网络安全等级保护测评采购项目

一、采购项目基本情况

在完成网络安全等级保护服务与配套设施建设项目后，按照国家信息安全等级保护制度的要求，对现有信息化基础设施进行全面网络安全等级测评。测评过程中将重点检查信息系统的安全防护能力，包括网络架构安全性、系统漏洞防范、数据加密保护、访问控制管理、入侵防御能力、日志审计系统等关键环节的实现程度。针对测评中发现的不足之处，医院将及时制定针对性修正方案，最终达到国家规定的网络安全等级保护三级标准。这一目标的实现将为医院信息化建设奠定坚实的安全基础，确保医疗数据安全，保障医疗服务的连续性和可靠性，维护患者信息安全，符合国家信息安全监管要求，项目预算为35万元。

附件

采购需求明细表（服务）

编制单位： 编制时间： 2025年6月23日

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目及品种名称 | 质量技术 标准 | 计量 单位 | 采购 数量 | 单价 （元） | 预算金额  （万元） | 交货(服务)地点 | 交付（实施）  时间 | 采购方式  建议 |
|  | 合计 |  | 年 | 1 | 350000/元 | 35 |  |  |  |
| 一 | 网络安全等级保护  测评服务（三级） | 见附件 | 年 | 1 | 180000/年 | 18 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |
| 二 | 网络安全培训服务 | 见附件 | 年 | 2 | 45000/年 | 4.5 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |
| 三 | 网络安全咨询服务 | 见附件 | 年 | 1 | 5000/年 | 0.5 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |
| 四 | 应急响应服务 | 见附件 | 年 | 1 | 20000/年 | 2 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |
| 五 | 攻防演习服务 | 见附件 | 年 | 1 | 40000/年 | 4 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |
| 六 | 数据分级分类服务 | 见附件 | 年 | 1 | 60000/年 | 6 | 甘肃兰州 | 自合同签订之日起5个自然日内提供服务 | 竞争性  谈判 |

附件

技术要求

#### 一、服务内容和标准

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | | **主要服务内容** |
| 1 | 网络安全等级保护测评服务 | 定级备案 | 整理编写HIS、LIS、PACS、EMR系统定级备案所需资料，并提交相关部门进行备案； |
| 安全技术测评 | 按照三级系统等保测评的要求，技术层面从以下五个层面进行测评：安全物理环境、安全通信网络、安全计算环境、安全区域边界、安全管理中心； |
| 安全管理测评 | 按照三级系统等保测评的要求，管理层面从以下五个层面进行测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理； |
| 渗透测试服务 | 对系统提供渗透测试服务，通过模拟恶意黑客的攻击方法，来评估计算机系统的安全状况。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析； |
| 漏洞扫描服务 | 漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为； |
| 信息系统安全整改建议咨询 | 提供本项目所涉及被测系统的安全整改咨询建议，并出具整改建议；对项目建设整改期提供必要的安全咨询建议服务； |
| 安全整改复测 | 提供整改建议，提供至少两次复测服务，最终以复测后的结果出具报告； |
| 等级保护测评报告 | 按照系统现状出具等级保护测评报告，每个系统一份，纸质版至少两份，电子版至少一份。 |
| 2 | 网络安全培训服务 | | 提供通用的网络安全意识培训服务，并根据医疗行业特性、业务系统特性、工作部门特性，制定定制化网络安全意识培训。提供3人次注册信息安全专业人员CISP培训与认证服务，以及2人次注册信息安全专业人员渗透工程师CISP-PTE培训与认证服务。 |
| 3 | 网络安全咨询服务 | | 提供信息安全领域相关政策要求、技术问题的咨询服务，技术问题答疑。包含网络安全体系规划建设咨询服务、网络安全建设整改咨询服务。 |
| 4 | 应急响应服务 | | 根据我方实际情况，建立、健全网络与信息安全运行应急工作机制。 |
| 5 | 攻防演习服务 | | 针对网络安全攻防演练、重大活动安全保障（如国家护网行动、攻防对抗等）场景设计，提供攻防演习服务。通过模拟真实攻击场景，结合主动防御、威胁监测、应急响应等手段，构建实战化安全防护体系，确保核心业务系统在攻防对抗中的安全性、稳定性和业务连续性。 |
| 6 | 数据分级分类服务 | | 通过对数据的自然属性、医疗业务价值及潜在风险进行综合分析，实现数据安全管控与高效利用的平衡，构建科学的数据资产管理机制。基于行业标准与实际数据现状制定数据识别规则，识别目标数据存储对象中的数据情况。输出包含但不限于《数据分类分级服务报告》、《数据安全管理制度》、《数据分类分级指南》、《数据资产清单》等文档；基于国家/医疗行业标准，以及我方合规性和安全性需求，建立成体系的数据安全管理制度，包含但不限于方针战略、管理办法、实施细则以及管理流程与表单等。 |

**1.等级保护测评服务**

**1.1.测评原则**

**符合性原则**

遵守国家27号文件提出的积极防御、综合防范的方针和等级保护的原则，应严格贯彻《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发【2003】27号）、《关于信息安全等级保护工作的实施意见》（公通字【2004】66号）、《信息安全等级保护管理办法》（公通字【2007】43号）等文件提出的各项要求。

**规范性原则**

服务方案与实施计划应依据国家、行业的相关标准进行设计。项目中将参考并遵循如：《GB∕T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB∕T 25058-2019 信息安全技术 网络安全等级保护实施指南》、《GB∕T 28448-2019 信息安全技术 网络安全等级保护测评要求》、《GB∕T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》、《GB∕T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》等相关信息安全标准和行业规范，同时充分吸收同类行业的成功经验，并结合项目自身特点，规范化的完成本次服务。

**可控性原则**

应遵循行业相关规范及项目管理要求，从以下几个方面对项目进行把控：

人员可控性：中标供应商应委派专门的项目经理，负责本项目的各项事宜。项目经理依据项目需求组建最优项目小组，明确各小组成员的服务角色与职责。在征得我方的同意后，开展各方面的测评工作。

工具可控性：中标供应商所使用的技术工具均须事我方相关信息系统负责人进行报备，并且提前介绍工具的使用目的及使用方法并进行测试，确保工具安全可靠。

项目过程可控性：本次服务项目应严格遵守网络安全等级保护测评相关要求及行业项目管理规范开展本次工作，确保项目过程的可控性。

**整体性原则**

中标供应商将按照我方提供的项目范围开展服务实施工作，从范围、深度上满足我方的要求。项目实施内容包括等级保护基本要求涉及的各个层面（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、安全管理制度、安全管理人员、安全管理机构、安全建设管理、安全运维管理），保证测评工作的全面性、测评结果的客观性以及整改建议的专业性。

**最小影响原则**

为了保障项目实施过程中尽可能小的影响系统和网络的正常运行，中标供应商从项目管理和技术应用两个层面，将安全服务可能对被测系统的正常运行所带来的影响降到最低，确保不会对当前运行的网络和业务系统产生显著影响（系统性能明显下降、网络拥塞、服务中断），同时在现场服务前协助我方做好备份和应急工作。

**保密原则**

中标供应商将与我方签署此项目特定的保密协议，对项目过程数据和结果数据严格保密。在进行数据交换时，使用数据加密软件及专用的加密U盘，防止明文数据共享带来的安全隐患。同时中标供应商应依据我方的要求，对相关文档、数据资料设置保管生命周期，在保管生命周期结束之后，项目组成员将彻底销毁所有和项目有关的数据和文档资料，并承诺不做任何恢复动作。

**1.2.测评范围**

（1）新医技楼和办公楼数据中心机房 （包括其环境、设备和设施等）、以及院内所有楼宇各楼层弱电井；

（2）存储被测系统重要数据的介质的存放环境；

（3）办公场地；

（4）整个系统的网络拓扑结构；

（5）安全设备，包括防火墙、入侵检测设备和防病毒网关等；

（6）边界网络设备，包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）等；

（7）对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚层交换机、路由器等；

（8）承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（8）管理终端和主要应用系统终端；

（9）能够完成不同业务的各个应用系统；

（10）业务备份系统；

（11）信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（12）涉及到信息系统安全的所有管理制度和记录。

**1.3.测评内容**

计划完成医院4个重要业务信息系统的三级等级保护测评。

等级测评的现场实施过程由单元测试和整体测评两部分构成。对应《基本要求》各安全控制点的测评称为单元测试，具体可分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理十项测试任务。

整体测评是在单元测评的基础上，通过进一步的分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。

测评的内容包括但不限于以下内容：

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、安全管理中心等五个方面的安全测评；

安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

基础环境安全测评

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

本次等级保护测评服务，主要依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》展开，具体情况如下：

**安全物理环境测评**

安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

安全物理环境测评实施过程涉及10个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 物理位置选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
|  | 物理访问控制 | 通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
|  | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
|  | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
|  | 防火 | 通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
|  | 防水和防潮 | 通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
|  | 防静电 | 通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
|  | 温湿度控制 | 通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
|  | 电力供应 | 通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
|  | 电磁防护 | 通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

**表1-1安全物理环境测评指标描述**

**安全通信网络测评**

安全通信网络测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅来获取证据（如相关措施的部署和配置情况），用于测评信息系统的网络安全保护。

安全通信网络测评涉及的测评对象主要为网络设备和安全。

安全通信网络测评实施过程涉及3个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 网络架构 | 测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
|  | 通信传输 | 测评通信过程中的完整性、保密性等。 |
|  | 可信验证 | 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，并在应用程序的关键执行环节进行动态可信验证。 |

**表2-1安全通信网络测评指标描述**

**安全区域边界测评**

安全区域边界测评主要涉及边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证6个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 边界防护 | 测评分析信息系统网络边界安全防护的状况。 |
|  | 访问控制 | 测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。 |
|  | 入侵防范 | 测评分析信息系统对攻击行为的识别和处理情况。 |
|  | 恶意代码和垃圾邮件防范 | 测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。 |
|  | 安全审计 | 测评分析信息系统审计配置和审计记录保护情况。 |
|  | 可信验证 | 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，并在应用程序的关键执行环节进行动态可信验证。 |

**表3-1安全区域边界测评指标描述**

**安全计算环境测评**

安全计算环境测评主要涉及身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护11个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 身份鉴别 | 检查服务器的身份标识与鉴别和用户登录的配置情况。 |
|  | 访问控制 | 检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
|  | 安全审计 | 检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
|  | 入侵防范 | 检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
|  | 恶意代码防范 | 检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。 |
|  | 可信验证 | 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，并在应用程序的关键执行环节进行动态可信验证。 |
|  | 数据完整性 | 测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。 |
|  | 数据保密性 | 测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。 |
|  | 数据备份恢复 | 测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
|  | 剩余信息保护 | 测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 |
|  | 个人信息保护 | 测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。 |

**表4-1安全计算环境测评指标描述**

**安全管理中心测评**

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控4个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 系统管理 | 测评信息系统的系统管理员对系统的管理情况。 |
|  | 审计管理 | 测评信息系统的安全审计员对系统的审计情况。 |
|  | 安全管理 | 测评信息系统的安全管理员对系统的安全策略的配置情况。 |
|  | 集中管控 | 测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。 |

**表5-1安全管理中心测评指标描述**

**安全管理制度测评**

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订4个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 安全策略 | 测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。 |
|  | 管理制度 | 测评信息系统管理制度在内容覆盖上是否全面、完善。 |
|  | 制定和发布 | 测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
|  | 评审和修订 | 测评信息系统管理制度定期评审和修订情况。 |

**表6-1安全管理制度测评指标描述**

**安全管理机构测评**

安全管理制度测评主要涉及岗位设置、人员配备、授权和审批、沟通和合作、审核和检查5个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 岗位设置 | 测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
|  | 人员配备 | 测评信息系统各个岗位人员配备情况。 |
|  | 授权和审批 | 测评信息系统对关键活动的授权和审批情况。 |
|  | 沟通与合作 | 测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
|  | 审核和检查 | 检查信息系统安全工作的审核和测评情况。 |

**表7-1安全管理机构测评指标描述**

**安全管理人员测评**

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理4个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 人员录用 | 测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
|  | 人员离岗 | 测评信息系统人员离岗时是否按照一定的手续办理。 |
|  | 安全意识教育和培训 | 测评是否对人员进行安全方面的教育和培训。 |
|  | 外部人员访问管理 | 测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

**表8-1安全管理人员测评指标描述**

**安全建设管理测评**

安全建设管理测评主要涉及定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择10个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 定级和备案 | 测评是否按照一定要求确定系统的安全等级并完成备案工作。 |
|  | 安全方案设计 | 测评系统整体的安全规划设计是否按照一定流程进行。 |
|  | 产品采购和使用 | 测评是否按照一定的要求进行系统的产品采购。 |
|  | 自行软件开发 | 测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
|  | 外包软件开发 | 测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
|  | 工程实施 | 测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
|  | 测试验收 | 测评系统运行前是否对其进行测试验收工作。 |
|  | 系统交付 | 测评是否采取必要的措施对系统交付过程进行有效控制。 |
|  | 等级测评 | 测评是否依据国家要求完成等级测评和整改工作。 |
|  | 服务供应商选择 | 测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

**表9-1安全建设管理测评指标描述**

**安全运维管理测评**

安全管理人员测评主要涉及环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理14个方面的安全保护能力，具体测评指标描述如下表所示：

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 环境管理 | 测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
|  | 资产管理 | 测评是否采取必要的措施对系统的资产进行分类标识管理。 |
|  | 介质管理 | 测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
|  | 设备维护管理 | 测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
|  | 漏洞和风险管理 | 测评是否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。测评是否定期开展安全测评。 |
|  | 网络和系统安全管理 | 测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
|  | 恶意代码防范管理 | 测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
|  | 配置管理 | 测评是否记录和保存系统的基本配置信息 |
|  | 密码管理 | 测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
|  | 变更管理 | 测评是否采取必要的措施对系统发生的变更进行有效管理。 |
|  | 备份与恢复管理 | 测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
|  | 安全事件处置 | 测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
|  | 应急预案管理 | 测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
|  | 外包运维管理 | 测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。 |

**表10-1安全运维管理测评指标描述**

**2.攻防演习防守服务**

自查阶段：通过资产与风险暴露面梳理、安全扫描、渗透测试等手段为重保提供基础数据和攻击面总体安全态势，为后续重大活动提供决策依据，保证医疗秩序有序进行。

加固阶段：通过标准化的检查复核和协助清除已发现风险。主要包括一轮或多轮的专项安全检查工作进行反复的风险识别与加固工作。

进阶阶段：推进实战工作部署，包括确认应急预案与演练各应急场景，可能的情况下组织开展实战攻防演习等工作，来检验前期工作成效，查缺补漏。

保障阶段：安排技术人员现场监测值守，并配备应急响应队伍应急处突，防止对重大活动造成影响，同步提供总结与报告等服务。

**3.安全培训服务**

**3.1.安全意识培训**

**（1）法律法规解读**

安全意识培训的首要环节是对相关法律法规的深入解读。所提供的培训内容涵盖了国家和地方关于安全的最新法律法规，包括但不限于《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等。通过专业的安全服务专家，对法律法规进行详细解读，确保参训人员能够准确理解并遵守相关法律法规，从而在日常工作中避免触犯法律红线，降低法律风险。

**（2）安全事件案例分析**

通过分析安全事件案例，帮助参训人员从真实的事件中吸取教训，理解安全事件发生的背景、原因、过程以及造成的后果。通过案例学习，参训人员能够更加直观地认识到安全意识的重要性，从而在实际工作中时刻保持警惕，预防类似事件的发生。

**3.2.安全技术培训**

**（1）渗透技术培训**

在安全技术培训方面，应提供专业的渗透技术培训。渗透测试是一种安全评估方法，通过模拟黑客攻击的方式，评估计算机系统、网络或Web应用的安全性。培训课程应涵盖渗透测试的整个流程，包括信息收集、漏洞分析、攻击模拟等环节。通过实际操作和案例分析，参训人员将掌握如何发现和利用系统漏洞，以及如何采取有效措施进行防范。

**（2）应急技术培训**

应急技术是处理突发事件和安全危机的关键技术。课程旨在教授参训人员如何在面对安全事件时迅速做出反应，采取有效的应急措施。内容包括但不限于应急响应流程、事故调查与分析、数据恢复、系统重建等。通过模拟演练和实战训练，参训人员将能够熟练掌握应急处置技能，确保在真实的安全事件中能够最大限度地减少损失。

**4.数据分级分类服务**

**4.1概述**

数据资产作为一种无形资产，需要经过系统化的识别与定义之后才能够成为数据安全管控的对象，依据GB/T 37988-2019数据安全能力模型针对数据生命周期安全的定义，数据分类分级是数据采集安全过程域的第一个基本实践，是数据生命周期安全管理的第一步，经有数据分类分级确定了数据类别与级别的数据在其生命周期中的各个环节才具备落实安全控制措施的可能。

近年来，随着信息技术进步与医疗信息化系统应用程度进一步加深，我院沉淀了大量医疗数据。一方面，需要有效甄别合理化的数据使用需求，明确关键环节的技术标准，确定使用新型技术的范围；另一方面需要结合医疗行业发展变化，有效识别新增风险隐患，持续加强数据安全管理，建立健全数据管理制度，采取必要的数据安全防护措施，切实维护系统安全运行。

采用规范的数据分类、分级方法，有助于我院理清数据资产、确定数据重要性或敏感度，并针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据开放共享。

（1）数据管理混乱问题

我院数据种类繁多、来源广泛，通过数据分类分级，可按照业务、类别、性质等维度对数据进行梳理归类，再进一步划分级别。使数据有序化，提高数据查找、使用和维护的效率，降低数据管理成本。

（2）数据安全风险问题

不同类型和级别的数据面临的安全风险不同，若采用统一的安全防护措施，要么存在防护不足导致数据泄露，要么造成资源浪费。数据分类分级后，可针对不同级别的数据制定差异化的安全策略。对于高敏感级别的数据，实施严格的访问控制、加密传输和存储等措施；对于低敏感级别的数据，可适当简化安全措施。这有效降低数据泄露、篡改等安全风险，保护我院数据安全。

（3）合规遵从问题

数据分类分级有助于我院明确各类数据的合规要求，确保数据处理活动合法合规。例如，对于涉及个人信息的数据，按照相关法规进行严格管理和保护，避免因违规操作引发法律纠纷。

（4）数据共享与流通障碍问题

在与卫健委、医保局、兄弟单位进行数据共享时，由于不清楚数据的敏感程度和使用限制，可能导致数据共享困难或过度共享。数据分类分级明确了数据的属性和使用范围，为数据共享提供指导。对于可以公开或共享的数据，可顺畅地进行流通和合作；对于受限数据，则在确保安全和合规的前提下进行有条件的共享，促进数据价值的最大化利用。

（5）数据价值挖掘不足问题

我院拥有大量数据，但由于缺乏有效的管理和分类，难以准确识别和利用有价值的数据。通过数据分类分级，可清晰地了解数据的价值所在，优先对高价值数据进行深度分析和挖掘。

（6）数据存储和处理成本问题

不合理的数据存储和处理方式会增加组织的成本。通过数据分类分级，可根据数据的重要性和使用频率，选择合适的存储介质和处理方式。对于重要且经常使用的高价值数据，采用高性能的存储设备和快速的处理算法；对于低频使用的历史数据或低价值数据，可采用低成本的存储方式。这在保证数据可用性的同时，降低数据存储和处理成本。

**4.2.数据分类分级方法**

**线分类法：**将分类对象按选定的若干个属性或特征，逐次分为若干层级，每个层级又分为若干类别。同一分支的同层级类别之间构成并列关系，不同层级类别之间构成隶属关系。同层级类别互不重复，互不交叉。

**面分类法：**将所选定的分类对象依据其本身的固有的各种属性或特征，分成相互之间没有隶属关系即彼此独立的面，每个面中都包含了一组类别。将某个面中的一种类别和另外的一个或多个面的一种类别组合在一起，可以组成一个复合类别。面分类法是并行化分类方式，同一层级可有多个分类维度。

**混合分类法：**将线分类法和面分类法组合使用，克服这两种基本方法的不足，得到更为合理的分类。混合分类法的特点是以其中一种分类方法为主，另一种做补充。

**4.3.数据分级分类流程**

第一阶段业务细分：按照业务线将各个业务进行细分，通过划分管理主体和管理范围，明确各管理部分有哪些子类业务；

第二阶段数据归类：收集数据并编写成数据表/数据项/数据文件等形式作为数据的分类；

第三阶段级别判定：按数据泄露后的影响对象、影响范围以及影响程度对数据做数据的分类分级判定。

**4.4.数据资产梳理**

数据资产梳理是数据分类分级的重要基础工作，通过全面梳理组织的数据资产，明确数据的来源、类型、存储、使用情况以及流动情况，方便后续分类分级工作结果更加准确。

**业务流程梳理**

（1）确定数据在业务流程中的流动路径，包括数据的输入、处理、输出和反馈等各环节流转详情，涵盖内外部数据，绘制出数据流图；

（2）梳理数据在不同系统或模块之间的传输接口，如API、ETL工具等。

**关联性分析**

（1）对数据资产进行关联性分析，明确不同数据集之间的相互关系。

（2）采用基于图模型的关联分析和基于统计模型的相关性分析，生成数据关联图。

**输出数据资产目录**

（1）形成数据资产目录，列出核心数据或核心的数据资产。

（2）数据资产目录采用主题-类目-表级的三级目录结构，并遵循统一的命名规则、编码规则。

**4.5.数据分类**

数据分类根据数据管理和使用需求，结合已有数据分类基础，灵活选择业务属性将数据细化分类。具体参考以下步骤开展行业领域数据分类。

（1）明确数据范围：首先将业务线作为第一层级，根据其下部门、岗位的不同数据管理范围，划分第二层级。同一层级中，每个类别的数据表、数据项、数据文件应由不同的部门、岗位管理。

（2）细化业务分类：对业务系统进行细化分类，包含但不限于诊疗业务平台、医技业务平台、医辅业务平台、管理业务平台、后勤业务平台、教学科研平台、统一信息平台、新技术支撑平台、军队事业平台。

（3）业务属性分类：选择合适的业务属性，对关键业务的数据进行细化分类。

（4）确定分类规则：梳理分析各关键业务的数据分类结果，根据医疗行业领域数据管理和使用需求，确定数据分类规则。

采取“业务线—关键业务—业务属性分类”的方式给出数据分类规则。对关键业务的数据分类结果进行归类分析，将具有相似主题的数据子类进行归类。

**4.6.数据分级**

根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为核心数据、重要数据、一般数据三个级别。

数据分级是为了保护数据安全，具体可参考以下步骤进行数据分级。

（1）确定分级对象：确定待分级的数据，如数据项、数据集、衍生数据等。数据项通常表现为数据库表某一列字段，数据集是由多个数据记录组成的集合，如数据库表、数据库一行或多行记录集合、数据文件等。

（2）分级要素识别：结合业务系统数据特点，按照数据分级要素识别数据涉及的分级要素情况。

（3）数据影响分析：结合数据分级要素识别情况，分析数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能影响的对象和影响程度。

（4）综合确定级别：按照级别确定规则和综合确定级别要求，综合确定数据级别。

**4.7.风险规避措施**

数据分类分级工作应实行质量控制，以保证分类分级结果的准确有效。在数据分类分级各个阶段，一是要根据相应的法规要求和管理规范开展分类分级工作；二是保证数据采集的准确性和有效性，同时保证数据分类分级细则制定的贴合性；三是充分了解我院所处的行业背景及安全特性要求，以及对被分类分级数据资产所承担的业务和自身流程的理解。

这里的数据调研过程风险主要指识别过程、人工梳理过程中存在的数据泄露和破坏风险。进行数据调研前，中标供应商需要提前向我院提交当前工作计划，经过双方确认后，双方共同为数据调研做好相应风险规避措施，再进行数据采集，防止因为采集数据（从业务系统、传输设备上），造成信息化系统中的相关数据泄露、破坏风险。

数据调资产调研计划完成后，数据采集人员需要提交工作确认单，经过双方确认数据采集工作后，开展下一步工作。可以通过工作确认，保证数据采集的有效性、准确性，防止进行重复性工作和工作的遗漏，同时避免上述风险。

**4.8.成果报告**

输出文档包含但不限于《数据分类分级服务报告》、《数据安全管理制度》、《数据资产清单》、《数据分类分级指南》等。

**5.其他要求**

项目实施过程中遇到不可控因素造成项目未在规定日期内完成的，需与甲方共同商定，确保工程顺利完成。乙方需在项目实施前阐述完善的实施方案、人员和技术保障方案，在施工过程中须根据甲方实际流程调整相应步骤。乙方提供本项目的实施方案应包括货物供货、运输配送、安装调试、验收、项目培训方案各个环节。确保实施方案完整、详细具体、合理可行、操作性强并符合本项目实际情况。

为确保项目顺利完成与施工质量，要求乙方至少指定1名项目总监，1名项目经理，同时配置相应的程序开发和安装实施技术工程师若干，以及其他辅助支持人员全职参与本项目的工作。

项目总监和项目经理应具备计算机行业高级职称资质，技术工程师则需具备计算机相关专业背景，并具备现场完成程序开发工作以及服务器、网络安全设备等基础设施的安装调试能力。

项目实施过程中遇到不可控因素造成项目未在规定日期内完成的，需与甲方共同商定，确保工程顺利完成。乙方需在项目实施前阐述完善的实施方案、人员和技术保障方案。

#### 二、履约验收

（一）服务分期考核验收

1.甲方按合同约定的分期考核内容、标准对乙方实施的服务进行验收。

2.合同约定的分期考核内容包括日常督导考核、岗位督查、专项检查、特殊部位或者场所检查、满意度调查、合同履约综合评价等。

（1）日常督导考核。甲方按考核标准对乙方实施的服务进行日常巡查，发现问题告知乙方，并做好督查记录。甲方根据乙方改进情况和问题的严重程度，按考核标准对乙方进行处理。

（2）岗位督查。甲方按考核标准检查乙方服务人员到岗情况，发现缺岗的，甲方按考核标准对乙方进行处理。

（3）专项检查。甲方针对服务的重点、难点问题或管理要求进行专项检查，双方共同记录。乙方对甲方在专项检查中发现问题，应当予以整改。乙方问题多次出现或整改不力的，甲方按考核标准进行处理。

（4）特殊部位或者场所检查。甲方对服务区域的特殊部位或者场所进行检查，发现问题甲方按考核标准对乙方进行处理。

（5）满意度调查：甲方按合同约定的考核时间组织服务对象或者委托第三方对服务效果进行满意度调查。甲方根据调查结果，按考核标准对乙方进行奖励或处罚。

（6）合同履约综合评价：甲方按合同约定的考核时间对乙方合同履行情况进行综合评价，综合评价可作为款项支付以及续签合同的依据。

3.服务分期考核内容、标准：包含但不限于服务人员管理、日常服务质量、网络安全培训质量、应急响应服务质量、攻防演习服务质量、数据分级分类服务质量；

4.服务分期考核验收的其他要求：包含但不限于人员考勤、服务态度、专业程度、工作效率、文档规范程度等；

（二）验收

1.乙方完成全部服务内容并具备验收条件，由乙方向甲方提出验收申请，由甲方组织验收，出具验收报告。

2.项目验收中，国家有强制性规定的，按国家规定执行。招标文件、乙方的承诺及投标文件、本合同及补充协议均成为本项目验收依据。验收过程中产生纠纷或存在异议的，由国家认可的检测机构检测，出具检测报告。

3.项目验收不合格，由乙方返工直至合格，连续2次项目验收不合格的，甲方可终止合同，由此带来的一切损失由乙方承担。

附件

经济要求

★一、服务时间、地点

服务期限：自合同签订之日起5个自然日内提供服务；

服务实施的期限：自合同签订之日起1年；

服务地点：甘肃省兰州市七里河区333号；

服务方式：现场交付。

★二、资金结算

本项目分阶段付款，第一阶段，自合同签订生效1个月后，乙方提供符合国家税务部门规定的技术服务增值税发票等结算资料，采购单位支付合同总金额的20%；第二阶段,网络安全等级保护测评通过后，乙方提交结算收据等资料，采购单位支付合同总金额的50%；第三阶段,自服务交付验收合格后，乙方提交结算收据等资料，采购单位支付合同总金额的剩余30%。

（二）乙方应当向甲方支付合同项下的违约金或赔偿金时，甲方有权从上述任何一笔应当付款中予以扣除。

（三）在结算过程中，乙方出具虚假发票或其他虚假材料的，按照提供虚假材料情况处理。

（四）未经军队采购平台合同管理信息系统编号或者未按照要求进行备案的物资工程服务采购合同书，不得办理支付手续。

（五）若后期军队审计部门、军队采购管理部门、纪检监察部门等职能部门抽查，提出价格虚高等问题，乙方需无条件配合甲方进行调查，积极提供相关审价资料，若审价结果低于合同价，乙方需无条件退还虚高款项；若审价结果高于合同价，按合同价进行结算。

★三、履约保证金

（1）本合同履约保证金为合同金额的5%，乙方应当在签订合同前10日内缴纳履约保证金。

（2）乙方在合同履行过程中存在违约行为，合同被甲方终止的，甲方有权没收乙方履约保证金。

（3）履约保证金在合同最终支付结算时无息返还（完成一年服务内容并达到验收合格后无息返还;若中途变更中标供应商，在支付当年度服务费时一并无息返还）。

（4）乙方应当向甲方支付合同项下的违约金或赔偿金时，甲方有权从履约保证金中予以扣除。

四、售后服务

无。

★五、知识产权

投标供应商应保证使用方在使用乙方交付的服务成果时，不受第三方侵权指控。同时，投标供应商不得向第三方泄露采购单位提供的技术文件等资料。

六、物资编目编码、打码贴签要求

本项目为服务类项目，所含配套物资有编目编码、打码贴签要求的，投标供应商应按采购单位资产管理部门要求予以配合，自行承担相关费用。

★七、合同履约要求

（一）违约责任：

（1）乙方未经甲方同意而延期履行的，应当向甲方偿付违约金，违约金每天按合同金额的5‰计算，违约金最高限额为合同金额的5%。如果达到违约金最高限额时仍不能履行，或因延期履行影响甲方任务实施，甲方可以终止合同，而由此给甲方造成的实际损失，乙方应当给予足额赔偿。

（2）乙方不能满足合同约定的服务内容和标准等要求，给甲方造成损失的，乙方应当赔偿甲方损失。甲方未按照设备原厂技术手册要求进行操作，造成设备故障的，甲方应当承担额外的维修费用。

（3）甲方需按约定及时足额支付服务款，未按约定及时足额支付服务款时，甲方向乙方偿付违约金。每迟付一天按合同金额的1‰向乙方偿付违约金，违约金最高限额为合同金额的 5%。

（4）如因不可抗力事件导致一方无法履行合同，该方应立即书面通知对方，并在合理期限内提供权威机构出具的证明。受影响方应尽力减轻不可抗力事件所造成的影响。如法律对不可抗力有其他规定，或合同迟延履行后发生不可抗力事件，本条款不免除违约方的责任。

（二）争议处理：

合同履行过程中，发生争议时，甲方和乙方协商解决。协商不一致的，甲方或者乙方向采购机构负责合同履约的部门反映情况，请求第一次调解处理；第一次调解不成功的，向军级单位采购管理部门或者同等权限的采购管理部门请求第二次调解处理。

调节不成功的，甲方或者乙方向甲方所在地仲裁机构提起仲裁或向甲方所在地人民法院提起诉讼。诉讼费由承担责任的一方承担。在诉讼期间，除正在诉讼的部分外，合同的其他部分应继续执行。