**网络安全等级保护评测(2024、2025年)）**

**目 录**

[1. 项目简介 1](#_Toc176428575)

[1.1. 项目名称 1](#_Toc176428576)

[1.2. 项目建设单位 1](#_Toc176428577)

[1.3. 项目建议书编制依据 1](#_Toc176428578)

[1.4. 项目概况 1](#_Toc176428579)

[1.5. 主要结论和建议 1](#_Toc176428580)

[2. 项目建设单位概况 3](#_Toc176428581)

[2.1. 项目建设单位与职能 3](#_Toc176428582)

[2.2. 项目实施机构与职责 4](#_Toc176428583)

[3. 项目建设的必要性 5](#_Toc176428584)

[3.1. 项目背景和依据 5](#_Toc176428585)

[3.2. 网络安全等级保护评测(2024、2025年)标准 5](#_Toc176428586)

[3.3. 现有网络安全等级保护评测状况 6](#_Toc176428587)

[3.4. 项目建设的意义和必要性 6](#_Toc176428588)

[4. 需求分析 8](#_Toc176428589)

[4.1. 安全保密与自主可控 8](#_Toc176428590)

[4.2. 系统需求分析 11](#_Toc176428591)

[5. 建设方案 15](#_Toc176428592)

[5.1. 建设原则和策略 15](#_Toc176428593)

[5.2. 项目建设目标 15](#_Toc176428594)

[5.3. 国内外网络安全等级保护评测技术对比 15](#_Toc176428595)

[5.4. 技术方案 15](#_Toc176428596)

[6. 环保、消防、职业安全、职业卫生和节能 22](#_Toc176428597)

[6.1. 环境影响和环保措施 22](#_Toc176428598)

[6.2. 消防措施 22](#_Toc176428599)

[6.3. 职业安全和卫生措施 22](#_Toc176428600)

[6.4. 节能目标及措施 23](#_Toc176428601)

[7. 项目实施进度 24](#_Toc176428602)

[8. 项目风险分析 25](#_Toc176428603)

[8.1. 协调风险及控制 25](#_Toc176428604)

[8.2. 项目技术风险控制 25](#_Toc176428605)

[8.3. 社会影响风险及控制 25](#_Toc176428606)

[附表1：项目软件配置清单及预算 27](#_Toc176428607)

[附表2：项目详细配置清单 28](#_Toc176428608)

# 项目简介

## 项目建议书编制依据

1、通过中讯邮电咨询设计院有限公司现场调查收集的资料，分别包括了信息科和相关科室人员的建议。

2、为进一步贯彻落实《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）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）等文件的精神，提高我国基础信息网络和重要信息系统的信息安全保护能力和水平，自2007年开始，从国家层面开始推动我国的政府、金融、电力、电信、交通等基础行业在全国范围内组织开展重要信息系统安全等级保护定级、备案、测评、整改工作。通过将等级化方法和安全体系方法有效结合，设计一套等级化的信息安全保障体系，是适合我国国情、系统化地解决大型组织信息安全问题的一个非常有效的方法。金融、电力、广电、医疗、教育、电子政务、人社等行业主管部门均发文要求开展等级保护工作。

## 项目概况

随着信息化不断发展，近年来，信息安全问题日益突显，安全事件频频发生。我国国家互联网信息办公室公布的数据表明，中国是网络攻击的受害国，由其是针对政府的攻击由其严峻，现在的网络攻击已经上升到了带政府背景的有组织的攻击。信息系统同时面临各种外部威胁和内部威胁，病毒、黑客入侵、间谍软件、网络钓鱼、SQL代码注入、垃圾邮件、恶意扫描、内部人员误操作、内部人员的信息安全意识不强、内部人员利用职务之便窃取机密信息，可谓内忧外患。

随着中央网络安全和信息化领导小组办公室正式成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，《中华人民共和国网络安全法》的颁布，国家对信息安全工作高度重视，信息安全已经是国家安全的重要组成部分，已经上升到与政治安全、经济安全、领土安全等并驾齐驱的战略高度。

## 主要结论和建议

结论：《网络安全法》颁布以来，全国各地都有应未履行等级保护工作的执法案例。《网络安全法》第二十一条明确规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

建议：为有利于该项目的顺利开展，建议及时组织相关信息化技术人员成立医院信息化项目工作小组，继续完善项目建设方案，加快项目推进步伐。并建议落实项目建设资金，继续本项目的工程设计及概算编制、招标文件编制及相关招投标工作，争取2024年底竣工验收。

# 项目建设单位概况

## 项目实施机构与职责

### 信息科

1、按照国家标准制定《信息安全管理制度》，明确了信息安全管理的范围、目标、职责、机构、程序、方法和保证措施等，保障了医院信息系统合法、正常、安全可靠的运行。明确医院信息安全管理的目标，以保护医院核心业务及数据不被非法窃取或损坏、保障信息处理和传输的安全和可靠性为主要目标；阐述医院各级负责人间的安全管理职责和制度指导责任，建立并实行完整的信息安全管理体系，确保所有相关人员都能履行自己的信息安全管理职责；详细规定医院信息安全管理制度的制定、执行、评估、维护等重要流程和闭环；以医院用户角色的分配，赋予用户不同的权限，确保用户分工明确，权限分明，数据规范，信息可靠性，以及切实防止非法窃取、分发、利用医院信息资源；明确规定网络设备、安全设备的购置、配置及管理要求，防范黑客和病毒的恶意攻击，对网络业务和操作人员加强管理和监督；制定合理、可行的备份计划和备份周期，确保数据备份完整、可靠。在系统或数据造成严重损坏或丢失时，按备份计划对数据再次备份，以防止数据永久性丢失。

2、定期对信息安全管理制度进行评估，发现及时制度漏洞，并加以修正完善以确保管理制度更加合理、科学、完善，真正达到预期的管理效果。

# 项目建设的必要性

## 项目背景和依据

等保测评，全称信息安全等级保护测评，‌是指根据国家标准《信息安全等级保护基本要求》(GB/T 22239-2008)和《‌信息安全技术 信息系统安全等级保护评估规范》‌(GB/T 28448-2012)，‌对信息系统的安全等级、‌安全需求、‌安全措施和安全管理进行综合评估，‌以确定信息系统是否符合相应的安全等级要求的过程。‌

等保测评的主要目的是确保信息系统的安全性和可靠性，通过评估信息系统的各项安全措施是否达到预定的安全标准，来保障信息系统的稳定运行和数据的安全。这个过程包括但不限于对信息系统的物理安全、网络安全、系统安全、应用安全以及管理安全等方面的综合评估。评估的内容可能包括但不限于访问控制、数据加密、身份认证、日志管理、漏洞扫描等多个方面，以确保信息系统的安全防护措施能够有效地抵御外部攻击和内部误操作带来的风险。

此外，等保测评还涉及到对信息系统安全管理措施的评估，包括但不限于安全策略的制定、安全教育和培训、应急响应计划的制定和实施等，以确保信息系统的安全管理能够有效地应对各种安全威胁和风险。通过等保测评，可以帮助医院或组织识别和解决信息系统中的安全隐患，提高信息系统的安全防护能力，保障信息的机密性、完整性和可用性。

## 网络安全等级保护评测(2024、2025年)标准

在相关国家标准或医疗标准中有规定的规范条文，提供的测评标准均应遵循公安部、卫健委相关文件要求和采购人的相关文件要求，所用的标准必须是其最新版本；如果这些标准内容矛盾时，应按最高标准的条款执行或按双方商定的标准执行；

《中华人民共和国网络安全法》

《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)

《信息安全等级保护管理办法》(公通字[2007]43号)

 GB/T 22240-2020：《信息系统安全等级保护定级指南》

GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

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 20984-2022：《信息安全技术 信息安全风险评估方法》。

## 现有网络安全等级保护评测状况

医院是中国医疗服务体系的主体。国家卫生部部长陈竺指出:“公立医院是体现公益性、解决基本医疗、缓解人民群众看病就医困难的主体，矛盾问题比较集中。要加强其公益性，就要扭转过于强调医院创收的倾向，让其成为群众医治大病、重病和难病的基本医疗服务平台。”积极响应国家网络安全等级保护制度，致力于提升医院信息系统的安全防护能力。近年来，医院紧跟国家网络安全战略步伐，不断完善网络安全等级保护制度，并引入了一系列先进的测评工具和技术，如自动化漏洞扫描、渗透测试、数据加密技术、访问控制管理系统等，以提高测评效率和准确性。

## 项目建设的意义和必要性

等保测评的重要性，等保测评是对信息系统的安全性能和等级的评估体系，它通过对信息系统的各项安全要素进行评估，包括硬件设施、软件系统、网络架构等，来确定系统的安全等级，并提出相应的安全增强建议。等保测评的重要性体现在它可以帮助机构全面认识系统的安全现状，提供一个客观的安全等级评估标准，提升安全管理水平。

等保测评面临的挑战，尽管取得了显著进展，但医院在推进等级保护测评工作时也面临着多方面的挑战：技术更新迅速、人才短缺、资源分配不均、合规性与实用性平衡等问题。

结论：等保测评的实践，不仅提升了我医院的信息安全水平，也为全国网络安全治理提供了可借鉴的模式和经验。面对不断变化的网络安全威胁，持续深化等保测评，加强技术创新与合作，将是未来网络安全建设的重要方向。

# 需求分析

## 安全保密与自主可控

### 安全保密配套设施建设

等保测评需要的安全设备主要包括以下几类：

1.防火墙（Firewall）：用于对网络流量进行过滤和监控，防止未经授权的访问和恶意攻击。

2.入侵检测和防御系统（Intrusion Detection and Prevention System，IDPS）：用于检测和防御网络中的入侵行为，包括外部入侵和内部滥用。

3.安全信息和事件管理系统（Security Information and Event Management，SIEM）：用于集中管理和分析网络设备和系统的安全事件和日志信息，快速发现和响应安全威胁。

4.数据加密和安全传输设备：用于对敏感数据进行加密和安全传输，防止数据泄露和窃取。

5.传输层安全协议（Transport Layer Security，TLS）设备：用于确保网络通信的安全性和私密性，防止数据被篡改或窃取。

6.身份认证和访问控制设备：用于确保用户身份的合法性，并对用户的访问进行控制和管理。

7.安全审计和合规性检测设备：用于对网络设备和系统进行安全审计和合规性检测，确保其符合相关安全标准和规范。

8.安全管理平台：用于集中管理和监控各种安全设备和系统，提供统一的安全管理和操作界面。

以上设备只是一些常见的等保测评安全设备，实际使用的设备可能根据具体的需求和环境而有所不同。

### 监管体系的融入

监督制度：等保测评机构应建立监督和审计制度，对测评过程进行全面监督和审计，确保测评结果的准确性和公正性。监督和审计制度应包括对测评人员的监督、测评过程的审计、测评结果的审核等方面。

资源管理制度：等保测评机构需要管理大量的业务和数据资源，应该建立资源管理制度，确保资源的规范配置和使用。包括基础设施、硬件和软件设备的管理，获得授权的鉴定人员、评测工具的管理等内容。

### 内控安全设计

测评工作本身也会引入安全风险，必须加强测评过程中的风险控制。项目实施前，双方应充分讨论并明确测评对系统可能带来的风险和隐患，确定测评对象、测评方法和工具，并制定应急恢复措施。

（1）操作的申请和监护

测评操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

（2）人员与数据管理

重视保密工作，加强测评过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备（系统）或临时搭建的模拟环境进行测评，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评实施前制定应急预案，加强系统在线应急处置能力。

### 安全保密检测评估改

安全部署：等保测评机构应按照安全管理要求采取必要的技术手段，加强其系统、网站和数据库等关键资源的安全防护。建立安全管理制度，实现安全漏洞及时发现与修复，给用户提供更可靠、保密性较强的服务。

保密制度：等保测评机构应建立保密制度，对涉及客户隐私和医院机密的信息进行严格管理，确保客户隐私和医院机密不被泄露。

### 国产自主可控要求的落实

网络安全的核心是技术安全，技术安全的一条核心原则就是关键的核心技术要自主可控。核心技术是我们最大的“命脉”， 实现网络安全，要尽可能把关键核心技术掌握在自己手里，才能避免处于被动地位，“网信领域具有高垄断性，新进入市场的国产软硬件如果不能打破垄断，就没法实现替代”。

过去我们对自主可控没有形成制度支撑，因而不能及时发现短板，容易被人“卡脖子”。现在我国技术自主可控的情况依然堪忧，迄今为止，我国政府采购等活动中仍有不利于自主可控的情况，影响了重要部门的网络安全。

目前“穿马甲”情况严重，也就是将不能自主可控的外国技术，假冒国产自主可控技术，混入政府采购和重要领域，（可能）成为特洛伊木马。我国亟需制订自主可控测评评估标准并由专门机构实施，形成制度保障。

自主可控测评还需要适应形势的发展，例如现在根据美国法律，如果根源在美国的技术发展，就会被计入属地比重，范围包括 IP 与相关核心技术，若美国技术成分占比超过25%，就会受到美国法律的管辖，这种情况也要在自主可控测评中加以考虑。

实践证明，如果网络安全空间不能实现自主可控的话，将有很大的风险。换句话说，只要不是实现完全自主可控，就有随时被“黑” 的可能性。

自主可控需制订客观、科学的测评标准，并由第三方机构实行测评；在关系到网信安全的重要场合，自主可控测评可起“一票否决”作用。为了客观地、科学地评估自主可控程度，有关部门提出了实行多维度测评的要求，即除了以往已经实施的“质量测评”和“安全测评”外，再增加了“自主可控测评”。

因此，多维度测评包含：自主可控测评，即对产品/服务/系统的自主可控性进行评估，该评估既能够针对CPU、OS等核心技术产品，也能够针对其他软硬件或服务，甚至也可针对一个信息系统或一项信息基础设施；质量测评，即对产品/服务/系统的功能、性能等技术指标进行测评；安全测评，即对产品/服务/系统的安全性进行测评，此种测评往往是实施“等保”“分保”制度的必要内容。

### 进度管控和保密管理

本次等保测评必须完成对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

本次等保测评必须签订保密协议，未经用户书面许可，不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

测评过程中提供的相关资料，医院与测评单位相互承担保密责任。

## 系统需求分析

### 环境适配

在等保测评中，安全计算环境控制项的内容在技术部分中是最多的，涉及到主机层面、应用层面、数据层面、备份恢复层面，这使得安全计算环境在等保建设中显得尤为重要。

通过对安全计算环境建设关键点的总结，进行等保三级建设时，安全计算环境相对等保二级建设强化了双因子认证、强制访问控制、数据完整性及保密性等方面的要求，这需要我们在进行等保建设时注重对网络、对业务系统的梳理，应用符合医院网络特点、业务特点的等保建设方案，根据医院等保定级进行建设，满足等保2.0及医院自身安全计算环境防护需求。

### 效能

通过等保测评，我医院加强需要网络安全保护，确保信息系统的安全稳定运行，这为医院信息化技术水平的健康发展提供坚实的基础；通过等保测评的实施提高我医院的信息安全水平，保障我医院医疗服务的连续性和稳定性，从而提升公共服务的效率和质量。

等保测评在智慧医院建设中具有举足轻重的作用。它不仅确保了数据的安全与隐私保护，还推动了数据的共享与整合，提升了医院整体治理的效能。面对新技术环境下的挑战，我们需要不断加强技术研究和培训，建立全面的安全风险评估体系，加强数据安全和隐私保护，并严格遵守相关法律法规和标准。只有这样，我们才能更好地应对信息安全的挑战，推动智慧医院的信息化发展。

### 完善体系

在数字化转型浪潮中，医院业面临着前所未有的机遇与挑战。信息安全作为医院发展的生命线，其重要性日益凸显。信息安全等级保护测评（简称“等保测评”）作为我国网络安全领域的基本国策之一，正驱动着医疗行业构建起坚固的全方位安全体系，确保医院平稳航行于数字蓝海。

根据医院业务性质、信息系统重要程度及面临的风险，精准评估并确定等保等级，为后续工作奠定基础。

强化基础安全防护，物理与环境安全：加强机房安全，确保物理访问控制和环境监测。网络架构安全：实施分区隔离、访问控制列表（ACL）、防火墙策略等，构建安全网络边界。

数据安全与隐私保护，加密技术：采用国产商用密码算法，实现数据传输与存储的加密保护。数据生命周期管理：从数据产生到销毁的全过程实施安全管理，确保数据合规性。

应用与系统安全，代码审计与漏洞扫描：定期进行应用代码审计，运用自动化工具扫描系统漏洞并及时修复。权限管理：实施最小权限原则，确保员工仅能访问完成工作所必需的信息资源。

应急响应与持续改进，建立应急响应机制：制定详尽的应急预案，建立快速响应团队，定期进行实战演练。持续监控与审计：部署安全运营中心（SOC），实现24小时安全监控，定期进行等保自评与第三方测评。

等保测评不仅是医疗行业必须跨越的合规门槛，更是推动医院安全能力跃升的催化剂。通过构建并不断完善全方位的安全体系，医院不仅能够有效应对外部威胁，还能在激烈的市场竞争中稳固根基，把握住信息化发展的黄金机遇。

### 提升能力

通过展示其在网络安全方面的努力和成就，我医院吸引更多的医疗服务能力和患者，促进了区域经济的多元化发展。

等保测评为大数据、云计算等新兴技术的应用提供安全保障，有助于培育新的医疗业务增长点和业态。

### 引领发展与成果共享

等保测评在促进产业发展方面发挥着重要作用，主要体现在以下几个方面：

资源有效利用：等保测评有助于医院明确信息安全的需求和重点，从而优化信息安全资源的配置。医院可以根据等保测评的结果，合理分配人力、物力和财力，确保关键信息系统的安全。

重点保障：等保测评强调对基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的保护。这有助于引导医院和社会资源向这些关键领域倾斜，提高整体的信息安全防护水平。

合规性要求：等保测评是国家对信息安全管理的重要要求之一。通过等保测评，医院可以确保其信息系统符合国家和地方的相关法规、政策以及标准的要求，避免因违规而面临的法律风险和经济损失。

标准化推进：等保测评的实施促进了信息安全标准化的推进。通过制定和实施统一的等保标准和规范，可以确保不同行业、不同领域的信息系统在安全防护方面达到一致的水平，提高整个社会的信息安全防护能力。

发现并修复系统中存在的漏洞和安全隐患，提高系统的安全性；确定系统的安全评级和等级保护要求，为后续的保密工作提供依据；完善医院的信息安全管理体系，促进信息安全工作的规范化和持续性；建立与相关部门和团队的合作机制，形成信息共享和风险协同防控的机制。

### 转化应用

医疗行业通过等保测评，着重保护电子病历、个人健康信息的安全。应用策略围绕数据加密存储、严格权限管理、医疗设备安全审计展开，确保医疗服务的连续性和患者隐私的保密性。

### 成本控制与管理

提前规划与准备，医院在面临等保测评时，首要任务是提前了解相关政策要求和测评流程，制定详细的规划和准备方案。明确测评的目标、范围、时间节点等关键要素，可以有效避免因准备不足而导致的额外成本和时间浪费。同时，通过内部培训或外部咨询，提升员工的安全意识和技能，为后续工作打下坚实基础。

合理选择测评机构，测评机构的选择直接关系到测评的质量和成本。医院应综合考虑机构的资质、经验、服务质量以及报价，选择具有丰富经验和专业技术的测评机构。这不仅能确保测评结果的准确性和权威性，还能在一定程度上降低因频繁整改而产生的额外成本。

精准定位等保级别和测评范围，医院应根据自身业务特点和信息资产价值，精准定位等保级别和测评范围。对于非关键系统，可以考虑采用简化措施或进行风险评估后适当降低要求，避免过度投入。

成本控制策略与技术创新，在硬件升级和软件采购方面，医院应优先考虑性价比高的产品和方案，避免盲目追求高端配置。此外，通过技术创新和流程优化，可以降低运维成本和人力成本。例如，采用自动化工具进行漏洞扫描和风险评估，减少人工干预，提高工作效率。

### 建设内容优化调整

符合国家法律法规要求，通过等保测评，医院能够确保信息系统符合国家安全标准，避免因违规而遭受的法律风险和处罚。这不仅有助于维护医院的合法权益，还能提升医院的社会责任感和公信力。

提升客户信任度，在数据泄露和网络攻击频发的背景下，医院的信息安全保障能力越来越重视。通过等保测评，医院能够提升患者对医院的信任度，增强市场竞争力。

降低经济损失和声誉损失，

网络安全事件往往会给医院带来巨大的经济损失和声誉损失。等保测评帮助医院识别并整改安全隐患，增强抵御网络攻击和数据泄露的能力，从而有效降低潜在的经济损失和品牌声誉损害。

促进内部管理优化，等保测评不仅关注技术层面的安全控制，还对医院的安全管理体系和流程进行全面评估。通过测评，医院可以发现内部管理中的薄弱环节，促进内部管理流程的优化，提升整体运营效率。

# 建设方案

## 建设原则和策略

为贯彻落实国务院147号令和中办27号文件，公安部会同有关部委出台了系列的文件以及具体工作的指导意见和规范,并在全国范围内组织完成了一系列工作。目前，信息安全等级保护工作已经进入安全建设整改阶段，公安部印发了《关于开展信息系统等级保护安全建设整改工作的指导意见》(公信安[2009]1429)，明确提出:“依据信息安全等级保护有关政策和标准，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求。

## 项目建设目标

为了贯彻国家对网络安全保障工作的要求,医院委托第三方测评机构对医院信息系统进行安全等级保护测评。测评工作将依据等级保护的相关管理规范、技术标准，实施安全测评工作。安全测评范围包括被测系统相关的网络设备、安全设备、服务器设备等;测评内容涵盖安全物理环境、安全通信网络,安全区域边界、安全计算环境、安全管理电心以及信息安全管理等方面。测评完成后针对系统中存在的安全问题进行风险分析，提出整改意见，并最终形成安全等级测评报告。

## 国内外网络安全等级保护评测技术对比

无对比，由国内有网络安全等级保护评测技术资质的企业完成。

## 技术方案

信息系统的等级保护测评技术服务项目，包括评估和测评技术服务要求、加固整改要求、验收要求。

等级保护测评工作需提交单位和公安部门认可的《等级保护测评报告》。

### 系统架构

测评内容主要包括两个方面:一是单元测评,测评指标与《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)相应等级的基本要求完全一致:二是系统整体测评，主要测评分析信息系统的整体安全性。

单元测评包括安全技术测评和安全管理测评两大部分，其中:

安全技术测评层面主要包含: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。

安全管理测评层面主要包含: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。

整体测评在单元测评的基础上进行进一步测评分析,在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

### 系统流程

网络安全等级保护测评流程如下图所示：



### 运行环境要求

等保测评的运行环境要求包括安全物理环境、网络安全、系统安全、应用安全、数据安全等多个方面。

安全物理环境要求包括机房场地的选择应具有防震、‌防风和防雨等能力，‌避免设在建筑物的顶层或地下室，‌并采取防水和防潮措施。‌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。‌设备或主要部件应标识不易除去的标识，‌通信线缆应铺设在隐藏安全处，‌各类机柜、‌设施和设备等应通过接地系统安全接地，‌机房应设置火灾自动消防系统，‌并能自动检测火情、‌自动报警和自动灭火。‌此外，‌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，‌采取措施防止雨水渗透和机房内水蒸气结露，‌设置温湿度自动调节设施，‌保持适宜的温度、湿度和洁净度等环境条件。‌

网络安全要求包括网络拓扑结构应具有一定的抗攻击能力，‌避免单一节点故障对整个网络的影响。‌应配备防火墙、‌入侵检测/防御系统、‌病毒防护系统等网络安全设备，‌实施访问控制策略，‌对不同用户进行分级管理，‌限制非法访问和恶意攻击。‌

系统安全涉及操作系统安全、‌数据库安全和应用软件安全。‌应使用安全漏洞较少的操作系统，‌如Linux、‌Unix等，‌并及时更新系统补丁和安全加固。‌使用安全的数据库管理系统，‌如Oracle、‌MySQL等，‌定期备份数据和更新密码等敏感信息。‌应用软件应经过漏洞扫描和安全测试，‌避免存在漏洞和恶意代码。‌

应用安全要求应用系统实现身份认证功能，‌对用户进行身份识别和权限控制，‌避免未经授权的访问。‌采用数据加密技术对敏感数据进行加密存储和传输，‌实现安全审计功能，‌记录用户操作日志和异常行为，‌以便及时发现和处理安全事件。‌

数据安全要求定期备份数据，‌保证备份数据的可用性和完整性。‌敏感数据采用数据加密技术进行加密存储和传输，‌不再使用的数据进行销毁处理，‌避免数据泄露和信息残留。‌

这些要求确保了信息系统的物理和环境安全、网络安全、系统安全、应用安全和数据安全，为等保测评提供了一个安全可靠的运行环境。

### 系统功能介绍

本次测评工作清单如下：

| 序号 | 名称 | 单位 | 数量 | 备注 |
| --- | --- | --- | --- | --- |
| 1 | HIS系统等级保护测评(3级) | 项 | 1 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |
| 2 | 电子病历系统等级保护测评(3级) | 项 | 1 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |
| 3 | PACS系统等级保护测评(2级) | 项 | 1 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |

本次测评指标和对象选择须符合国标《GB/T 28448-2019网络安全等级保护测评要求》的相关要求。具体测评要求如下：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：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和系统运维管理等五个方面的安全测评。

安全物理环境测评对象为对对支持运行的基础物理设施环境以及相关的硬件设备和介质等，包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等方面的安全状况。

安全通信网络是对通信网络的构成组件进行测评。通信网络的构成组件负责支撑信息系统进行网络互联，为等级保护对象各个部分进行安全通信传输，一般包括网络设备、通信链路以及网络拓扑等。测评内容主要包括网络架构、通信传输和可信验证。

安全区域边界需要对边界防护、访问控制、入侵防范、恶意代码和反垃圾邮件防范和安全审计等方面进行测评。

安全计算环境需要对身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等方面进行测评。

安全管理中心需要对系统管理、审计管理、安全管理和集中管控等方面进行测评。

安全管理制度测评是对系统的安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

安全管理机构测评是对整个管理组织架构和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

人员安全管理测评是对人员管理模式提出的安全控制要求，包含对人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

安全建设管理测评是对系统建设过程中的系统定级和备案、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、安全服务商选择等情况进行测评。

系统运维管理测评是对系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等情况进行测评。

（1）随着等级保护测评标准的变化，至复测评开始前，若系统发生变更，应答人需负责专家评审及当地网安部门备案工作。

（2）上级管理部门对采购人进行专项、重大事件、重要节日检查时，应答人需配合检查工作，同时对检查中发现的问题进行处理并做好记录。

（3）在遇到网络安全事件时，应答人需根据要求进行网络安全事件溯源工作，需要在半小时内安排至少中级测评师以及渗透人员进行安全排查工作。

（4）根据采购人需求，在整体网络安全项目改造实施过程中提供对每个实施部分板块的整体标准要求进行规范，在项目实施前期，中期，后期安排技术人员进行安全基线检查，确保整体网络安全项目实施顺利。

(5)应答人根据采购人需求，结合客户单位实际情况，开展信息安全培训工作，强化安全意识，了解安全相关法律法规，提升客户有关信息安全方面的基本常识，确保相关人员树立信息安全观念，提高信息安全风险意识，增强信息安全责任感。

（6）根据密码法的要求，应答人需要提供商用密码应用安全技术相关咨询，帮助采购人了解最新的商用密码应用相关政策及标准规范，并协助采购人发现有重要网络与信息系统的密码应用现状、风险及需求，针对发现的密码应用风险结合采购人实际密码需求提出合理的商用密码应用合规建议，为后续密码建设改造工作提供支撑。

根据国家等级保护相关标准，安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，应答人提供整改建议书，配合采购人根据测评范围进行整改实施。

# 环保、消防、职业安全、职业卫生和节能

## 环境影响和环保措施

本项目建设不对环境造成影响，不产生污染。但要保证所选设备和机房局部空间无污染，符合消防安全要求，选用绿色电脑、外设和绿色节能照明光源。机房建设工程遵循国家机房设计标准规范的要求。

项目场地建设遵循建设部颁布的《民用建筑工程室内环境污染控制规定》（GB50352），国家质量监督检验检疫总局颁布的《室内装饰装修材料有害物质限量》等国家标准。

场地建设后，系统运行过程中不产生有害废气、废水、废渣等物质，不会污染环境。而空调、风机等硬件基本选用低噪声设备，并采取双层玻璃、隔离屏蔽等有效的消声措施。电磁辐射完全符合国际标准，对人体健康并不造成较大威胁。

## 消防措施

在项目建设中严格按照国家消防规范《建筑内部装修设计防火规范》（GB50222）、《中华人民共和国消防法》等国家法律和规定。在各个区域内都装自动喷淋系统和报警装置，配置七氟丙烷灭火器，以及适量手提式二氧化碳气体灭火器。

## 职业安全和卫生措施

项目建设根据有关国家和部门标准规范，采取的主要安全卫生措施有：

1）所有用电设备的金属外壳、金属底座、电缆金属铠装层、电缆保护管以及所有金属支架均与接地装置连接，设有安全接地，配电系统设有短路保护、过电流保护装置，以保证操作人员的安全和设备安全；

2）建筑内设计足够的人行通道和运输通道，设置疏散标志，以保证通行安全。在主要通道和出入口均设置应急照明；

3）办公环境配有空调、空气净化等装置，为工作人员提供舒适的工作环境；

4）对消防、电磁干扰满足工作人员的卫生环境要求；

5）场地设有值班室、货物间、男女洗手间等辅助用房。

## 节能目标及措施

项目建场地建设遵循《公共建筑节能设计标准》、《建筑节能工程施工质量验收规范》等国家规定，场地建设后，系统运行过程中主要是使用计算机设备、网络设备和检测设备，运行能耗较小。在项目实施中，仍将严格遵守国家有关规定，控制能耗。根据有关国家和部门标准规范，采取的主要节能措施有：

1）引进国内先进的关键计算机设备、网络设备和检测设备，要求能耗低、可靠性高；

2）国内生产与办公设备选用优质节能产品；

3）设计中选用的各类配套设备，均选用优质节能系列产品；

4）各种管道应采取保温、隔热等措施；

5）建筑墙面、吊顶作保温层或双层隔离，减少能量损耗。

# 项目实施进度

本次信息化建设项目建设的实施分为以下三个阶段：

第一阶段：项目建设的准备阶段

项目建设的准备阶段，主要是一系列前期准备工作的完成。包括全省、市、区同类项目考察、资料的收集和调研、项目建议书和可研报告的拟定、各项信息系统需求的确定、专家评审、项目建设经费的来源以及项目建设期限的确立等。

第二阶段：项目建设的确立

本阶段的工作内容主要包括项目建设方案设计、项目招标、承建单位等。

第三阶段：项目的实施

本阶段为项目建设的实施阶段，工作内容包括了项目建设合同，信息系统分批建设、验收申请及竣工交付使用等。

第四阶段：项目的验收

本阶段为项目建设的验收阶段，要点涉及是否按规定程序和要求组织验收，检查有关手续是否齐全，以及是否按要求开展各子项专业验收。需审查合同履行是否全面、真实，有无违约行为等。

# 项目风险分析

## 协调风险及控制

由于医院信息化建设项目涉及到门诊科、信息科、医务科、护理科等科室之间的业务协同，且它们分布在不同的业务部门，因此处理各自的工作时出现不统一的工作节奏，因此要建设统一模式，需要协调各个相关部门，统一认识。

医院信息化建设项目是为重庆市市民提供健康、医疗服务的，要求动员和依靠医管局及兄弟单位方方面面的力量来共同完成。因此领导必须重视，规章制度要健全。由于工作牵涉的单位多、部门杂，实现统一集中运作，需要各联动单位积极响应，希望用户单位牵头召开有关会议，进行组织协调工作，在技术集群、人员集中、集成管理等方面统一思想，形成共识，为实现“通过医疗信息化建设，加强监管能力、提高决策水平和管理效能；优化医疗服务流程、降低运行成本、提高医疗服务质量、减轻市民就诊及医药费用负担；加强公共卫生应急处理能力。”的构想提供有力的思想和组织保障。

## 项目技术风险控制

医院信息化建设项目是一个跨学科、跨专业的综合系统工程，这一系统工程是以计算机网络系统、物联网平台为基础，以通信系统、云计算技术为纽带，以集成数据采集与交换、全数字化医疗临床信息应用和医院综合运营管理服务系统为技术支撑的技术综合体，因此技术发展给项目的建设带来一定的风险，避免系统投入使用，技术已落后的可能。由于不同地区、部门系统的设计理念及技术规范的不同，系统和硬件设计的不同，因此没有经过实际运行的技术，是可能存在技术风险。但我们在整体设计中尽可能使用较为成熟的技术，并部分开展物联网及虚拟化技术的应用，同时利用先进的ITSM技术运维管理系统的支持，是能够把握“稳中快跑、适度超前”的建设思路的，总体在技术风险上是可控、可规避的。

## 社会影响风险及控制

项目的参与单位对项目系统重要性认识不到位、服务意识不强、业务人员技术问题、网络发展不平衡，项目建设阶段的问题，都可能使医院智能化建设项目在社会各阶层造成不好的影响。

可以通过各种途径提高医院信息化建设项目在重庆市的认知率，为本项目工作创造良好的舆论氛围，项目相关单位成员结合本单位的实际情况，加强基本硬件建设，同时通过培训提高内部人员的实际工作能力。联动单位加强内部沟通，防止出现互相推倭，扯皮现象，这样才能提高联动系统在社会的影响力。

# 附表1：项目软件配置清单及预算

系统软件配置：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名 称 | 数量 | 预算单价 | 预算总价 |
| 1 | 网络安全等级保护评测(2024、2025年) | 2套 | 20万元 | 40万元 |

清单如下:

| 序号 | 名称 | 单位 | 数量 | 备注 |
| --- | --- | --- | --- | --- |
| 1 | HIS系统等级保护测评(3级) | 项 | 2 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |
| 2 | 电子病历系统等级保护测评（3级） | 项 | 2 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |
| 3 | PACS系统等级保护测评（2级） | 项 | 2 | 提交相关系统《等级保护测评报告》，通过单位相关部门的验收。 |

本次测评指标和对象选择须符合国标《GB/T 28448-2019网络安全等级保护测评要求》的相关要求。具体测评要求如下：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：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和系统运维管理等五个方面的安全测评。

安全物理环境测评对象为对对支持运行的基础物理设施环境以及相关的硬件设备和介质等，包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等方面的安全状况。

安全通信网络是对通信网络的构成组件进行测评。通信网络的构成组件负责支撑信息系统进行网络互联，为等级保护对象各个部分进行安全通信传输，一般包括网络设备、通信链路以及网络拓扑等。测评内容主要包括网络架构、通信传输和可信验证。

安全区域边界需要对边界防护、访问控制、入侵防范、恶意代码和反垃圾邮件防范和安全审计等方面进行测评。

安全计算环境需要对身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等方面进行测评。

安全管理中心需要对系统管理、审计管理、安全管理和集中管控等方面进行测评。

安全管理制度测评是对系统的安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评。

安全管理机构测评是对整个管理组织架构和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

人员安全管理测评是对人员管理模式提出的安全控制要求，包含对人员录用、人员离岗、人员考核、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

安全建设管理测评是对系统建设过程中的系统定级和备案、安全方案设计、产品采购和使用、自主软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、安全服务商选择等情况进行测评。

系统运维管理测评是对系统运行维护过程中的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等情况进行测评。

（1）随着等级保护测评标准的变化，至复测评开始前，若系统发生变更，应答人需负责专家评审及当地网安部门备案工作。

（2）上级管理部门对采购人进行专项、重大事件、重要节日检查时，应答人需配合检查工作，同时对检查中发现的问题进行处理并做好记录。

（3）在遇到网络安全事件时，应答人需根据要求进行网络安全事件溯源工作，需要在半小时内安排至少中级测评师以及渗透人员进行安全排查工作。

（4）根据采购人需求，在整体网络安全项目改造实施过程中提供对每个实施部分板块的整体标准要求进行规范，在项目实施前期，中期，后期安排技术人员进行安全基线检查，确保整体网络安全项目实施顺利。

(5)应答人根据采购人需求，结合客户单位实际情况，开展信息安全培训工作，强化安全意识，了解安全相关法律法规，提升客户有关信息安全方面的基本常识，确保相关人员树立信息安全观念，提高信息安全风险意识，增强信息安全责任感。

（6）根据密码法的要求，应答人需要提供商用密码应用安全技术相关咨询，帮助采购人了解最新的商用密码应用相关政策及标准规范，并协助采购人发现有重要网络与信息系统的密码应用现状、风险及需求，针对发现的密码应用风险结合采购人实际密码需求提出合理的商用密码应用合规建议，为后续密码建设改造工作提供支撑。

根据国家等级保护相关标准，安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，应答人提供整改建议书，配合采购人根据测评范围进行整改实施。