采购技术要求

1. 概述

1.1 背景

网络安全等级保护是国家关于网络安全的基本政策，《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），（以下简称 27 号文）等文件明确要求我国信息安全保障工作实行等级保护制度，提出“抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

为了进一步提高武威市凉州医院重要信息系统的安全保障能力，根据国家及各部委、各行业主管单位相关要求对其重要信息系统进行信息安全等级保护测评及相关安全服务。

现拟邀请具有相应资质的信息安全等级保护测评机构依据《信息系统安全等级保护测评要求》等管理规范和技术标准，检测评估武威市凉州医院重要信息系统安全等级保护状况是否达到相应等级基本要求，并出具相应的《信息安全等级保护测评报告》。

1.2 目标

本项目中，技术服务方需要给武威市凉州医院重要信息系统提供全面的安全服务，服务内容包括：等级保护测评服务、应急保障服务等。通过对重要业务系统的等级保护测评，进一步提升武威市凉州医院重要信息系统的安全防护能力。

技术服务方在本次武威市凉州医院重要信息系统安全服务项目中需要达到以下目标：

- 查找薄弱环节、落实防护措施、消除安全隐患，提高应用系统的风险抵御水平。
- 通过等级保护测评，检查客户业务系统是否符合等级保护相关要求，并给出结论。
- 通过等级保护测评发现网络环境中的问题，确定网络安全配置策略。
- 通过等级保护测评发现系统中配置是否符合等级保护要求，并确定主机安全策略。
- 通过等级保护测评发现相关应用系统中数据库系统中的脆弱性问题。
- 通过等级保护测评发现相关应用系统中存在的风险，提前规避业务运营风险。
- 梳理业务系统的安全隐患。
- 通过等级保护测评服务，发现应用系统中的存在风险，提出合理可行整改建议，并提供整改建设建议方案，协助用户提升应用系统的方案防护能力。

- 通过应急保障服务，在特殊敏感时期和重大活动期间，对客户方本次项目中的信息系统进行安全监控和现场应急响应，保障关键业务的正常运行。

1.3 范围

本次服务方案主要涉及以下应用系统：

序号	系统名称	定级情况
1	武威市凉州医院所属重要信息系统	三级

1.4 内容

本项目对武威市凉州医院相关系统进行网络安全服务工作，明确系统的等级保护符合程度，提高武威市凉州医院重要信息系统的整体安全水平和防护能力。

具体工作内容如下：

- 对信息系统中的核心业务系统进行等级保护测评；
- 根据测评结果输出等级保护测评报告；
- 根据测评结果，进行系统科学的分析，提出整改建设，输出整改建议；
- 针对采购方信息系统现状，提供应急保障服务等。

2. 安全服务

2.1 等保测评服务

2.1.1 测评标准

2.1.1.1 国家安全政策

- 《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）
- 《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）
- 《信息安全等级保护备案实施细则（公信安[2007]1360 号）》
- 《关于开展信息安全等级保护安全建设整改工作的指导意见(公信安[2009]1429 号)》

2.1.1.2 国家安全技术标准

- 《信息保障技术框架》（IATF）
- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）
- 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）
- 《信息安全技术 信息系统安全等级保护定级指南》（GB/T22240－2020）
- 《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）
- 《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）
- 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）
- 《信息安全技术 信息系统安全等级保护测评要求》（GB/T28448-2018）
- 《信息安全技术 信息系统安全等级保护测评过程指南》（GB/T28449-2018）
- 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）
- 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）
- 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）
- 《信息安全技术 服务器技术要求》（GA/T671-2006）
- 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T672-2006）

2.1.2 测评原则

本次等级保护测评项目中，技术服务方需遵照以下原则开展安全服务的实施工作：

2.1.2.1 符合性原则

符合国家 27 号文件指出的积极防御、综合防范的方针和等级保护的原则。

技术服务方在项目过程中将严格贯彻《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(试行)》(公通字[2006]7 号）等文件传达的各项精神。

技术服务方将综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全测评工作。坚持“积极防御、综合防范”的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。

2.1.2.2 标准性原则

服务方案的设计与实施将依据国内和行业的相关标准进行。

项目中将参考并遵循国内相关信息安全标准和行业规范 ISO15408（GB/T18336）、ISO27002（GB/T17916）、ISO27001、ISO13335、SSE-CMM、《GB17859-1999 计算机信息系统安全保护等级划分准则》、《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》等，有效结合国际国内信息安全的最佳实践，充分吸收先进同类行业的成功经验，最大限度适应组织业务拓展的要求。

2.1.2.3 规范性原则

服务实施厂商在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；

技术服务方在提供本次安全服务中，除了依据相关的国内和国际标准之外，还根据本项目的需要，遵循自身的一些规范和要求。

2.1.2.4 可控性原则

安全服务实施的相关工具、方法和过程要在双方认可的范围之内，安全服务实施的进度要按照进度表的安排，保证武威市凉州医院对于工程实施的可控性。

技术服务方将遵循行业相关规范及自有项目管理规范，从以下几个方面达到对整个服务项目的可控性，主要包括：

- 人员可控性：技术服务方将指定项目的专职人员实施现场各方面工作，并在服务的工作说明中明确定义其职责，并得到双方的同意、确认和签署。

- 工具可控性：技术服务方项目组所使用的所有技术工具都事先通告武威市凉州医院重要信息系统相关负责人，并且在必要时可以按照信息系统负责人的要求，介绍主要工具的使用方法，并进行一些测试实验。
- 项目过程可控性：本评估项目的管理将依据 PMI 项目管理方法学等项目管理方法。特别是在项目管理中突出“沟通管理”，达到项目过程的可控性。

2.1.2.5 整体性原则

在信息收集阶段、测评指导书开发阶段和现场测评阶段的实施范围和内容应当整体全面，包括安全涉及的各个层面（应用、系统、网络、管理制度、人员等），避免由于遗漏造成未来的安全隐患。

技术服务方将按照武威市凉州医院提供的项目范围进行全面的服务实施，从范围、深度上满足用户的要求。项目实施包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患，保证测评工作的全面性，以及安全管理策略、制度和流程建设的完整性。

2.1.2.6 最小影响原则

安全服务项目实施过程中应尽可能小的影响系统和网络的正常运行，不能对各系统的正常运行产生影响(包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在向用户详细描述)。

技术服务方会从项目管理和技术应用的层面，将安全服务对系统和网络的正常运行所可能的影响降到最低程度，不对当前运行的网络和业务系统产生显著影响（包括系统性能明显下降、网络拥塞、服务中断），同时在现场测评前做好备份和应急措施。

2.1.2.7 保密原则

对安全服务项目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武威市凉州医院的行为，否则武威市凉州医院有权追究安全服务商责任。武威市凉州医院有权要求安全服务商在工程结束之后销毁所有和本工程有关的数据和文档。

2.1.3 测评内容

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：

a) 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、安全计算环境和安全管理中心等五个方面的安全测评；

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

1.1 安全物理环境

根据武威市凉州医院重要信息系统机房和现场安全测评记录，针对机房和现场在“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”以及“电磁防护”等物理安全方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

1.2 安全通信网络

根据武威市凉州医院重要信息系统安全通信网络测评记录，针对网络方面在“网络架构”、“通信传输”、“可信验证”等安全通信网络方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

1.3 安全区域边界

安全区域边界现场测评包括对武威市凉州医院重要信息系统网络边界的测评，测评内容包括“边界防护”、“访问控制”、“入侵防范”、“恶意代码防范”、“安全审计”以及“可信验证”。

1.4 安全计算环境

安全计算环境现场测评包括对武威市凉州医院重要信息系统中网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其它设备的测评，测评内容包括“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”以及“个人信息保护”方面。

1.5 安全管理中心

武威市凉州医院重要信息系统安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中管控”四个方面的测评。

1.6 安全管理制度

根据现场安全测评记录，针对武威市凉州医院重要信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

1.7 安全管理机构

根据现场安全测评记录，针对武威市凉州医院重要信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

1.8 安全管理人员

根据现场安全测评记录，针对武威市凉州医院重要信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

1.9 安全建设管理

根据现场安全测评记录，针对武威市凉州医院重要信息系统在安全建设管理方面的“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”、“系统交付”、“等级测评”以及“服务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

1.10 安全运维管理

根据现场安全测评记录，针对武威市凉州医院重要信息系统在安全运维管理方面的“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”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

2.1.4 测评交付物

项目实施完成后，测评技术服务方须提供以下交付物：

信息系统定级备案证明：

《武威市凉州医院重要信息系统定级备案证明》（每个系统一份）

信息系统等级保护测评报告：

《武威市凉州医院重要信息系统等级保护测评报告》（每个系统一份）

CISP 认证培训：

CISP 证书考试的相关培训和辅导资料、证书，CISP 证书/1 人

附属材料：

《武威市凉州医院重要信息系统等级保护整改建议》

《武威市凉州医院重要信息系统等保测评项目过程文档汇编》

2.2 安全服务内容

2.2.1 概述

本次项目中，技术服务方除为武威市凉州医院相关系统提供等级保护测评工作外，还需通过应急保障服务等服务内容进一步提升武威市凉州医院重要信息系统的安全防护能力。

2.2.2 应急保障服务

在特殊敏感时期和重大活动期间，技术服务方需对武威市凉州医院的重要信息系统进行安全监控和现场应急响应，保障重要时期关键业务的正常运行，同时出具相应的安全日报。

2.3 项目实施要求

2.3.1 保密要求

技术服务方对项目实施过程中所获得数据及文档等保密信息，承担以下保密义务：

1.中标方应按要求与【委托方】会签署保密协议。

2.主动采取加密措施对上述所列及之保密信息进行保护，防止不承担同等保密义务的任何第三者知悉及使用。

3.不得刺探或者以其他不正当手段（包括利用计算机进行检索、浏览、复制等）获取与本职工作或本身业务无关的甲方关于该项目的商业秘密。

4.不得向不承担同等保密义务的任何第三人披露甲方关于该项目的商业秘密。

5.不得允许（包括出借、赠与、出租、转让等行为）或协助不承担同等保密义务的任何第三人使用甲方关于该项目的商业秘密。

6.不论何种原因终止参与委托方关于该项目的工作后，都不得利用该项目之商业秘密为其他与委托方有竞争关系的企业（包括自办企业）服务。

7.该项目的商业秘密所有权始终全部归属委托方，中标方不得利用自身对项目不同程度的了解申请对于该项目的商业秘密所有权，在本协议签订前中标方已依法具有某些所有权者除外。

8.如发现委托方关于该项目的商业秘密被泄露或者自己过失泄露秘密，应当采取有效措施防止泄密进一步扩大，并及时向委托方相关部门报告。

2.3.2 服务实施要求

1.在项目实施过程中，技术服务方应做好计划与安排，不影响武威市凉州医院正常业务办公的开展。技术服务方要给予承诺，并承担由此引起的损失。

2.在技术服务过程中，每周五下午技术服务方需提交工作周报，内容应包括本周工作内容和下周工作安排等内容。

3.等保测评工作应严格按照双方确认的工作方案开展，如遇任何变动，须在工作周报中及时提出，经采购人批准后方可变更。

4.测评过程中技术服务方测评人员须记录在途经路径上涉及的可被利用存在漏洞的相关主机等设备的信息，以便于被测单位对相关漏洞进行全面修补。

5.测评工作全部结束后技术服务方测评人员须卸载安置在目标机器或途径机器上的各类工具、脚本、文件等，还原各机器和系统的原始状态。

6.测评结果中应包括测评过程中发现的所有漏洞，不能遗漏。

7.在测评过程中若发现重大安全问题（如已被控制或存在严重安全隐患等），测评机构应在 24 小时之内以书面形式通知甲方，以便甲方第一时间做出处理。

8.测评过程中，技术服务方测评人员在进入被测单位办公网络后若发现测评范围之外的未知信息系统，须列出系统名称、服务器 IP 地址、操作系统类型、数据库系统类型等信息，并与采购人协商是否继续进行测评。

9.测评过程中不得获取测评范围以外的数据，获取的数据不得用于本次测评以外的其他用途。

10.测评过程中应控制风险，防止测试对网络及系统运行造成影响，因测试造成系统运行问题应及时报告。

11.测评过程中，测评机构应该针对被测系统发现的漏洞提交可行性的解决方案。

2.3.3 质量保证要求

1.为保证信息安全等级测评项目质量，要求在测评过程中就等级测评过程控制、等级测评过程监督、等级测评结果的验证等方面严格按照国家相关标准要求执行。

2.参与等级测评的每个人都应具有等级测评师安全服务资质。

3.项目成员必须提供测评师的证书（复印件加盖公章）及社保缴费证明。