**风险告知与规避方案**

**项目编号：**

**项目名称：**

等级测评工作，是指测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检测评估的活动。等级测评是合规性评判活动，依据网络安全等级保护的国家有关标准，按照特定方法对信息系统的安全保护能力进行科学公正的综合评判过程。按照国家标准，在等级测评过程中会采用访谈、核查、渗透测试等测评方法，根据不同的方法在等级测评过程中会产生风险，针对在测评过程中产生的相关风险，提出规避方案，如下：

风险一：在等级测评过程中需要对测评对象所在网络部署的机房进行实地核查与检测，在进出机房与针对机房的标准检测过程中会在机房进行停留，对机房以及机房内部署的基础硬件设施的封闭运行和日常巡检等工作可能会产生变量影响。

规避方案：在等级测评过程中，在机房进行的核查工作需向客户单位进行申请并经过有效流程的审批通过后，测评人员方可持证明进入机房。测评人员进入机房后需在管理运维人员的陪同下，在机房内的规定区域进行活动和检查工作。

风险二：在等级测评过程中需要对测评对象所在网络环境中的硬件设备进行检测和核查（包括如安全设备、网络设备、服务器等相关设备），需要对设备进行登录、配置核查、运行情况观察等相关操作，会对相关硬件设备产生变量影响。

规避方案：测评人员在对机房设备进行配置核查工作时全程需由管理人员对设备进行连接、登录、查询等技术操作，测评人员以访谈和观察记录的方式进行核查，在无特殊授权的情况下不得亲自动手操作。测评人员在核查结束时应检查设备的运行情况和状态，删除测试账户和相关测评痕迹，并与管理员确认后方可离场。

风险三：在等级测评过程中需要对测评对象进行漏洞扫描、渗透测试等验证性检测工作，采用接入工具等相关方式对系统进行检测，会对系统产生不同程度的运行影响，如产生攻击警告、系统运行速度变慢或系统运行短暂中断等不同程度的影响。

规避方案：测评人员在进行工具扫描活动前，应提前询问管理员系统应用的业务高峰期和业务运行状态，并与管理员确认最佳扫描时间和工具接入点。测评人员在工具扫描时，需全程在管理员的陪同下进行工具接入、开始扫描、结束扫描（或中断扫描）、拔出工具、恢复系统原样等一系列规定动作。如在扫描过程中出现如系统中断等事故时，应及时中断扫描并配合管理人员进行问题排查和系统恢复。渗透测试人员在进行渗透测试前，需提前与管理人员进行沟通，确认渗透时间与范围，并取得管理人员的授权。

风险四：在等级测评过程中需要进行访谈类检测方式，会产生沟通渠道不通顺、交流产生误差等变量影响。

规避方案：测评人员在测评过程中遇到沟通不通畅问题时，及时与业务对接人员进行沟通与情况说明，尽快排除问题，恢复测评流程。

风险五：不可抗力因素，在等级测评过程中任何因测评方无法控制的因素，包括但不限于地震、水灾、火灾、政府管制、国际或国内限制以及停电、技术故障、电子故障等其他无法预料或防范的不可抗力事件都可能对测评对象的正常运行产生变量影响。

规避方案：测评人员在测评过程中遇到不可抗力因素（包括但不限于地震、水灾、火灾、政府管制、国际或国内限制以及停电、技术故障、电子故障等）无法进行测评活动时，应立即采取保护措施保证安全，在可恢复工作时继续进行测评工作。

上述风险皆为列举事项，未能包括在等级测评中可能出现的所有风险，客户在统一开始测评工作前还应认真的对其他可能产生的风险进行了解和掌握。在等级测评过程中若非由于测评工作人员的操作失误而产生的意外风险所导致的后果由客户自身承担。针对测评过程中遇到的风险类别可采取的防范与应对措施，测评人员与被测评对象管理方应仔细阅读后方可开始测评工作。

本风险告知规避方案请客户认真阅读并仔细考虑，在确认无误无异议后双方进行签字盖章后生效。本告知书一式两份，由双方妥善保存，丢失不予补办。

委托方（盖章）： 测评方（盖章）：

委托方签字： 测评方签字：

年 月 日 年 月 日