网络信息安全等保测评服务招标采购要求

常德技师学院门户网站、一卡通系统、教务管理系统二级等保护测评项目，项目业主为常德技师学院，现对本项目的等级保护测评服务进行公开招标。欢迎有资质的投标人参与本项目的投标。

项目名称：常德技师学院门户网站、一卡通系统、教务管理系统二级等保护测评

标段划分：1个标段

资金来源：自筹

合同签定后，中标方在六个月之内完成本次招标之等级保护测评服务内容。

### 1、投标人基本资格条件：

投标人需具备《中华人民共和国政府采购法》第二十二条规定的基本资格条件，并提供以下资格证明文件：

（1）法人提交企业法人营业执照副本以及组织机构代码证副本复印件；

（2）依法缴纳税收和社会保险费的证明材料,各提供下列材料:

①缴纳税收证明资料:《税务登记证》复印件，或者近三个月依法缴纳税收的证明（纳税凭证复印件）；

②缴纳社会保险证明资料：《社会保险登记证》复印件，或者近三个月依法缴纳社会保险的证明（缴费凭证复印件）；

（3）法人提交法定代表人身份证明原件或者法定代表人授权委托书原件并附法定代表人身份证明原件，自然人提交身份证复印件；

（4）投标人具有实行了“三证合一”登记制度改革的新证并提交的，视同为持有并提交了工商营业执照、组织机构代码证和税务登记证，符合基本资格条件的相关条款。

 **2、投标人特定资格条件：**

★要求投标人是《全国信息安全等级保护测评机构推荐目录》中的服务单位，并提供网上（www.djbh.net）查询的证明材料。

**3、开标时间及地点**

时间：2019年1月3日星期四上午9:30

地点：常德技师学院综合楼310办公室

联系人：彭翠兰 0736-7722146

**4､评标计分权值：**

|  |  |  |
| --- | --- | --- |
| 序号 | 项 目 | 权值的取值 |
| 1 | 商务 | 40 |
| 2 | 技术 | 40 |
| 3 | 价格 | 20 |
| ∑(1+2+3)=100 | 100 |
| 评标因素和标准 | (提示：因评标因素“技术”项涉及政府采购政策优惠，为便于计算，应与其他评标因素分列) |
| 权值 | 评审因素 | 权值 |
| 商务 | 0.40 |
| 技术 | 0.40 |
| 价格 | 0.20 |
| **评审因素** | **分值** | **评分标准** |
| **投标报价(F1)** | **投标总价** | **100** | 满足招标文件基本资格要求、特定资格要求、实质性条款要求且投标报价中最低的投标报价为评标基准价其价格分为满分；其他投标人的价格分统一按照以下公式计算：投标报价得分=（评标基准价/投标报价）×100注：此栏中的计分因素“投标报价”为依据政策调整后的投标报价。 |
| **技术性能(F2)** | 满足招标文件技术要求程度 | 20 | 完全满足招标文件技术指标的计 20分，一般技术条款（ 非“★”条款）每负偏离一项扣2分 ；如应答时缺项，则视同负偏离处理。 |
| 项目实施方案 | 20 | 以招标文件的技术要求为基准，应详细描述项目实施中涉及到的各个方面，包括人员安排、安全域划分拓扑图、项目分工界面、现场实施工作表单，符合项目要求的接入点示意图等。分档计分：优计20分,良计10分,一般计5分。（以上三档，每档取一名，其他不计分）。 |
| 技术实力 |  60 | ■投标人具有中国合格评定国家认可委员会CNAS检验机构认可证书的计10分（提供证书复印件并加盖公章）■投标人具有高级信息安全等级测评师或者CISP证书的,计5分（提供证书复印件和相关人员在投标单位近三个月的社保证明。）■投标人参与本项目的测评师于2017年获得国家信息安全等级保护工作协调小组办公室颁发荣誉证书的计10分（提供测评师证书和荣誉证书的复印件及相关人员在投标单位近三个月的社保证明）■投标人具有公安部等级保护评估中心核发的重要信息系统保护人员CIIP-A的资质的工程师,每个人员计5分（提供证书复印件并加盖公章和相关人员在投标单位近三个月的社保证明）最多计15分。■投标人具有《网络安全等级保护测评机构》证书计10分（提供复印件）■投标人具有中国互联网协会网络与信息安全工作委员会国家互联网应急中心 (CNCERT)颁发的“国家信息安全漏洞共享平台原创漏洞证明”证书的计10分。（提供证书复印件和相关漏洞发掘人员在投标单位近三个月的社保证明）。 |
| **商务部分(F3)** | 资质能力 | 10 | 投标人获得公安部信息安全等级保护推荐时间六年以上的计10分，三年以上的计4分，一年及以内的计2分（提供[www.djbh.net](http://www.djbh.net)查询截图文件，未提供证明文件的，不予计分） |
| 20 | 投标人具有省级及以上保密行政部门颁发的涉密信息系统集成（运行维护）资质证书的，计20分（提供证书复印件并加盖公章） |
| 15 | 投标人具有省级及以上质量技术监督局核发的计量认证证书的计15分（提供证书复印件并加盖公章） |
| 同类业绩 | 10 | 投标人提供自2015年以来测评服务案例，每个计2分，最多10分。（须提供加盖投标人公章的项目合同；没提供合同复印件的，不予计分） |
| 本地服务能力 | 20 | 投标人在湖南省本地设有服务机构的计20分；承诺中标后在湖南省本地成立服务机构的计5分（须提供湖南省的工商注册证明文件复印件或承诺函原件） |
| 企业信誉 | 15 | 投标人2016年和2017年都获得国家信息安全等级保护工作协调小组办公室颁发先进单位的得15分（投标时须提供证书复印件并加盖投标人公章） |
| 10 | 投标具有“信息安全管理体系认证证书”的计10分（提供相关证明复印件） |
| 评委评分=F1×A1+F2×A2+……+Fn×An |
| F1、F2……Fn分别为各项评分因素的汇总得分 |
| A1、A2……An分别为各项评分因素所占的权值（A1+A2+……An=1） |

常德技师学院等级保护测评项目

**技术要求**

# 一．项目背景

根据国家《中华人民共和国网络安全法》、《信息安全等级保护管理办法》（以下简称管理办法）和公安部等部委的要求，对我单位教务系统、一卡通系统、官网定级为二级进行等级保护测评和渗透测试工作，以全面了解信息安全现状，同时为之后的信息安全整改建设工作提供依据。

# 二．采购内容及技术要求

## 1. 总则

1.1 本技术需求书条款所提出的各项要求，是本次信息系统安全等级保护测评依据投标人应根据本文件中的相关说明和要求，提供方案。

1.2 投标人在测评方案书中，对能提供的信息系统安全等级保护测评进行说明，可根据具体情况在项目方案中提出建议，并附详细资料和说明。

1.3 投标人应对提供信息系统安全等级保护测评时所使用的设备及软件保证拥有设备软硬件的知识产权和所有权，并对所涉及的专利、知识产权等法律条款承担义务，采购人对以上问题不承担任何法律责任。

1.4 若投标人的设备和系统包含自己的专用标准，应在建议书中具体说明，并附上相应的详细技术资料。

## 2.主要应用系统

 常德技师学院教务系统、一卡通系统、学院门户网站定级为二级。

## 3．依据政策及标准

投标人应依据国家相关政策标准开展工作，依据标准包括但不限于如下国家政策标准：

《中华人民共和国网络安全法》

《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）

《关于进一步推进全省信息安全等级保护工作的函》湘公函【2011】21号

《关于对全省重要信息系统开展信息安全等级保护专项检查工作的函》湘公函【2011】74号

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 17859-1999 信息安全技术 计算机信息系统安全保护等级划分准则

GB/T 20984—2007信息安全技术 信息安全风险评估规范

## 4. 项目工作内容

根据相关文件及标准要求，对常德技师学院信息系统安全等级保护测评和安全培训。

信息系统安全等级保护测评包含以下系统：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 级别 | 备注 |
| 1 | 教务系统 | 二级 |  |
| 2 | 一卡通 | 二级 |  |
| 3 | 学院门户网站 | 二级 |  |

## 工作内容：

### 5.1信息系统安全等级保护测评

依据《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）等级保护测评的要求，找出系统与国家标准要求之间的差距，对存在的风险进行评估，并出具《信息安全等级测评报告》。

a) 测评范围

 被测系统所涉及的基础网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。

b) 测评内容

具体分为网络安全、主机系统安全、应用安全、数据安全及备份恢复、安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等几个方面，同时配合漏洞扫描工具对检查结果进行验证、分析。

物理安全

物理安全测评将通过访谈和检查的方式评测信息系统的物理安全保障情况。主要涉及对象为机房。

在内容上，物理安全层面测评实施过程涉及10个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 物理位置的选择 | 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 4 | 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。 |
| 5 | 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。 |
| 6 | 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。 |
| 7 | 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。 |
| 8 | 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。 |
| 9 | 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。 |
| 10 | 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。 |

网络安全

网络安全测评将通过访谈、检查和测试的方式评测信息系统的网络安全保障情况。主要涉及对象机房的网络设备、网络安全设备以及网络拓扑结构等三大类对象。在内容上，网络安全层面测评过程涉及7个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 结构安全 | 通过访谈网络管理员，检查网络拓扑情况、核查核心交换机、路由器，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 | 访问控制 | 通过访谈安全员，检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等，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。 |
| 3 | 安全审计 | 通过访谈审计员，检查核心交换机、路由器等网络互联设备的安全审计情况等，测评分析信息系统审计配置和审计记录保护情况。 |
| 4 | 边界完整性检查 | 通过访谈安全员，检查边界完整性检查设备,接入边界完整性检查设备进行测试等过程，测评分析信息系统私自联到外部网络的行为。 |
| 5 | 入侵防范 | 通过访谈安全员，测评分析信息系统对攻击行为的识别和处理情况。 |
| 6 | 恶意代码防范 | 通过访谈安全员，检查网络防恶意代码产品等过程，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的防护情况。 |
| 7 | 网络设备防护 | 通过访谈网络管理员，检查交换机、路由器等网络互联设备以及防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、登录失败处理、限制非法登录和登录连接超时等，考察网络设备自身的安全防范情况。 |

主机系统安全

主机系统安全测评将通过访谈、检查和测试的方式评测信息系统的主机和服务器（操作系统、数据库管理系统）安全保障情况。在内容上，主机系统安全层面测评实施过程涉及7个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 4 | 剩余信息保护 | 检查服务器鉴别信息的存储空间，被释放或再分配给其他用户前得到完全清除。 |
| 5 | 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。 |
| 6 | 恶意代码防范 | 检查服务器的恶意代码防范情况。 |
| 7 | 资源控制 | 检查服务器对单个用户的登录方式、网络地址范围、会话数量等的限制情况。 |

应用系统安全

应用安全测评将通过访谈、检查和测试的方式评测信息系统的应用安全保障情况。在内容上，应用安全层面测评实施过程涉及9个工作单元，具体如下表：

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 身份鉴别 | 检查应用系统的身份标识与鉴别功能设置和使用配置情况；检查应用系统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 | 检查应用系统的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 | 检查应用系统的安全审计配置情况，如覆盖范围、记录的项目和内容等；检查应用系统安全审计进程和记录的保护情况。 |
| 4 | 剩余信息保护 | 检查应用系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。 |
| 5 | 通信完整性 | 检查应用系统客户端和服务器端之间的通信完整性保护情况。 |
| 6 | 通信保密性 | 检查应用系统客户端和服务器端之间的通信保密性保护情况。 |
| 7 | 抗抵赖 | 检查应用系统对原发方和接收方的抗抵赖实现情况。 |
| 8 | 软件容错 | 检查应用系统的软件容错能力，如输入输出格式检查、自我状态监控、自我保护、回退等能力。 |
| 9 | 资源控制 | 检查应用系统的资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。 |

数据安全及备份恢复

数据安全及备份恢复测评将通过访谈和检查的方式评测信息系统的数据安全保障情况。本次测评重点检查系统的数据在采集、传输、处理和存储过程中的安全。

在内容上，数据安全层面测评实施过程涉及3个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 数据完整性 | 检查操作系统、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。 |
| 2 | 数据保密性 | 检查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。 |
| 3 | 安全备份和恢复 | 检查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。 |

安全管理制度

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

在内容上，安全管理制度测评实施过程涉及3个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 管理制度 | 通过访谈安全主管，检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 2 | 制定与发布 | 通过访谈安全主管，检查有关制度制定要求文档等过程，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。 |
| 3 | 评审和修订 | 通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |

安全管理机构

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

在内容上，安全管理机构测评实施过程涉及5个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 岗位设置 | 通过访谈安全主管，检查部门/岗位职责文件，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。 |
| 2 | 人员配备 | 通过访谈安全主管，检查人员名单等文档，测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 通过访谈安全主管，检查相关文档，测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通和合作 | 通过访谈安全主管，检查相关文档，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。 |
| 5 | 审核和检查 | 通过访谈安全主管，检查记录文档等过程，测评信息系统安全工作的审核和检查情况。 |

人员安全管理

人员安全管理测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

在内容上，人员安全管理测评实施过程涉及5个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 人员录用 | 通过访谈人事负责人，检查人员录用文档等过程，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。 |
| 2 | 人员离岗 | 通过访谈人事负责人，检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续办理。 |
| 3 | 人员考核 | 通过访谈安全主管，检查有关考核记录等过程，测评是否对人员进行日常的业务考核和工作审查。 |
| 4 | 安全意识教育和培训 | 通过访谈安全主管，检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。 |
| 5 | 外部人员访问管理 | 通过访谈安全主管，检查有关文档等过程，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。 |

系统建设管理

系统建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

在内容上，系统建设管理测评实施过程涉及11个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 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，测评是否按照一定要求确定系统的安全等级。 |
| 2 | 安全方案设计 | 通过访谈系统建设负责人，检查系统安全建设方案等文档，测评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、系统建设负责人和安全产品等过程，测评是否按照一定的要求进行系统的产品采购。 |
| 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等，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。 |
| 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。 |
| 6 | 工程实施 | 通过访谈系统建设负责人，检查相关文档，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。 |
| 7 | 测试验收 | 通过访谈系统建设负责人，检查测试验收等相关文档，测评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，检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 系统备案 | 通过访谈系统运维负责人，检查系统定级和备案材料和相关工作记录，测评是否已经上报主管部门和公安机关完成备案工作。 |
| 10 | 等级测评 | 通过访谈系统运维负责人，检查测评报告和整改记录，测评是否依据国家要求完成等级测评和整改工作。 |
| 11 | 安全服务商选择 | 通过访谈系统运维负责人，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。 |

系统运维管理

系统运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

在内容上，系统运维管理测评实施过程涉及13个工作单元，具体如下表：

| **序号** | **工作单元名称** | **工作单元描述** |
| --- | --- | --- |
| 1 | 环境管理 | 通过访谈物理安全负责人，检查机房安全管理制度，机房和办公环境等过程，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。 |
| 2 | 资产管理 | 通过访谈资产管理员，检查资产清单，检查系统、网络设备等过程，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。 |
| 3 | 介质管理 | 通过访谈资产管理员，检查介质管理记录和各类介质等过程，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。 |
| 4 | 设备管理 | 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 | 监控管理和安全管理中心 | 通过访谈系统运维负责人，测评是否采取必要的措施对重要主机的运行和访问权限进行监控管理。 |
| 6 | 网络安全管理 | 通过访谈安全主管、系统管理员，检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测评是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
| 7 | 系统安全管理 | 通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。 |
| 8 | 恶意代码防范管理 | 通过访谈系统运维负责人，检查恶意代码防范管理文档和恶意代码检测记录等过程，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。 |
| 9 | 密码管理 | 通过访谈安全员，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。 |
| 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 | 备份与恢复管理 | 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。 |
| 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等过程，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。 |

工具测试

 根据工具测试过程管理表单，使用漏洞扫描工具对信息系统的设备进行扫描，扫描结束后，根据目标设备的具体情况，判断漏洞验证的风险程度。

c) 实施流程

1.测评准备活动：测评准备活动中，评估中心主要完成启动测评项目，组建测评项目组；通过收集和分析被测系统的相关资料信息，掌握被测系统的大体情况；并准备测评工具和表单等测评所需的相关资料。

2.方案编制活动：方案编制活动中，评估中心主要完成确定测评对象和测评指标，选择测试工具接入点，从而进一步确定测评实施内容，并从已有的测评指导书中选择本次需要用到的测评指导书，最后根据上述情况编制测评方案。

3.现场测评活动：现场测评活动中，评估中心在与测评委托单位就测评方案达成一致意见，并进一步确定测评配合人员，完成测评指导书各项测评内容，获取足够的测评证据。

4.分析与报告编制活动：分析与报告编制活动中，测评人员通过分析现场测评获得的测评证据和资料，判定单项测评结果及单元测评结果，进行整体测评和风险分析，形成等级测评结论，并编制测评报告。



6.技术服务要求

6.1本次等级测评应满足的原则

（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招标人的行为，否则招标人有权追究投标人的责任。

（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：投标人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，保证招标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的正常运行、业务的正常开展产生任何影响。

投标人应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

6.2本次等级测评的整体要求

（1） 投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2） 投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

（3） 本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由投标人推荐，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。

（4） 信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

### 5.2安全培训

针对终端用户、技术人员、安全管理人员提供信息安全意识、安全技术、黑客攻击手段与防御、安全运维培训及定制培训服务。提高用户的信息安全意识，提高安全技术人员的安全运维技能和安全管理水平。

通过这一整套体系的服务，不但能解决我院当前的问题，也能在未来信息安全建设、维护工作中大大降低信息安全事件发生概率，并且在不可抗事件发生后能及时做出应对，避免事态升级，影响扩大。

## 服务交付物

表. 项目交付物

|  |  |
| --- | --- |
| **服务** | **交付物** |
| 信息系统等级保护测评服务 | 《常德技师学院差距分析报告》；《常德技师学院教务系统等级测评报告》；《常德技师学院一卡通系统等级测评报告》；《常德技师学院官网系统等级测评报告》；系统通过本次测评后协助我院填写《定级报告》和《备案表》，并协助我院获取备案证明。 |
| 信息安全培训服务 | 《常德技师学院培训方案》《培训课件》 |