注入、WEBSHELL、XSS 等），2 年升级服务； 2、2 年硬件维保服务； 3、一年 4 次现场巡检支持服务； 4、每年 2 次 web 安全事件应急支持服务； 5、需提供原厂售后服务承诺函。

4、漏洞扫描系统原厂维保服务要求

序号	设备名称	采购服务	服 务 要 求
1	绿盟漏洞扫描系统	绿盟漏洞扫描系统原厂维保服务	对现有绿盟远程安全评估系统采购三年原厂维保服务，包含软件更新服务、特征库更新、产品保修服务、远程支持服务。 1、软件更新服务 服务方式：网站提供补丁和规则下载，通过电话、传真和电子邮件等方式远程受理许可证补发需求； 服务内容：提供最新产品补丁和产品规则文件下载，许可证补发支持； 服务效果：产品最新规则和补丁在线可用，产品许可证损坏和丢失后可于 1 工作日内提供。 2、特征库更新 服务方式：网站提供补丁和规则下载，通过电话、传真和电子邮件等方式远程受理许可证补发需求； 服务内容：提供最新产品补丁和产品规则文件下载，许可证补发支持； 服务效果：产品最新规则和补丁在线可用，产品许可证损坏和丢失后可于 1 工作日内提供。 3、产品保修服务 产品保修服务包括产品保修服务期内产品的维修和超时提供替换用机的服务； 产品保修服务期内用户的产品在出现故障并且经过原厂确

			认为产品故障时，用户可将产品送至原厂，由原厂在收到用户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给用户；如 15 个工作日内原厂无法修复该故障产品，需为用户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 4、远程支持服务 远程支持服务包括远程受理和解决客户问题、资料提供和其他应用咨询等内容。提供网站、电话、传真、邮件、CallCenter 等途径。 5、巡检服务 对远程安全评估系统提供季度巡检服务，每次巡检提供相应巡检报告。 6、需提供原厂售后服务承诺函。

四、具体要求

（一）维保要求

（1）本项目设备维保服务由设备原生产厂商直接提供；

（2）设备如果在质保期内出现保修范围内的故障并且原厂不提供上门保修服务的，中标人负责将设备送回原厂进行维修以及维修后将设备返还给用户，期间产生的一切费用由中标人负责；

（3）质保期内，如设备或零部件因非人为因素出现故障而造成短期停用时，则质保期和免费维修期相应顺延，如停用时间累计超过 60 天则质保期重新计算。

（二）服务总体要求

（1）★投标人须提供加盖其公章的承诺函：完全响应及满足投标文件涉及的性能指标和服务要求，如未来招标方和用户在验收或使用过程中发现不满足招标文件中要求的性能指标，经确认属实后，将不予以验收和付款。

（2）★投标人须提供加盖原厂家公章的售后服务承诺函。

（3）响应标准

1）1 级故障-关键业务中断：10 分钟内响应，2 小时内到场，8 小时内恢复中断的业务，24 小时内排除故障。

2）2 级故障-非关键功能失效或性能下降，但不至于中断业务或影响面有一定局限：半小时内响应，4 小时内到场，48 小时内排除故障。

3）3 级故障-系统可以运行，但出现系统报错：1 小时内响应，双方协商到场和排除故障时间。

（4）备件服务

中标人应有备件库，提供校园网安全设备的备件服务，并负责联系厂家进行故障设备的维修。备件要求：要求能提供满足功能且性能不低于现有在用设备的备件。

（5）运维服务质量要求

1）应能在 10 分钟内准确诊断并告知用户故障原因，诊断差错率要控制在 5%以内。并向最终用户解释故障发生原因，可能导致的后果，以及拟采取的措施。

2）故障修复过程中可能影响用户工作或对系统应用数据有影响的，要先咨询用户意见再处理。

3）如果配件需要送修或更换（涉及费用由中标人承担），维修期间提供同档次的备用设备，并需要配合用户登记故障配件的型号和产品序列号，并由用户签字后再送维修。

4）如果设备送修，需要保护好磁盘等存贮设备。要先将用户数据备份好，再送维修。

5）设备维修结束后，维修人员需向用户出示服务维修单。服务维修单上需注明维修日期、维修人员、维修地点、故障、故障原因分析、修复结果等。

6）中标人须向用户提供项目负责人及维护人员的详细联系方式。

7）响应类型要求：热线电话、手机支持，上门现场解决。

8）服务类型要求：送修、现场。

（三）服务期限要求

根据服务清单制定委托服务期，自签订合同之日起计算。

（四）验收要求

1.中标人在维保期向用户提供如下服务：

（1） 现场巡检服务（每季度一次）

1）中标人协调网络安全设备厂商通过巡检报告分析信息资产存在的安全漏洞，分析信息资产面临的安全威胁及威胁发生的可能性，检查现有安全措施的有效性，从而识别出信息资产中存在的安全风险点，并根据用户所能接受的风险，对其信息资产所面临的风险程度做出准确的评价，提供相关整改修复加固建议。

2）安全设备升级检查：中标人协调网络安全设备厂商定期对安全设备的软件版本、特征库进行升级，确保安全设备的安全稳定运行的同时，也确保安全设备规则最新。检查安全设备规则库、病毒库定期升级情况，可以通过合理配置安全设备，对设备的 CPU 利用率、内存利用率、磁盘利用率、网络接口连通性等各项功能指标设置告警阈值和告警规则，实时进行监控，及时发现安全设备运行状态异常的情况，如果确认是设备故障则启动故障处理流程。

（2）协助应急处置服务

1）中标人协调网络安全设备厂商为用户网络安全突发应急事件提供 7*24 小时的技术支

持；对网络安全防护措施提供5×8小时的安全咨询。

2）中标人协调网络安全设备厂商协助用户制定网络安全事件应急处置流程与预案。

3）中标人协调网络安全设备厂商协助用户处理网络安全事件，按照应急处置流程配合相关工作人员进行处置，并跟进实施，并总结上报。

4）中标人协调网络安全设备厂商开展针对信息安全事件的事后分析工作包括损失评估、审计分析以及对应急预案的评估修正。

5）安全事件处理结束后，中标人应协调网络安全设备厂商对该安全事件进行总结，并整理编制报告。

2. 中标人向用户提供服务期间以下各类服务输出文件：

（1）设备升级服务报告；

（2）软件更新服务报告；

（3）厂家上门故障处理报告；

（4）产品巡检报告；

（5）信息安全事件报告；

（6）信息安全事件处理规定；

（7）信息安全事件调查分析及处理报告；

（8）厂家出具的本项目所含设备的漏洞处置报告。

3.用户对中标人服务进行年度考核服务评价，得分在80分以下， 不予验收。年度考核服务评价表如下所示。

年度考核服务评价表			
考核项目	考核得分标准	分值	得分
故障处置	未按招标及合同要求按时、按质量完成故障处置，一次扣2分。	20分	
备件服务	设备发生需要返厂修复的故障时，未能按招标及合同要求，按时提供备件服务，一次扣4分。	20分	
巡检服务	未按招标及合同要求开展巡检服务，每缺一次服务，扣5分。严格按照学校网络安全规范进行相关的巡检工作，不得擅自改变安全设备服务进程、账号、密码，每违反一次扣2分。	20分	
服务报告	完成设备升级、软件升级、故障处置、产品巡检后需提供报告，每缺一份报告扣2分。	20分	
漏洞管理	当本项目所含设备存在厂家已知漏洞或被官方通报的漏洞时，该设备厂家需24小时内通知学校，48小时内修复漏洞，未按要求完成，一次扣5分。由于设备自身漏洞未及时修复导致被攻击而发生重大安全事件，一次扣10分。	20分	

加分项	安全厂家在服务期间发现本项目服务内容之外的重大安全隐患，每次加 2 分。安全厂家对学校日常安全工作提出合理可实施的策略优化建议，每次加 1 分。（**需提供安全隐患处置报告或策略配置截图作为佐证材料**）		

（五）付款方式

合同签署生效后采购方向中标人支付预付服务费（合同总额的 50%）；

合同签订满一年后，中标人无违约行为，并按验收要求向用户提供年度服务报告及通过年度考核，采购人向乙方支付合同的部分服务费（合同总额的 30%）；

合同签订满两年后，中标人无违约行为，并按验收要求向用户提供年度服务报告及通过年度考核，采购人向中标人支付合同的剩余服务费（合同总额的 20%）；

每笔款项通过银行汇款支付，支付需按采购人规定执行，每次支付时，中标人同时向采购人提供相应金额的票据。

（六）知识产权归属要求

中标人应保证本项目的投标技术、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷；如因第三方提出其专利权、商标权或其他知识产权的侵权之诉， 则一切法律责任由中标人承担。

（七）保密要求

（1）中标人应对招标人提供的一切资料、数据、用户信息等材料，以及因履行本合同接触到的用户一切数据、信息、资料等履行保密义务，如中标人泄密，则中标人应赔偿招标人和用户因此遭受的全部损失。

（2）中标人在项目中须和用户单位签订《项目保密协议》，将履行《项目保密协议》中规定的保密条款。

（3）所有参与安全服务项目实施的项目组成员须和中标人签订《员工保密协议》，项目组成员必须遵守中标人的《员工保密协议》，并做到以下几点和项目相关的要求：

1）保守客户的商业秘密，不得对外透露。

2）客户访谈内容不得随意向项目组以外的人透露。

3）项目的过程文件与资料不得随处乱放，以免泄露。

4）安全服务的品质保证：中标人承诺保证原厂指派工作经验丰富、技术实力雄厚的安全顾问结合技术领先、准确可靠的安全工具为招标人提供安全管理服务。承诺安全服务过程按照国际标准进行，确保服务的先进性原则。