# 台州市路桥区中医院关于二级等级保护测评的项目介绍

# 一、项目背景和必要性

**（一）建设背景**

为贯彻落实国家信息安全等级保护制度，进一步完善台州市路桥区中医院信息系统安全管理体系和技术防护体系,增强信息安全保护意识,明确信息安全保障重点,落实信息安全责任,切实提高台州市路桥区中医院系统信息安全防护能力,同时加强对台州市路桥区中医院信息系统安全的指导和检查工作，特拟请独立、专业的第三方测评机构对台州市路桥区中医院信息系统进行等级保护测评服务。

**（二）项目建设必要性**

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

# 二、项目依据、原则以及资质要求

**（一）项目依据**

报价方应依据国家等级保护相关标准开展工作，依据标准（包括但不限于）如下国家标准：

1. GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》
2. GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》
3. GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》
4. GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》
5. GB/T 25058-2019 《信息安全技术网络安全等级保护实施指南》

**（二）项目原则**

本次安全保护等级保护测评实施方案设计与具体实施应满足以下原则：

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人的行为，否则采购人有权追究报价方的责任。
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：报价方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。
4. 可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。
5. 整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。
6. 最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能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。

**（三）资质要求**

1、报价方必须具备网络安全等级测评与检测评估机构服务认证证书

# 三、项目具体内容及要求

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 数量 |
| 1 | 基础支撑系统二级等级保护测评 | 1 |
| 2 | 面向患者服务系统二级等级保护测评 | 1 |

## （一）服务内容

### 1、网络安全等级保护测评

通过等级保护测评应全面分析应用系统的安全保护措施与等级保护相应级别之间的差距，进行合规性分析，为系统等级保护加固整改提供客观依据，测评的内容包括但不限于以下内容：

一是安全通用要求（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）。

二是现场测评完成后的整改建议服务。

具体如下：

**（1）安全物理环境**

安全物理环境测评主要关注机房在物理位置选择、物理访问控制、供电等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 |
| --- | --- | --- |
| 1 | 物理位置的选择 | 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。 |
| 2 | 物理访问控制 | 测评信息系统在物理访问控制方面的安全保护能力。 |
| 3 | 防盗窃和防破坏 | 测评信息系统是否采取了必要的安全措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 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。 |
| 9 | 电力供应 | 测评是否具备为信息系统提供一定电力供应的能力。 |
| 10 | 电磁防护 | 测评信息系统是否具备一定的电磁防护能力。 |

**(2)安全通信网络**

安全通信网络测评主要关注网络架构、通信传输、可信验证3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 |
| --- | --- | --- |
| 1 | 网络架构 | 通过访谈网络管理员，检查网络设计/验收文档，检查网络拓扑图、检查交换机等网络互联设备，测试系统网络拓扑结构，访问路径，路由控制策略和网络带宽分配情况等过程，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。 |
| 2 | 通信传输 | 检查是否提供密码技术的设备或组件，核查是否能够保证通信过程的保密性和完整性。 |

**(3).安全区域边界**

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、安全审计和可信验证6个个方面的安全保护能力，具体的测评指标描述如下表所示。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 边界防护 | 访谈网络管理员，查看网络拓扑和实际部署情况，是否通过边界设备的受控接口进行通信，是否部署终端管理系统对非法内外联行为进行检查或限制，是否对无线网络的使用进行限制等 |
| 2 | 访问控制 | 访谈网络管理员，查看网络拓扑和实际部署情况，是否部署了访问控制设备，检查访问控制规则配置情况。 |
| 3 | 入侵防范 | 访谈网络管理员，查看网络拓扑和实际部署情况，是否部署了入侵防范产品，核查产品运行情况和检测库更新情况，核查能够检测的攻击类型、范围等。 |
| 4 | 恶意代码和垃圾邮件防范 | 访谈网络管理员，查看网络拓扑和实际部署情况，是否部署了网络层的防恶意代码产品，核查产品运行情况和恶意代码库更新情况；是否部署了防垃圾邮件产品，核查产品运行情况和规则库更新情况。 |
| 5 | 安全审计 | 访谈网络管理员，查看网络拓扑和实际部署情况，是否部署了综合安全审计系统或类似功能的系统平台，安全审计范围是否覆盖到每个用户，审计记录是否充分完整，是否对审计记录进行保护。 |
| 6 | 可信验证 | 检查是否提供可信验证的设备或组件，检查相关设备或组件是否实现可信验证，并在可信性受到破坏后进行报警。 |

**(4)安全计算环境**

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

|  |  |  |
| --- | --- | --- |
| 序号 | 安全子类 | 测评指标描述 |
| 1 | 身份鉴别 | 检查终端和服务器的操作系统（宿主机和虚拟操作系统）、移动终端管理系统、数据库管理系统、业务应用系统、中间件、网络设备、安全设备、感知节点设备、网关节点设备和控制设备等，核查身份标识与鉴别功能设置和使用配置情况，核查对用户登录各种情况的处理，如登录失败处理、登录连接超时等。 |
| 2 | 访问控制 | 检查终端和服务器的操作系统（宿主机和虚拟操作系统）、移动终端管理系统、数据库管理系统、业务应用系统、中间件、网络设备、安全设备、感知节点设备、网关节点设备和控制设备等，核查访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。 |
| 3 | 安全审计 | 检查终端和服务器的操作系统（宿主机和虚拟操作系统）、移动终端管理系统、数据库管理系统、业务应用系统、中间件、网络设备、安全设备、感知节点设备、网关节点设备和控制设备等，是否启用安全审计功能，安全审计范围是否覆盖到每个用户，审计记录是否充分完整，是否对审计记录和审计进程进行保护。 |
| 4 | 入侵防范 | 检查终端和服务器的操作系统（宿主机和虚拟操作系统）、移动终端管理系统、数据库管理系统、业务应用系统、中间件、网络设备、安全设备、感知节点设备、网关节点设备和控制设备等，是否遵循最小安装原则，是否关闭不必要的服务和端口，是否限制管理方式和管理地址，是否采取入侵防范措施等。 |
| 5 | 恶意代码防范 | 检查终端和服务器的操作系统、移动终端管理系统、控制设备等是否安装了防恶意代码软件或相应功能的软件，是否定期升级恶意代码库。 |
| 6 | 可信验证 | 检查是否提供可信验证的设备或组件，检查相关设备或组件是否实现可信验证，并在可信性受到破坏后进行报警。 |
| 7 | 数据完整性 | 检查业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等，核查重要数据在传输和存储过程中完整性保护情况。 |
| 8 | 数据保密性 | 检查业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等，核查重要数据在传输和存储过程中保密性保护情况。 |
| 9 | 数据备份恢复 | 检查数据备份情况，如备份方式、备份策略、异地备份等；检查重要数据处理系统的冗余情况。 |
| 10 | 剩余信息保护 | 检查操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档，核查鉴别信息和敏感数据所在的存储空间被释放或重新分配前是否得到完全清除。 |

**(5)安全管理中心**

安全管理中心测评将通过访谈和检查的方式评测集中安全管理系统的情况。在内容上，安全管理中心测评实施过程涉及4个方面，具体的测评指标描述如下表所示。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 系统管理 | 检查安全管理中心的身份鉴别和日志记录情况，检查是否对系统管理的操作进行审计，是否只允许系统管理员进行系统管理操作。 |
| 2 | 审计管理 | 检查安全管理中心的身份鉴别和日志记录情况，检查是否对安全审计操作进行审计，是否只允许审计管理员进行安全审计操作。 |
| 3 | 安全管理 | 检查安全管理中心的身份鉴别和日志记录情况，检查是否通过安全管理员对系统中的安全策略进行配置。 |
| 4 | 集中管控 | 检查安全管理中心及部署情况，是否对各类设备运行状况进行集中监测，是否对各类设备的审计数据进行集中收集和分析，是滞对安全策略、恶意代码、补丁升级等事项进行集中管理。 |

**(6)安全管理制度**

安全管理制度测评主要关注安全策略、理制度体系、制定与发布以及评审和修订4个方面，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 |
| --- | --- | --- |
| 1 | 安全策略 | 主要核查：总体方针策略类文件 |
| 2 | 管理制度 | 主要核查：各类安全管理制度及操作手册的制定情况。 |
| 3 | 制定和发布 | 主要核查：管理制度的制定与发布流程。 |
| 4 | 评审和修订 | 主要核查：管理制度的评审和修订流程。 |

**(7)安全管理机构测评**

安全管理机构测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等测评对象。

安全管理机构测评主要关注岗位设置、人员配备、授权和审批等5个方面，具体测评指标描述下表所示。

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 岗位设置 | 主要核查：各类安全管理制度及操作手册的制定情况。 |
| 2 | 人员配备 | 主要核查：管理制度的制定与发布流程。 |
| 3 | 授权和审批 | 主要核查：管理制度的评审和修订流程。 |
| 4 | 沟通与合作 | 主要核查：各类安全管理制度及操作手册的制定情况。 |
| 5 | 审核与检查 | 主要核查：管理制度的制定与发布流程。 |

**(8)安全管理人员测评**

安全管理人员测评实施过程涉及人员录用、人员离岗、人员考核等4方面，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 |
| --- | --- | --- |
| 1 | 人员录用 | 主要核查：人员录用的标准与流程。 |
| 2 | 人员离岗 | 主要核查：人员离岗的流程。 |
| 3 | 安全意识教育和培训 | 主要核查：安全意识教育和培训的计划与安排、安全责任的惩罚措施情况。 |
| 4 | 外部人员访问管理 | 主要核查：外部人员访问重要区域的控制手段。 |

**(9)安全建设管理测评**

安全建设管理测评涉及系统定级、安全方案设计和产品采购和使用等10方面，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 |
| --- | --- | --- |
| 1 | 系统定级 | 通过访谈安全主管，检查系统定级相关文档等过程，测评信息系统是否按照一定要求确定其等级。 |
| 2 | 安全方案设计 | 通过访谈系统建设负责人，检查系统安全建设计划等文档，测评被测评单位对系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 通过访谈安全主管、系统建设负责人，检查相关采购制度等过程，测评被测评单位是否按照一定的要求进行信息系统的产品采购。 |
| 4 | 自行软件开发 | 通过访谈系统建设负责人，检查相关软件开发文档和管理制度文档，测评被测评单位对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。 |
| 5 | 外包软件开发 | 通过访谈系统建设负责人，检查相关文档，测评被测评单位对外包开发的软件是否采取必要的措施保证开发过程和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 通过访谈系统建设负责人，检查相关制度文档和实施文档，测评被测评单位对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。 |
| 7 | 测试验收 | 通过访谈系统建设负责人，检查相关制度文档和测试验收文档，测评被测评单位在信息系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 通过访谈系统运维负责人，检查系统交付清单和系统交付管理制度等过程，测评被测评单位是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 通过访谈系统运维负责人，检查相关报告和记录文件，测评被测评单位是否定期进行等级测评，选择的测评机构是滞符合国家有关规定等。 |
| 10 | 安全服务商选择 | 通过访谈系统运维负责人，测评被测评单位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。 |

**(10)安全运维管理测评**

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等测评对象。

安全运维管理测评主要关注环境管理、资产管理和介质管理等14方面，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 |
| --- | --- | --- |
| 1 | 环境管理 | 通过访谈安全物理环境负责人，检查主机房安全管理制度和办公环境管理文档等过程，测评被测评单位是否采取必要的措施对主机房的出入控制和办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 通过访谈资产管理员，检查资产清单和系统、网络设备等过程，测评被测评单位是否采取必要的措施对信息系统资产进行分类标识管理。 |
| 3 | 介质管理 | 通过访谈资产管理员，检查介质管理记录、介质安全管理制度以及各类介质等过程，测评被测评单位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。 |
| 4 | 设备维护管理 | 通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规程等过程，测评被测评单位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。 |
| 5 | 漏洞和风险管理 | 通过访谈系统运维负责人，检查安全报告或记录，测评被测评单位是否采取必要的措施对漏洞进行识别和修补。 |
| 6 | 网络和系统安全管理 | 通过访谈安全主管、系统管理员、网络管理员，检查各管理员角色分工情况及权限，查看网络和系统安全管理制度，是否覆盖安全策略、帐户管理、权限审批和分配、配置文件的生成及备份、变更审批、日志管理等内容。 |
| 7 | 恶意代码防护管理 | 通过访谈系统运维负责人，检查恶意代码防范管理制度和恶意代码检测、分析记录等过程，测评被测评单位是否采取必要的措施对恶意代码进行集中管理，确保信息系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 通过访谈系统管理员，检查基本配置信息保存情况，检查配置变更流程记录文件。 |
| 9 | 密码管理 | 通过访谈安全员，检查密码管理制度等过程，测评被测评单位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。 |
| 10 | 变更管理 | 通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评被测评单位是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份和恢复管理 | 通过访谈系统管理员、网络管理员，检查系统备份管理文档和记录等过程，测评被测评单位是否采取必要的措施对数据、设备和系统进行备份，并确保必要时能够对信息系统进行有效地恢复。 |
| 12 | 安全事件处置 | 通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和处置管理制度等过程，测评被测评单位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。 |
| 13 | 应急预案管理 | 通过访谈系统运维负责人，检查应急响应预案文档，应急预案培训记录等过程，测评被测评单位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。 |
| 14 | 外包运维管理 | 通过访谈运维负责人，检查是否有外包运维服务情况；检查外包运维服务单位是否符合国家有关规定，检查外包运维服务协议等。 |

## （二）测评方法

测评方法必须符合GB/T 28448-2019 信息系统安全等级保护测评要求，满足国家等级保护备案相关标准规范，在开展等级测评工作时，从管理和技术两个层面，通过多种方法来采集测评证据，以确定被测系统与基本要求之间的符合性。采集测评证据的方式分为“人员访谈”、“文件审核”、“现场观察”、“技术测试”等手段。

人员访谈：测评人员与被测单位信息技术人员进行面谈，测评人员可以了解其职责范围、工作陈述、基本安全意识、对安全管理获知的程度等信息。

文件检查：测评人员对被测单位与信息安全管理活动相关的所有文件进行审查，包括安全方针和目标、程序文件、作业指导文件和记录文件等。

现场观察：测评人员通过到现场参观，观察并获取关于被测系统现场的物理环境、信息系统的安全操作和各类安全管理活动的第一手资料。

技术测试：测评人员通过对测评对象采用各种技术手段，获得被测系统在技术性控制的效力及符合性方面的证据。这些技术性措施包括：自动化的扫描工具、网络拓扑结构分析、本地主机审查、渗透测试等。

## （三）测评报告等要求

1. 报价方应对采购人的信息系统进行等级保护测评，形成相应的测评报告；

2. 报价方在测评后出具符合公安主管部门要求的系统安全保护等级测评报告；

3. 对上述系统不符合信息安全等级保护有关管理规范和技术标准的，报价方出具可行的整改建议方案，并为采购人提供整改咨询服务；

4. 报价方协助采购人完成信息系统安全保护等级测评的相关备案手续。

# 四、其他要求

1. 本次等级保护测评实施过程中所使用到的各种工具软件由报价方推荐，经采购人确认后由报价方提供并在测评中使用。

2. 安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由报价方推荐，经采购人确认后由报价方提供并在测评中使用。

3. 安全测评需要的运行环境（如场地、网络环境等）由采购人提供，报价方实施时应详细描述需要的运行环境的具体要求。

# 五、商务要求

**（一）本次等级保护测评实施要求**

1. 实施方在项目实施过程中应服从采购方的统一领导和协调，采购方有权裁决实施方的责任范围，实施方必须执行，在采购方限定的时间内解决问题。如果实施方不能按时完成测评内容，采购方有权中止项目、索赔或拒付款项；

2. 实施过程中形成的阶段性成果文件须指定相关责任人，明确相关职责；

**（二）项目服务承诺**

1. 报价方应满足采购人提出的标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质。

2. 保密性要求：报价方必须和采购人签订保密协议和非侵害性协议，报价方必须要与参加此次测评项目的所有项目组成员签订保密协议和非侵害性协议，在合同签定时一并提供给采购人。

3. 报价方具体测评工作和等级保护测评报告的编写，必须在采购人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，报价方不得带离该地点。

4. 报价方对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。

5. 等级保护测评的品质保证：报价方应承诺指派工作经验丰富、技术实力雄厚的安全顾问，结合技术领先、结论可靠的测评工具为客户作全面等级保护测评。承诺测评过程按照国家标准进行，并保证对客户的资料严格保密。

**（三）项目验收**

1.本项目输出包括且不仅仅包括以下成果：

《等级保护测评报告》（每系统一份）

《等级保护整改建议书》（每系统一份）