第四章 采购需求及其技术、服务及其他要求

前提：本章中标注“★”的条款为实质性要求，未响应或不满足，按无效响应处理；

一、项目概述

包 2：随着网络尤其是因特网在我国的迅速普及，针对我国境内信息系统的攻击正在呈现快速增长的势头，利用网络传播有害信息的手段日益翻新。虽然我校现有较为完善的网络安全设备，但是也频频出现网络安全事件（我校网站前端代码中出现不合法链接）。这类网络安全事件皆为信息内容安全，安全设备难以防范。本项目为学院教学管理的网络安全服务项目，具体包括针对学院 2 台深信服负载均衡、2 台深信服防火墙、2 台深信服上网行为管理、华为堡垒机、数据库审计、日志审计、漏洞扫描等 16 台安全设备和系统提供资产安全状态进行整体安全评估，提出安全加固方案并协助实施；对加固后的资产进行日常安全运维，并在重大活动时期提供安全保障与应急响应、安全态势告知及关键系统运维保障服务等；还包含提供安全设备升级服务、综合性安全服务、人员驻场服务、其它安全等相关服务。

二、标的名称及所属行业

包号	（采购内容）标的名称	所属行业
2	网络安全运维服务	软件和信息技术服务业

三、服务要求

包 2 网络安全运维服务

（一）服务内容

服务项	服务内容	服务方式	服务量
综合安全服务	配置安全管理服务	现场服务	4 次/年
	安全加固服务	现场服务	4 次/年
	安全培训服务	现场理论授课	2 次/年

	信息安全风险评估	现场服务	1 次/年
	安全配置检查服务	现场服务	4 次/年
	应急响应服务	现场+远程	1 年
	系统上线前检测服务	现场+远程	1 年
	重大节假日保障	现场+远程	1 年
	完善管理制度方案	远程服务	1 次/年
	攻防演练方案	现场服务	1 次/年
	通信传输加密服务方案	原厂	域名年
其它安全服务	站群系统服务	站群原厂	系统年
	互联网业务安全托管服务	原厂	域名年
	通报预警服务	原厂	域名年
	安全渗透服务	现场+远程	4 次/次
设备延保服务	主要安全设备延保服务	现场+远程	设备
人员驻场服务	安全人员驻场服务	现场服务	1 年

（二）技术要求

序号	服务项目	服务内容	服务质量要求（范围）
1	安全服务体系	建立安全运维监控管理机制	1.对全面地对各类事件做出快速、准确的定位和处置，实现对系统运行动态的快速掌握； 2.建立通报预警流程机制； 3.对安全事件进行深入调查和原因分析； 4.在事件发生前明确系统当前存在的安全风险； 5.完善各个系统、数据库、中间件、网络安全设备的安全极限和标准配置规范。
		建立安全运维告警机制	
		建立安全运维事件响应机制	
		建立安全运维审核评估机制	
		建立安全基线及各系统配置规范	
2	综合安全服务	风险评估	1. 对学院现有的网络系统进行整体安全状态分析； 2. 对日常运维中发现的网络系统的脆弱性进行安全加固； 3. 通过安全意识和技术培训后，学院相关人员能具有一定的网络安全
		安全加固	
		安全培训	
		系统上线前检测	
		重大节日保障	
		完善管理制度	

		攻防演练	认知，提高学院的网络安全水平； 4. 保证新系统上线后不带病运行； 5. 重大节日中提供安全保障服务； 6. 完善一套符合学院的网络安全管理标准体系； 7. 通过攻防演练的方式发现学院存在的漏洞和脆弱性，并及时修补。
3	其他安全服务	站群系统服务	应能通过风险管控及时发现互联网安全问题，及时处理，且对指定系统定期进行渗透测试，及时发现可能存在的漏洞并提出修补建议。
		互联网业务安全托管服务	
		通报预警服务	
		安全渗透服务	
		通信传输加密服务	针对学院网站使用未加密方式进行数据传输的系统采用 https 等方式进行加密传输，保障数据的完整性和保密性。
4	设备延保服务	主要安全设备延保服务	对软硬件设备相关系统的漏洞、规则、病毒库等进行升级，并达到最新。
5	人员驻场服务	2 人安全人员驻场服务	安全工程师驻场后，应能对整个信息系统的网络故障进行及时的排查和处理。

2)服务要求

能够对学院现有资产安全状态进行整体安全评估，针对发现的存在的已知漏洞提出安全加固方案和协助措施，对加固后的资产能够进行日常安全运维，并在重大活动时期提供安全保障与应急响应、安全态势告知及管件系统运维保障服务。

3)服务目标

建立安全基线及各系统配置规范以及安全运维监控管理、告警、事件响应、审核评估机制，能够对学院现有的网络系统进行整体安全分析，在日常运维发现的网络系统的脆弱性能够进行安全加固，对学院的相关人员进行安全意识和技术培训后，使得学院相关人员具有一定的网络安全认知，提高学院的网络安全水平，保证新上线的系统不带病运行，完善一套符合学院的网络安全管理体系，对学院制定系统进行渗透测试，保障系统的安全性，驻场人员需对整个信息系统的网络

故障进行及时的排查和处理，升级相关系统的漏洞、规则、病毒库，保证学院相关系统的安全等级达到最优。

4)服务产出物包括但不限于：

服务项	服务内容	服务方式	服务量	服务交付
综合安全服务	配置安全管理服务	现场	年	《安全管理报告》季/年报
	安全加固服务	现场	年	《安全加固报告》季/年报
	安全培训服务	现场	48 课时	《信息安全意识培训》 《信息安全技术培训》
	信息安全风险评估	现场	年	《系统信息安全风险评估报告》
	安全配置检查服务	现场	年	《安全检查报告》季/年报
	应急响应服务	现场+远程	年	《应急事件处理报告》
	系统上线前检测服务	现场+远程	年	《系统上线前检测报告》
	重大节假日保障	现场+远程	年	《重大节假日安全保障报告》
其它安全服务	站群系统服务	原厂	系统年	《网站系统安全运行报告》
	互联网业务安全托管服务	原厂	域名年	《互联网业务安全托管报告》
	通报预警服务	原厂	域名年	
	安全渗透服务	原厂	次	《业务系统渗透测试报告》 《业务系统渗透测试复测报告》
	教育网域名 SSL 证书	原厂	域名年	提供 SSL 证书
人员驻场服务	2 人安全人员驻场服务	现场	年	法定工作时间驻守 应急值守
其它安全服务	主要安全设备延保服务	现场+远程	设备	四个校区软件升级,硬件质保,库升级(包括华为、深信服等)

5)安全服务体系

（1）建立安全运维监控管理机制

在安全运维中整合学院核心应用系统和安全设备厂商资源，融合线上和线下安全专家的专业能力，通过学院部署的各类安全设备以及云眼互联网监控工具建立全面覆盖信息及安全系统的监测机制，并对各类事件做出快速、准确的定位和

处置。实现对信息系统运行动态的快速掌握，以及运行维护管理过程中的事前预警、事发时快速定位。其主要包括：

1. 集中监控：监控的主要内容包括：网络、通信、安全设备、主机和核心应用系统等。
2. 统一处理：合理规划与布控，整合来自各种不同的安全设备、管理工具的安全警告与日志信息，进行标准化、归一化的处理。
3. 快速定位和预警：将依据相关规则、事件知识库、关联关系进行快速的故障定位，并根据预警条件进行预警。

6)、建立安全运维告警机制

1. 建设学院的“网络安全通报预警中心”，建立通报预警流程机制，全面发现安全风险，不漏报。
2. 告警响应和处理：提供短信告警、邮件告警、启动预案等多种响应方式。

7)建立安全运维事件响应机制

对我院业务环境中的安全事件进行响应，对相关安全数据进行分析、全方位监测发现的威胁和异常进行快速响应和处置，并针对安全事件进行深入调查和原因分析；同时输出事件响应处理报告，帮助我院正确应对攻击入侵事件，降低安全事件带来的损失。

8)建立安全运维审核评估机制

全面分析信息系统和网络中存在的各种安全问题，同时将发现的安全问题与信息资产的重要程度相关联，明确系统当前的安全风险。主要评估内容包括：物理层安全风险评估、网络层安全风险评估、系统层安全风险评估、应用层安全风险评估、数据层安全风险评估。通过评估使用户了解安全需求、认知安全风险、采取相应的保护和控制，有效的保证信息化安全的建设效益。

9)建立安全基线及各系统配置规范

在安全运维过程中建立各操作系统、数据库、中间件、网络安全设备的安全基线和标准配置规范。

10)安全服务内容

（1）综合安全服务

a.配置安全管理服务

形成安全软硬件设备台账，记录和保存其基本配置信息，包括网络拓扑结构、

各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等信息进行安全管理；

将各设备配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

b. 安全加固服务

在信息系统投入使用前和使用中，对操作系统、数据库系统等进行安全加固，以提高系统安全防范能力，减少安全事件的发生。

c. 安全培训服务

安全培训教育

通过技术培训提高我院相关岗位的安全意识和安全技能，使之能够符合相关信息安全工作岗位的能力要求，全面提高我院整体的信息安全水平。

有针对性地进行有关信息安全管理的理论培训、安全管理制度教育、安全防范意识宣传和专门安全技术训练，确保组织信息安全策略、规章制度和技术规范的顺利执行，从而最大限度地降低和消除安全风险。

安全意识培训

通过安全培训和教育工作，提高我院相关工作人员的信息安全意识和操作水平，降低由于人为原因引发的安全风险。

安全流程制度培训

针对相关的安全流程、安全制度、安全规范、安全运维计划进行培训，使我院相关工作人员了解相关的、系统级的安全体系操作流程和制度。

d. 安全评估服务

网络设备评估

根据信息系统中设备类型的不同，对核心层、交换层和接入层及防火墙、入侵检测等边界网络安全设备的访问控制和安全策略，现状有针对性进行风险评估。

操作系统评估

对操作系统开放的服务、安全配置、访问控制、系统漏洞进行安全脆弱性风险评估。

应用程序评估

为保证重要业务系统保密性、可用性，对操作系统上基于 WEB 服务及第三方应用程序做安全评估。

e.安全配置检查服务

收集我院业务系统及各关键设备和主机操作系统的安全补丁，检查各主机的系统和业务补丁加载情况，以及关键设备上的安全策略配置情况，划分高、中、低风险提交安全加固方案和加固计划，并对加固效果进行评估。

参照行业安全检查规范，适当的补充安全基线检查内容，对我院操作系统、中间件、数据库及业务应用系统进行全面检查及抽样检查，并输出报告。

f. 应急响应服务

对我院业务环境中的安全事件进行响应，对主机安全数据进行分析、全方位监测发现的威胁和异常进行快速响应和处置，并针对安全事件进行深入调查和原因分析；同时输出事件响应处理报告，帮助我院正确应对攻击入侵事件，降低安全事件带来的损失。

入侵影响抑制；入侵威胁清除；入侵原因分析；加固建议指导

应急响应服务另需根据我院需求，在安全事件发生后提供追踪、诱捕服务，协助相关部门取证。

g .系统上线前检测服务

制订系统上线前的安全检测方案，并根据信息系统平台建设情况，按照系统上线前安全检测方案实施检测工作，进行彻底全面的安全弱点评估，发现潜在的安全漏洞。上线前检测需采用对系统非侵害的测试方法，检验系统的安全防护能力，发现安全风险及漏洞，提出安全改进建议。

11)、其他安全服务

（1）站群系统服务

a.基础服务

基础服务包括日常运维问题处理、安全问题处理、应急问题响应、24 小时技术服务咨询等内容。通过基础服务可保障网站群平台的正常运行，具体包含以下内容：

日常运维服务

产品使用过程中遇到的任何技术问题包括产品操作、技术疑难与故障、产品功能，都可以进行沟通并处理。

安全服务

① 安全问题的分析处理

对安全厂商、上级部门的漏洞扫描报告进行一对一分析处理， 并对存在的安全问题提供书面的回复报告。

② 安全补丁主动更新服务

网站群相关的安全补丁发布后及时主动更新。

应急服务

日常维护过程中，遇到系统故障、网站安全类问题时，可获取紧急技术支持。具体内容包含：

① 紧急安全事件及时响应

发生紧急安全事件时，确保 7*24 小时及时响应处理。

② 平台故障修复

系统故障引发的网站群前后台无法访问，7*24 小时及时响应处理，避免造成不良的影响。

③ 数据恢复

当数据意外损坏或丢失，工程师可使用现存的数据备份进行技术恢复，保证损失最小化。

安全加固

对已知的问题隐患进行优化、加固或补丁更新，确保运行环境安全稳定。

b. 安全运维服务

安全运维服务包括云监控、重大活动保障、网站群保养、敏感字清理、应急演练等内容，主动发现并处理问题，最大程度保障系统的安全、稳定、高效运行。具体包含以下内容：

系统健康预警服务

实时监控系统健康状态，发现问题后主动预警，在我院允许的情况下第一时间介入处理，避免出现业务中断的情况。具体内容包含：

① 主站实时监控

实时监控主站首页的改动记录，发现页面重大变化时（例如页面变形/篡改等问题），及时预警并主动处理。避免网站首页错乱造成社会不良影响。

② 磁盘空间监控

监控磁盘使用率，大于 80%或剩余空间不足 20G 时进行预警。避免因磁盘空间耗尽导致平台异常，无法维护和新增资料。

③ 授权状态监控

④ 监控网站群授权状态，当授权可用时间小于 30 天或授权错误时预警。避免因授权文件错误，导致网站群平台无法使用，前台访问动态功能访问异常等重大问题。

⑤ 数据备份有效性监控

监控是否配置备份计划、是否有一周内的备份文件。发现备份异常时及时预警。避免数据意外损坏时，无备份包或备份包损坏的风险。

⑥ 异常时间段登录预警

监控网站群登录日志，在非工作时间（00：00 至 06：00）异常登录预警，及时发现异常并介入处理。防止因站点管理员密码泄露导致恶意登录，页面篡改等问题。

⑦ 网站群环境稳定性监控

通过实时监控系统资源占用、应用进程状态、访问连接数统计等信息，及时发现系统隐患，避免可能存在的不稳定因素。

重大活动保障服务

在重大节日、活动、事件中提供保障服务，7*24 小时及时响应。例如国庆节、春节等。

网站群保养服务

① 用户信息检查

进行检查账号安全性，例如长期未登录的账号信息，便于系统管理员进行管理。

② 垃圾清理

网站群系统在长期运行后会产生较多的垃圾文件，通过清理释放存储空间，并提升系统可靠性。

③ 安全补丁更新完整性检查

检查并更新系统安全补丁更新情况，确保所有安全补丁没有遗漏，全部成功更新。

敏感字清理

① 静态文件扫描及清理

对全盘数据进行扫描，发现敏感信息进行人工判断后，进行清理。

② 数据库扫描及清理

从数据库查询包含敏感关键字的数据，并进行清理。

c.安装与部署服务

在服务器、存储设备或虚拟化平台等基础设施发生变更或故障时，提供在此平台上运行的网站群产品的迁移与配置服务。例如：设备老化更换、操作系统故障重装等情况，部署环境包括：单机部署迁移、多机服务器部署迁移等。

d.主站服务

对主站进行日常的内容维护，具体内容包含：

图片设计

按照日常需求，提供图片定制化设计服务。

网站栏目框架调整

提供栏目框架增加、删除、修改等服务，按照实际需求进行调整，提供一对一技术指导及操作。

页面兼容性优化

对现有页面出现的兼容性问题，提供专业技术处理。

死链、暗链配合修复

对第三方机构检测出的死链、暗链提技术支持，指导修改及必要的修复工作。

紧急页面、栏目框架、模板调整

新闻网等重要站点，出现紧急页面、栏目框架、模板调整工作时，提供多对一实施、设计支持工作，确保相关紧急事件得到快速处理。

附件：主要安全设备清单表

序号	名称	品牌	设备型号	数量/单位
1	防火墙 1	深信服	AF-1820	2 台
2	防火墙 2	深信服	AF-6020	2 台
3	负载均衡	深信服	AD-4000	1 台
4	二合一网关	深信服	VPN-3050	1 台
5	防火墙 3	深信服	AF-1000-G640	4 台
6	负载均衡器	深信服	AD-1000-E640	2 台
7	防火墙 4	华为	WAF5000	1 台
8	漏洞扫描器	华为	VSCAN1508	1 台
9	BRAS 网关	石斧	10000M	2 台

（2）互联网业务安全托管服务

防止互联网业务被监管单位通报，被篡改以及被黑客入侵，保障互联网业务更加安全稳定的运行，并以全程可视的方式让我院随时随地掌握安全状况。

具体服务内容：

a 持续评估

资产梳理与识别

Web 暴露面监测

漏洞风险管理

高危 0day 事件告警

业务可用性监测和预警

b 持续加固

序号	服务特点	服务内容
1	关联分析	持续的分析安全设备以及云眼云盾安全日志，发现恶意攻击和策略漏洞等问题。
2	动态防护	根据资产变更导致的新风险暴露情况及威胁情况，持续优化安全策略。
3	定向防护	发现针对 0day 漏洞的攻击流量采用虚拟补丁对漏洞进行修复，并对流行攻击行为和可疑攻击做针对性安全策略。
4	实时对抗	在线专家持续对抗恶意攻击和未知威胁。
5	应急对抗	实时分析流量发现黑客定向攻击，快速阻断攻击流量
6	持续升级	实时更新 IPS、WAF、URL 等安全特征库。

c 主动响应

序号	服务特点	服务内容
1	篡改监测和处置	首页 5 分钟 1 次，二级页面 60 分钟一次，全部页面 24 小时，融入人工审核，实现预警 0 误报。
2	黑链、网马监测和处置	首页 5 分钟 1 次，二级页面 60 分钟一次，全部页面 24 小时，融入人工审核，实现预警 0 误报。
3	恶意文件检测和处置	恶意文件检测和处置，防暴力破解。
4	应急响应	WEB 入侵、系统入侵、病素木马、 信息泄漏等安全事件发生即发现，发现即响应。
5	本地专家处置	采购人认定的重大事件主动上门处置。

（3） 通报预警服务

要求对采购方管辖范围内整体网络业务安全风险的管控，快速发现互联网安全问题，及时处置，帮助采购人落实网络安全法监测职责，避免被网安/网信部门通报，导致承担连带安全责任。

具体服务内容：

序号	服务类别	服务名称	服务内容说明
1	建立通报预警流程	建立通报预警流程	建立通报预警流程，掌控下属单位资产信息，并根据资产信息开展安全监控，并根据监控结果进行通报，针对事件进行复查、归档，建立组织的通报预警流程机制，落地安全责任
2	全面风险监测	暴露面检测	关键资产系统域名发现、开放端口监测、网站后台暴露监测、WAF 防御检测
3		漏洞脆弱性检测	Web 漏洞扫描、信息泄漏检测、弱口令检测
4		高危 0day 事件告警	高危 0day 实时检测：出现 0DAY 漏洞时，主动对所监控用户业务做扫描发现，检测结果第一时间定向推送到客户
5		业务可用性监测	页面响应监测、网站存活监测
6		篡改监测	网页篡改监测：对目标站点的关键页面进行实时篡改监测，每 5 分钟监测 1 次。发现网页篡改事件第一时间通过微信通知用户，监测内容能够在周报月报中进行呈现。
7		黑链监测	网页黑链检测：对目标站点提供 7×24 小时网页黑链监测能力，每 5 分钟检测 1 次。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在周报、月报中进行呈现。
8	精准风险定位	安全专家在线值守	提供云端安全专家 7*24 小时值守及应急响应，确保响应的及时性和可靠性
9	通报预警	整体安全态势感知	通过态势感知服务页面全局掌握辖区内互联网业务的整体态势，直观呈现目前发现风险情况、事件通报情况、整改情况，整体把控区域的安全态势。
10		权威通报预警	结合网络安全监测、第三方事件通报平台、云端安全专家、本地化安全工程师进行网络安全通报及响应，通报方法结合邮件、微信等多种方式，实现直属业务的信息互通，可为监管人员和通报成员单位信息系统负责人提供实时告警，提升管

			理员安全响应速度。
11	事件归档	风险复查	由在线安全专家审核整改结果，根据修复情况做审批或驳回
12		事件归档	根据复查结果，做事件归档管理
13		汇总分析	将所有的安全事件进行汇总分析
14	驻场人工服务	人工服务	平台的整体使用由本地安全专家整体运维；
15			通过配套本地化安全服务工程师执行，降低应急响应、安全评估时间成本，最大程度上降低安全事故危害性，切实提高网络安全能力。

（4）渗透服务

尽可能发现提供的渗透范围内，所有系统的安全隐患，包括但不限于网络、系统、应用、终端、人员、开发测试等层面的安全问题。

12)、人员驻场服务

a. 运维值守服务的服务规范

驻场工程师在接到故障反应后，响应时间不超过 10 分钟，2 小时内到达现场，2 小时内排除故障。如因其他维护工作未完成而不能及时处理的，须及时告知采购人具体的故障情况及服务时间；

b. 运维值守服务的主要内容

服务内容：对整个信息系统的网络故障进行及时的排查和处理；对于突发性事件派驻采购人的工程师在确保每日 7*24 小时各种有效形式（电话、远程、现场技术支持等服务）的应急响应处理；做好整个信息系统的网络安全保障、安全加固指导及具体的实施工作；每天须结合专业分析和检查工具对重要网络设备和安全设备进行日志分析和设备运行状况检查工作，以做到能够及时处理和预防设备可预见性故障的发生；

结合采购人已有的网络监控软件和供应商提供的专业网络监控工具，并保障网络监控数据正常采集数据，同时派驻工程师须做好日常的网络监控工作，及时发现网络异常状况并作出相应的处理，派驻工程师须根据采购人的需求，每周提交相应的监控报告供采购人审核和存档；

成交供应商在维护过程中产生维修费用须向采购人提交申请，经采购人审核

同意后维修；配合采购人完成日常网络设备和安全设备的日常管理工作，以及采购人安排的其他临时性工作；

运维值守服务应配备储备技术人员。储备人员定期（每月至少 1 次）前往项目服务单位了解日常运维情况和网络安全架构，具备运维值守服务所需的各种能力要求，以保障 2 名运维值守人员调休期间和临时工作任务中，项目服务单位对运维值守服务的人员人数和能力需求。

服务方式：现场

服务交付：法定工作时间驻守、应急值守。

★四、商务要求

包2网络安全运维服务

1、服务地点

四川水利职业技术学院羊马校区(四川省成都崇州市羊马镇永和大道 366 号)

2、服务期限

服务期限：合同签订后 365 日内。

3、提供的配套服务（包括人员培训等）

要求提供不少于 48 课时的培训，培训结束后提供培训证书。

4、付款方式

（1）合同签订后 20 日内以转账的方式支付 50%的合同款项；每月末考核后支付该月的费用。

(2)供应商须向采购人出具合法有效完整的完税发票及凭证资料进行支付结算。

（3）(跨年度合同）若因财政资金未及时下达等客观原因导致不能及时支付合同款项的，采购人可以延期支付，在财政资金下达后及时支付所有应付款项。

5、违约责任

（1）采购人供应商双方必须遵守本项目合同并执行合同中的各项规定，保证本项目合同的正常履行。

（2）如因供应商工作人员在履行职务过程中的的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、

由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任。

6、售后服务：服务期内出现质量问题（或紧急情况），成交供应商在接到通知后0.5时内响应，2小时提出解决方案，4小时内到达现场，24小时内排除故障；如逾期未到场处理，则采购人有权另行聘请他人处理，且服务期内产生的一切费用均由成交供应商承担。

7、验收标准及要求

（一）验收方案

（1）验收组织方式：自行验收

（2）是否邀请本项目的其他供应商：否

（3）是否邀请专家：否

（4）是否邀请服务对象：否

（5）是否邀请第三方检测机构：否

（6）履约验收程序：一次性验收

（7）履约验收时间：投标人提出验收申请之日起30日内组织验收

（二）技术履约验收内容

按照本项目采购文件在“服务要求”中的约定执行。

（三）商务履约验收内容

按照本项目采购文件在“商务要求”中的约定执行。

（四）验收组织的其他事项

（1）符合国家、行业标准、四川省地方标准规定的验收标准。

（2）其他未尽事宜应严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《政府采购需求管理办法》（财库〔2021〕22号）的要求进行验收。