# 网络安全等级保护测评服务项目采购需求

**一、资格要求**

1、符合《中华人民共和国政府采购法》第二十二条规定的供应商资格条件；

2、投标人应具有国家公安部颁发的网络安全等级测评与检测评估机构服务认证证书；

3、在最近五年内未发生过被责令停产停业、暂扣或者吊销许可证、营业执照等行为；

**二、测评要求**

根据国家等级保护相关标准，投标人对上述信息系统完成测评、整改、报备等工作。要求对以上业务信息系统进行摸底、分析和梳理，提出测评方案。逐一对信息系统进行安全等级保护测评，信息系统安全等级保护测评的内容包括但不限于以下内容：

(1) 安全技术测评：包括安全物理环境、安全区域边界、安全计算环境、安全通信网络、安全管理中心五个方面的安全测评；

(2) 安全管理测评：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五个方面的安全控制测评；

(3)完成测评工作后，提出整改方案并实施整改，最后出具符合公安机关要求的信息系统安全保护等级测评报告，并协助上述系统单位完成信息系统安全保护等级备案工作；

(4)所有等保测评实施工作须在3个月内完成（不包含整改时间）。

**三、测评范围**

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 系统等级 |
| 1 | 永康市电子政务外网 | 三级 |
| 2 | 永康市公共数据平台 | 三级 |

**四、依据标准**

开展重要信息系统等级测评等服务，依据标准包括但不限于以下要求及标准：

(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 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》；

(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 22240-2020 《信息安全技术 网络安全等级保护定级指南》；

(5)GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》。

**五、服务内容**

1、基于GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》的等级保护测评服务（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、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十个方面的安全测评），并提交符合公安部门主管单位要求的信息系统安全保护等级测评报告。

2、对被测系统提出整改意见，协助被测单位完成测评系统的问题整改和修复工作，通过公安部门主管单位的网络安全等级保护要求。

**六、服务原则**

1、标准性原则：服务方案的设计与实施应依据国家等级保护相关标准进行。

2、规范性原则：服务工作过程中的文档，具有良好的规范性，便于项目的跟踪和控制。

3、可控性原则：服务工作的进度要严格进度表的安排。

4、整体性原则：服务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。

5、最小影响原则：服务工作对系统和网络的影响必须在可控范围内，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。

**七、保密要求**

对服务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方的责任；

对涉及客户的检查项目、资料、检查过程和结果以及客户的知识产权、所有权等其它信息采取保密措施；

在接收客户的检查项目时，应对检查项目加强监管，防止泄密。信息安全等级保护评测之前必须签订保密协议。所有检查项目，不经用户同意，不得向与检查无关人员展示；

所有检查过程对外保密，与检查无关人员未经批准，不得擅自进入检查现场；

在未经许可的情况下与检查无关的人员不得接触被检查项目及相关资料，不得参与检查和编制检查报告；

出具的检查报告应为客户保密，未经客户授权，不得将检查报告转交他人，不得擅自公布检查结果；

当客户要求用电话、图文传真或其它方式传送检查结果时，应有客户正式的书面委托并证实相关通讯方式可靠后方可执行；

不得向无关人员泄露任何有关客户资料和检查结果，检查结果只能通过相关程序及约定的告知方式通知相应业务单位和个人；

对接触客户检查项目、资料及其它相关信息的人员应履行为客户保护所有权的义务，不得利用客户的有关知识产权为己牟利。