第三章 谈判项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1、采购项目概况

本项目共一个包，采购等级保护测评项目。

3.2、服务内容及服务要求

3.2.1 服务内容

采购包 1：

采购包预算金额（元）: 600,000.00

采购包最高限价（元）: 600,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	网络安全等级保护测评	1.00	600,000.00	项	软件和信息技术服务业	否	否	否	否

3.2.2 服务要求

采购包 1：

标的名称：网络安全等级保护测评

参数性质	序号	技术参数与性能指标
★	1	**（一）、项目目标及范围** 根据《中华人民共和国网络安全法》、《四川省卫生健康行业网络安全等级保护工作实施方

案》川卫函（2019）11号、川卫办信统便函【2023】21号《关于加强医疗卫生机构网络安全和数据安全工作的通知》的指导要求，对游仙区妇幼保健院的相关信息系统开展等级保护测评服务和网络安全服务工作，每月进行网络安全评估，同时出具安全分析报告包括防攻击、容灾、数据安全的内容。服务期间开展一次攻防演练，出具演练报告。全员网络安全培训≥1次/年，网络安全管理人员的技术培训≥1次/年，网络安全培训以及重保服务；突发网络安全事件10分钟响应，1小时内到达现场进行应急咨询处理。本次服务相关信息系统情况如下：

序号	信息系统名称	定级
1	HIS系统	3级
2	LIS系统	3级
3	PACS系统	3级
4	电子病历	3级
5	微信公众号	2级
6	官方网站	2级
7	院感系统	2级
8	护理平台	2级
9	体检系统	2级
10	手麻系统	2级

（二）、项目需求

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度，以

		及云计算安全、移动互联安全、物联网安全、工控制系统安全等扩展方面的要求。 Ⅰ、等保测评具体服务内容包括： （1）协助业主单位进行信息系统的信息安全等级定级和备案工作。 （2）差距测评，至少包括： 安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心方面的安全测评。 安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。 形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以、整改意见。 （3）协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。 （4）等级测评，至少包括： 按照等级保护相关

		标准对系统从安全技术、安全管理等方面进行等级测评工作。 编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。 Ⅱ、安全分析内容包括： 模拟黑客的攻击行为，在不影响业务的情况下从攻击者的角度来发现系统存在的安全隐患和网络风险，出具包含防攻击、容灾、数据安全内容的《安全分析报告》，从取得测试证书后每月开展 1 次，共计 12 次。 Ⅲ、攻防演练内容包括： 1 筹备阶段 协助企业组建实战攻防演练工作小组，小组人员，并依据各自职责明确分工，制定工作小组的沟通、协作、响应流程。参照行业内先进的防御体系理论模型，结合企业当前的安全建设情况，为企业提供体系优化方案，完善企业的技术防御体系，为企业有效地应对有组织的实战攻击奠定技术基础。 2 检查阶段 协助企业进行互联网未知资产的排查、正常暴露面的漏洞排查、泄露在互联网上的敏感信息、源代码和企业员工个人信息等内容的排查。同时对企业内部网络及重要信息系统开展安全检查

		及加固，包括内网漏洞整改、内部弱口令整改、内部失陷主机整改、访问控制策略优化、集权系统安全评估及加固、重要业务系统安全评估及加固等相关工作。 3 安全值守 通过防护类安全设备如：防火墙、WAF 对网络攻击、系统漏洞、Web 漏洞等利用进行检测、识别和分析。 3.1 应急处置 现场防守小组当检测到安全事件时，即可在现场进行实时分析与研判，当发现有针对性或攻击方正在攻击所保护的信息系统时立刻采取行动，封锁攻击行为。同时输出响应应急处置报告。 3.2 攻击溯源 在对安全事件进行原因初步分析和影响抑制后，防守小组将对当前安全事件进行进一步处理并对证据进行留存。由企业运维人员协助防守小组成员，从网络流量情况、主机系统日志、网站服务日志、业务应用日志、数据库日志等，结合已有安全设备数据，分析入侵方式，还原造成安全事件的过程。同时输出溯源报告。 4 演练完毕后，根据整个演练情况进行分析汇总并提交《xx 网络攻防演练总结》，针对安全事件现象、处理过程、处理结果进行陈述，同时对入侵原因进行分析，并给

出相应的安全加固建议和安全防御体系建设指导。

Ⅳ、网络安全培训：

服务内容：安排具备《注册信息安全专业人员》证书的工程师，提供面向全院职工、面向信息科的专业技术人员两个层次人员的培训会各一次，培训内容包含：网络安全意识、相关法律法规以及网络安全技术等。

Ⅴ、重保服务：

服务内容：针对每年的重大活动以及上级单位检查期间,提供专项保障服务,通过事前发现与预防，事中处理与恢复，保障后总结改进三步为用户重保提供保驾护航，具体包括安全驻场值守、安全应急支持、安全监控等服务。

（三）、服务内容指标

三级系统通用指标要求

分类	**子类**	**基本要求**
安全物理环境	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问	机房出入口应配置电子门禁系统，控制、鉴别和记

				控制	录进入的人员。
				防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； b）应将通信线缆铺设在隐蔽安全处； c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
				防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地； b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
				防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； c）应对机房划分区域进行管理，区域

					和区域之间设置隔离防火措施。
				防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
				防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施； b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
				温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
				电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备； b）应提供短

					期的备用电力供应，至少满足设备在断电情况下的正常运行要求； c）应设置冗余或并行的电力电缆线路为计算机系统供电。
				电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰； b）应对关键设备实施电磁屏蔽。
			安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要； b）应保证网络各个部分的带宽满足业务高峰期需要； c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

					e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
				通信传输	a）应采用校验技术或密码技术保证通信过程中数据的完整性； b）应采用密码技术保证通信过程中数据的保密性。
				可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
			安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行

					通信； b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
				访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许

					/拒绝数据包进出； d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
				入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报

					警。
				恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
				安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d）应能对远程访问的用

					户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
				可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
			安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动

					退出等相关措施； c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
				访问控制	a）应对登录的用户分配账户和权限； b）应重命名或删除默认账户，修改默认账户的默认口令； c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； d）应授予管理用户所需的最小权限，实现管理用户的权限分离； e）应由授权主体配置访问控制策略，

					访问控制策略规定主体对客体的访问规则； f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
				安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d）应对审计进程进行保护，防止未经

					授权的中断。
				入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序； b）应关闭不需要的系统服务、默认共享和高危端口； c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
				恶意	应采用免受恶意代码攻

				代码防范	击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
				可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
				数据完整性	a）应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b）应采用校验技术或密码技术保证

					重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
				数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
				数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能； b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地； c）应提供重

				要数据处理系统的热冗余，保证系统的高可用性。
			剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
			个人信息保护	a）应仅采集和保存业务必需的用户个人信息； b）应禁止未授权访问和非法使用用户个人信息。
		安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行

					的异常处理、数据和设备的备份与恢复等。
				审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
				安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对

					主体进行授权，配置可信验证策略等。
				集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； e）应对安全策路、恶意代码、补丁升级等安全相关事项进行集中管理； f）应能对网络中发生的各类安全事件进行识别、

				报警和分析。
		安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
			管理制度	a）应对安全管理活动中的主要管理内容建立安全管理制度； b）应对管理人员或操作人员执行的日常管理操作建立操作规程； c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
			制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定； b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
			评审和	应定期对安全管理制度的合理性和

				修订	适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
			安全管理机构	岗位设置	a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
				人员配备	a）应配备一定数量的系统管理员、审计管理员和安全管理员等； b）应配备专职安全管理员，不可兼任。

				授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
				沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c）应建立外

					联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
				审核和检查	a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
			安全管理人员	人员录用	a）应指定或授权专门的部门或人员负责人员录用； b）应对被录用人员的身份、安全背景、专业资格或资质等进

					行审查，对其所具有的技术技能进行考核； c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
				人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
				安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； c）应定期对不同岗位的人员进行技能考核。

				外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； c）外部人员离场后应及时清除其所有的访问权限； d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
			安全建设管理	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性

					进行论证和审定； c）应保证定级结果经过相关部门的批准； d）应将备案材料报主管部门和相应公安机关备案。
				安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
				产	a）应确保网

				品采购和使用	络安全产品采购和使用符合国家的有关规定； b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
				自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； c）应制定代码编写安全规范，要求开发人员参照规范编写代码； d）应具备软件设计的相关文档和使用指南，并对文档使用进

					行控制； e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； g）应保证开发人员为专职人员、开发人员的开发活动受到控制、监视和审查。
				外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码； b）应保证开发单位提供软件设计文档和使用指南； c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
				工程实施	a）应指定或授权专门的部门或人员负责工程实

					施过程的管理； b）应制定安全工程实施方案控制工程实施过程； c）应通过第三方工程监理控制项目的实施过程。
				测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
				系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； b）应对负责运行维护的技术人员进行相应的技能培训； c）应提供建设过程文档和运行维护文档。
				等级	a）应定期进行等级测评，

				测评	发现不符合相应等级保护标准要求的及时整改； b）应在发生重大变更或级别发生变化时进行等级测评； c）应确保测评机构的选择符合国家有关规定。
				服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定； b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
			安全运维管理	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

					b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
				资产管理	a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
				介质管理	a）应将介质存放在安全的环境中，对各类介质进

					行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
				设备维护管理	a）应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理； b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据

					应加密； d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
				漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； b）应定期开展安全测评，形成测评报告，采取措施应对发现的安全问题。
				网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

					c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计

					日志，操作结束后应同步更新配置信息库； h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
				恶意代码防	a）应提高所有用户的防恶意代码意识，对外来计算机或存储

				范管理	设备接入系统前进行恶意代码检查等； b）应定期验证防范恶意代码攻击的技术措施的有效性。
				配置管理	a）应记录和保存基本配置信息，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； b）应将基本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。
				密码管理	a）应遵循密码相关国家标准和行业标准； b）应使用国家密码管理主管部门认证核准的密码技术和产品。
				变更管理	a）应明确变更需求，变更前根据变更需求制定变

					更方案，变更方案经过评审、审批后方可实施； b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
				备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等； b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
				安全事	a）应及时向安全管理部门报告所发

				件处置	现的安全弱点和可疑事件； b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训； d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
				应急预案管理	a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； b）应制定重要事件的应

					急预案，包括应急处理流程、系统恢复流程等内容； c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； d）应定期对原有的应急预案重新评估，修订完善。
				外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定； b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； d）应在与外包运维服务商签订的协议中明确所

				有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

二级系统通用指标要求

分类	子类	基本要求
安全物理环境	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； b）应将通信线缆铺设在隐蔽安全处。
	防雷击	应将各类机柜、设施和设备等通过接

					地系统安全接地。
				防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
				防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
				防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
				温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
				电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备； b）应提供短

				期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
			电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
		安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
			通信传输	应采用校验技术保证通信过程中数据的完整性。
			可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计

				记录送至安全管理中心。
		安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
			访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
			入侵	应在关键网络节点处监

				防范	视网络攻击行为。
				恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
				安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
				可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并

				在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
		安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
			访问控制	a）应对登录的用户分配账户和权限； b）应重命名或删除默认账户，修改默认账户的默认口令； c）应及时删除或停用多

					余的、过期的账户，避免共享账户的存在； d）应授予管理用户所需的最小权限，实现管理用户的权限分离。
				安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
				入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序； b）应关闭不需要的系统服务、默认共享和高危端口； c）应通过设

					定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
				恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
				可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形

				成审计记录送至安全管理中心。
			数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
			数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能； b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
			剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
			个人信息保护	a）应仅采集和保存业务必需的用户个人信息； b）应禁止未授权访问和非法使用用户个人信息。
		安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b)应通过系

					统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
				审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
			安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
				管	a）应对安全

				理制度	管理活动中的主要管理内容建立安全管理制度； b）应对管理人员或操作人员执行的日常管理操作建立操作规程。
				制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定； b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
				评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
			安全管理机构	岗位设置	a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； b）应设立系统管理员、审

					计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
				人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
				授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
				沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c）应建立外联单位联系

				列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
			审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
		安全管理人员	人员录用	a）应指定或授权专门的部门或人员负责人员录用； b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
			人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
			安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
			外部人	a）应在外部人员物理访问受控区域

				员访问管理	前先提出书面申请，批准后由专人全程陪同，并登记备案； b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案;； c）外部人员离场后应及时清除其所有的访问权限。
			安全建设管理	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； c）应保证定级结果经过相关部门的批准； d）应将备案材料报主管部门和相应公安机关备案。
				安	a）应根据安

				全方案设计	全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b）应根据保护对象的安全保护等级进行安全方案设计； c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
				产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定； b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
				自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b）应在软件开发过程中对安全性进

					行测试，在软件安装前对可能存在的恶意代码进行检测。
				外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码； b）应保证开发单位提供软件设计文档和使用指南。
				工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理； b）应制定安全工程实施方案控制工程实施过程。
				测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b）应进行上线前的安全性测试，并出具安全测试报告。
				系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

					b）应对负责运行维护的技术人员进行相应的技能培训； c）应提供建设过程文档和运行维护文档。
				等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； b）应在发生重大变更或级别发生变化时进行等级测评； c）应确保测评机构的选择符合国家有关规定。
				服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定； b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
			安全运维管理	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、

					空调、温湿度控制、消防等设施进行维护管理； b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等； c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
				资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
				介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的

					归档和查询等进行登记记录。
				设备维护管理	a）应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理； b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
				漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
				网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b）应指定专门的部门或人员进行账户管理，对申请账户、建立

					账户、删除账户等进行控制； c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定； d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
				恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶

					意代码库升级、恶意代码的定期查杀等； c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
				配置管理	应记录和保存基本配置信息，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。
				密码管理	a）应遵循密码相关国家标准和行业标准； b）应使用国家密码管理主管部门认证核准的密码技术和产品。
				变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。
				备份与	a）应识别需要定期备份的重要业务

				恢复管理	信息、系统数据及软件系统等； b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
				安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件； b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录

				处理过程，总结经验教训。
			应急预案管理	a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
			外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定； b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

（四）、完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

《系统等级保护测评问题汇总及整改意见报告》

《网络安全等级测评报告》及过程资料

《xx 网络攻防演练总结》

《安全分析报告》

《培训课件资料》

（五）、技术标准和规范

《中华人民共和国

		计算机信息系统安全保护条例》(国务院令 147 号) 《信息安全等级保护管理办法》（公通字[2007]43 号） 《计算机信息系统安全保护等级划分准则》（GB17859-1999） 《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020） 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019) 《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019） 《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018） 《信息安全技术信息安全风险评估规范》（GB/T20984-2022） **（六）、安全要求** 成交供应商在项目实施过程中，必须遵守以下技术原则： 1 保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。 2 标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。 3 规范性原则：供应商的工作中的过程和文档，具有很好的规范性，

		可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。 4 可控性原则：等保测评服务的进度要按照招标文件 的要求，保证采购方对于测评工作的可控性。 5 整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。 6 安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。 （七）测评机构资质及人员要求： （1）从事信息系统检测评估相关工作人员无违法犯罪记录（**投标时提供承诺函**）。 （2）测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。 （3）项目经理 1 名：具有网络安全等级测评师(高级)证书或者信息安全等级测评师(高级)证书**（投标时提供证书扫描件）**；现场测评工程师 2 名：具有网络安全等级测评师（中级）证书或者信息安全等级测评师（中级）证书**（投标时提供证书扫描件）**。项目经理及现场测评工程师须驻场测评 1 个月，

		并承诺签订合同前提供以上人员证书原件及在职证明（**投标时提供“**项目经理及现场测评工程师驻场测评 1 个月**”**及“签订合同前提供项目经理及现场测评工程师证书原件及在职证明”的**承诺函**）。

3.2.3 人员配置要求

采购包 1：
按 3.2.2 服务要求中相关要求执行。

3.2.4 设施设备要求

采购包 1：
/

3.3、商务要求

3.3.1 服务期限

采购包 1：
自合同签订之日起 365 日

3.3.2 服务地点

采购包 1：
采购人指定地点。

3.3.3 验收标准和方法

采购包 1：
严格按照《绵阳市财政局关于进一步做好政府采购项目履约验收工作的通知》(绵财采〔2021〕15 号)的要求进行验收，由采购人组织验收。

3.3.4 支付方式

采购包 1：
分期付款

3.3.5 支付约定

采购包 1： 付款条件说明： 采购人收到供应商出具的纸质版盖章的《网络安全等级测评报告》后 ，达到付款条件起 30 日内，支付合同总金额的 60.00%。
采购包 1： 付款条件说明： 完成所有服务内容并通过采购验收后 ，达到付款条件起 30 日内，支付合同总金额的 40.00%。

3.3.6 违约责任与解决争议的方法

采购包 1：
按合同约定执行

3.4 其它要求

1、服务期限：接到采购人测评通知后 60 日内完成测评工作，并取得测评报告，出具报告后，开始计算服务周期，服务周期为 1 年，每月开展 1 次网络安全分析，出具《安全分析报告》，共计 12 次。 2、投标人所投价格包含服务、人工、税金、成果文件等实施本项目所需的一切费用，招标人不再支付任何其他费用。 注：3.3.1 服务期限与 3.4 其他要求中所述服务期限不一致时以 3.4 其他要求中相关要求为准。