# 南通市城市管理局网络安全等级保护测评及安全运维服务项目需求

1. **项目背景：**

网络安全在我国新的互联网发展形势下已经变的越来越重要，伴随着《网络安全法》的颁布，全国范围的所有网络运营单位都在响应法律号召，积极做好网络安全防护工作，落实网络安全等级保护制度。

南通市城市管理局对此也高度重视积极响应，定期对单位网络系统进行网络安全等级测评工作，以及同步对网络进行安全建设整改。现为进一步缩小单位网络与国家等级保护GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》标准之间的差距，参照国家等级保护GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》标准（2.0标准），采购专业的网络安全服务对单位信息系统进行网络安全防护。

**二、服务需求清单**

**1、等保测评服务内容**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 系统数量 | 备案情况 | 备注 |
|  | 南通市智慧停车综合监管平台 | 1个 | **三级** |  |
|  | 南通市建筑垃圾监管服务综合管理系统 | 1个 | **二级** |  |
|  | 南通市城市管理综合执法平台 | 1个 | **二级** |  |

**2、网络安全服务内容**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务项目 | 服务内容 | 服务时间 |
| 1 | 安全巡检（核查）服务 | 1.安全配置检查服务：检查安全设备的安全策略是否合规，配置是否生效、特征库等是否更新；  2.逐一核查本单位的重要信息系统，特别是关基、功能和服务范围是否同互联网连接；  3.逐一核查设备、软件漏洞情况及数量；  4.核查高危漏口关闭、核查漏洞补丁，禁止共享和远程桌面；  5.邮件系统核查：更新密码、删除离职人员账户、关闭自动转发功能；是否使用社会邮箱；  6.核查网络防护、定时扫描发现篡改、劫持、暗链发现等事件、是否能抵御DDOS攻击；  7.核查云平台是否通过安全评估；  8.其他应该核查的内容。 | 服务期内每月1次 |
| 2 | 安全日志分析 | 对网络中所有安全系统包括防病毒、客户端管理系统的日志汇总与分析，评估网络安全系统的运行状态。 | 服务期内每季度1次 |
| 3 | 漏洞扫描 | 1.对网络设备、安全设备、服务器操作系统和业务应用系统的安全扫描检测服务，通过安全扫描检查设备操作系统和应用系统的漏洞；  2.有新设备或新业务上线时，对业务及设备进行安全扫描检查，并提供结果报告。 | 服务期内每月1次 |
| 4 | 网络安全加固 | 提供安全设备的配置核查，并定期进行日志分析，对当前的网络攻击给出合理有效建议，并优化安全设备的配置以达到更安全的目标。 | 服务期内每月1次 |
| 5 | 等保云防服务 | 提供服务期一年的网站防护服务。 | 一年 |
| 6 | 应急演练服务 | 在服务过程中，提供一次信息系统网络安全应急演练相关服务。提供完整的应急演练方案，同时做好应急演练相关预案。应急演练完成后提供相关应急演练报告。 | 服务期内1次 |
| 7 | 安全咨询服务 | 日常咨询服务、项目咨询服务 | 按需、实时 |
| 8 | 应急响应服务 | 对发生的安全事件，如恶意攻击、病毒入侵等协助进行应急响应处理。 | 按需、实时 |
| 9 | 安全培训服务 | 合同期限内对单位内部人员开展集中的网络安全培训1次，提供培训的讲师及培训内容资料。 | 1次 |

**3、提供网站安全及微信公众号等相关业务**

3.1对南通市城市管理局网站及微信公众号提供7\*24小时可用性检测。发现访问异常后报告，并协助处置。

3.2定期每月对网站系统开展应用系统漏洞扫描，发现漏洞及时配合软件开发商及时修补相关漏洞。

**三、具体需求说明**

### 等保测评需求

**（一）测评内容**

1.总体要求：

A．完成上述系统安全等级测评工作，测评后经用户方确认，出具符合网络安全等级保护测评要求的测评报告；

B．对上述系统不符合网络安全等级保护有关管理规范和技术标准的，提出可行性整改方案，提供相应的安全整改建议书。

2.质量要求：

A．等级测评及服务原则：符合性原则、标准性原则、规范性原则、可控性原则、整体性原则。

B．网络安全等级保护定级及测评服务依据：

《中华人民共和国网络安全法》

《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》，

《GB/T28448-2019 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》，

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

3.网络安全等级保护测评内容：

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

B．安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理五个方面的安全控制测评

4.提供整改咨询服务，根据所测系统的最终测评报告，对系统现状提出安全整改建议并协助整改工作，以期达到整改目的。

**（二）测评原则**

1.客观性和公正性原则：

测评人员应当没有偏见，在最小主观判断情形下，按照评估双方相互认可的评估方案，基于明确定义的测评方式和解释，实施评估活动。

2.可重复性和可再现性原则：

依照同样的要求，使用同样的评估方式，对每个评估实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同评估者评估结果的一致性有关，后者与同一评估者评估结果的一致性有关。

3.连续性原则：

确保在高速变化的信息安全环境中，在有效的服务期间内，保证采购方风险评估结论的准确性和及时性，对于采购方单位新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。从经济上，降低了采购方单位的成本，从信息安全性上，保证信息安全测评的动态稳定性。

4.扩展性原则：

在评估过程结束后，信息安全测评过程要保持扩展性，从扩展的属性上进一步加强测评结束后采购方的安全管理有效性和可用性。

5.保密原则：

在测评过程中，需严格遵循保密原则，双方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购方利益。

6.互动原则：

在整个测评过程中，强调采购方的互动参与，每个阶段都能够及时根据采购方的要求和实际情况对测评的内容、方式做出相关调整，进而更好的进行风险评估工作。

7.最小影响原则：

测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

8.规范性原则：

网络安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

9.质量保障原则：

在整个测评过程中，须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

**（三）测评人员和时限要求**

1.测评人员要求：本次测评至少需要1名高级测评师，1名中级测评师，2名初级测评师。本次等保测评项目不得转包或者分包，所有测评师必须是成交供应商自己的正式员工,所有测评师必须持证上岗，响应文件中应提供项目组成员名单、社保主管部门出具的响应单位为其缴纳社保的证明、相关证书复印件等，未经采购方同意，项目组成员不得更改。

2.测评时间要求：按照被测单位要求，合同签订完毕一周内启动测评工作。

3.测评期限要求：签订合同后60天内完成网络安全等级保护测评并出具盖章报告，并完成备案。

**四、其他**

1.网络安全服务期限要求：合同签订起一年。

2.测评期限要求: 签订合同后60天内完成网络安全等级保护测评并出具盖章报告，并完成备案。

3、交货（服务）地点：采购方现场。

4、付款方式：合同签订后收到成交供应商正式合法有效税务发票的30日内支付合同款50%；提交测评报告后，采购人于2023年12月20日前收到成交供应商正式合法有效税务发票后支付余款。以上付款均不计利息。

5、由于供应商的原因所造成的额外费用，由供应商自行承担。如果采购人要求删除或增加功能，供应商应适当调整，但是响应文件中的各项优惠条件保持不变。供应商如果有其他优惠条件，必须作专门说明。

6、以上条款的内容如果需要修改或者有其他未涉及的事项，由双方协商解决。

**五、违约情况**

1、若在供应商服务期间发生重大网络安全事故，每发生一次扣除供应商合同总金额的5%。

2、若供应商未经采购人书面同意转让本合同下的业务，采购人有权拒绝支付或扣减转让部分的服务费用，扣减费用如不足以弥补采购人损失，则供应商还应补偿采购人因此造成的损失。

3、因供应商原因造成的设备损坏的，供应商应进行修理、更换并赔偿采购人因此造成的损失。