**赣州市中心血站网络安全等级保护**

**测评服务采购需求**

# 供应商资格要求

1、供应商需具有公安部第三研究所颁发的《网络安全服务认证证书等级保护测评服务认证》；

2、供应商应未被列入“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中。

3、本项目不接受联合体参与投标。

# 二、服务背景及目标

为加强日常网络安全运行维护，落实等级保护制度，同时为满足网络安全监管和新等级保护等工作要求，赣州市中心血站组织开展网络安全等级保护测评工作。参与测评的机构应根据赣州市中心血站需求，按照等保测试要求提供切实有效的整改方案、咨询方案，并对整改后的信息系统进行复测，出具符合要求的《等级保护测评报告》。

# 三、标准和规范

《GBT 20272—2006 信息安全技术 操作系统安全技术要求》

《GBT 20273—2006 信息安全技术 数据库管理系统安全技术要求》

《GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南》

《GBT 22239—2019 信息安全技术 网络安全等级保护基本要求》

《GB/T 25070—2019 信息安全技术 网络安全等级保护设计技术要求》

《GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求》

《信息安全等级保护管理办法》（公通字[2007]43号文件）

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

# 四、实施原则

本项目实施方案设计与具体实施必须满足以下原则：

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招标方的行为。

2标准性原则：测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。

3规范性原则：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：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

5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。

6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。

# 五、服务内容及范围

**1.服务内容**

|  |  |  |
| --- | --- | --- |
| **系统名称** | **系统等级** | **测评次数及周期** |
| 血液管理信息系统 | 三级 | 两次（每年1次） |

**2.定级备案服务**

协助赣州市中心血站对需要进行测评的信息系统编写定级、备案材料，协助采购方到公安监管等部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。

**3.等级保护测评服务**

依据《GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求》《[GB/T 28448-2019 信息安全技术信息系统安全等级保护测评要求](http://www.baidu.com/link?url=mXgRblKIGLNk3k6UhKsFa_-6T1vQsBrKifbgzd1LtI4JXx5BRGffiSBkI_QepRsUF5AeucrF2fSo1nJ3VT3DFMXXpjVad_vwO2qPQqzDVaq" \t "_blank)》等标准的要求，对赣州市中心血站需要进行测评的信息系统进行等级测评，出具符合国家网络安全等级保护格式要求的等级测评报告。测评内容应包括但不限于以下内容：

（1）安全物理环境

测评内容主要包括：物理位置的选择、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、电磁防护等。

（2）安全通信网络

测评内容主要包括：网络架构、通信传输、可信验证等。

（3）安全区域边界

测评内容主要包括：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、可信验证等。

（4）安全计算环境

测评内容主要包括：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、个人信息保护等。

（5）安全管理中心

测评内容主要包括：系统管理、审计管理、安全管理、集中管理等。

（6）安全管理制度

测评内容主要包括：安全策略、管理制度、制定和发布、评审和修订等。

（7）安全管理机构

测评内容主要包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等。

（8）安全管理人员

测评内容主要包括：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等。

（9）安全建设管理

测评内容主要包括：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、服务供应商选择等。

（10）安全运维管理

测评内容主要包括：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、外包运维管理等。

**4.实施要求**

（1）供应商应详细描述本次信息系统安全等级保护测评的技术方案，包括整体实施方案、等级保护测评方案、测试设备清单、时间安排、阶段性文档提交等；

（2）供应商在项目现场实施周期内，必须为本项目成立等级保护测评项目部，安排包括项目经理和各测评实施小组进场调研、测评工作；

（3）在采购方进行整改过程中提供必要的技术支持；

（4）能按照采购方规定的工作内容及进度安排协助完成等级保护工作。

（5）为了保障测评服务质量与服务效果，服务过程中供应商需通过检测工具对网络中的系统、主机、流量等进行扫描和检测。

**5.协助安全建设整改**

供应商按照测评标准的相关指标，对被测评信息系统及相关设施进行预测评，根据测评结论提出安全整改意见和安全策略调整建议，并梳理被测评单位确实的安全管理制度，完善后形成安全管理制度汇编。

**6.项目验收**

供应商和采购人依据项目内容和进度共同实施验收工作，验收结果和验收报告经双方确认后生效。

供应商必须提交《信息系统等级保护测评报告》，协助采购人办理信息系统安全保护等级备案手续，并取得备案证书。

采购人确认取得相应等保证书后全额支付服务款。

# 六、其他要求

1、人员要求：

（1）项目经理:供应商必须任命一名具备高级测评师证书的技术人员为项目经理，全面负责项目实施工作。

（2）派驻现场测评师不少于4人，其中须具有至少一名高级测评师或注册信息系统安全专业人员（CISP或CISSP）。

2、质量要求：质量管理是贯穿整个项目的一项任务。通过实施有效的质量管理措施，保证本项目能够按工作范围要求、按时间、按质量完成，供应商应提供质量管理方案。

3、保密要求：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。

4、售后服务：提供7\*24小时售后服务，现场服务需2小时内到场。