项目编号：（DJCP2019110XXX）-XXXXX

**测评风险告知书**

在现场测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机验证并查看一些信息，这就可能对系统运行造成一定的影响，甚至存在误操作的可能。

使用测试工具进行漏洞扫描测试、性能测试及渗透测试等，可能会对网络和系统的负载造成一定的影响，渗透性攻击测试还可能影响到服务器和系统正常运行，如出现重启、服务中断、渗透过程中植入的代码未完全清理等现象。

具体测评中面临的安全风险如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **可能存在的风险** | **风险等级** | **控制措施** |
| 信息资产调研 | 资产信息泄漏 | 高 | 保密协议、规章、制度、法律、法  规 |
| 安全管理测评 | 安全管理信息泄漏 | 高 | 合同、保密协议、规章、制度、法  律、法规 |
| 网络设备测评/ 安全设备测评 | 误操作引起设备崩溃或数据丢失、损坏 | 高 | 测评人员不进行上机操作，修改策略，由被测评单位配合人员进行操作。  规范测评流程； 严格选择测评师；  签署《现场测评授权书》甲方进行全程监控；  制定可能的恢复计划 |
| 网络/安全设备资源占  用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 漏洞扫描/渗透测试 | 网络流量 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 主机资源占用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **可能存在的风险** | **风险等级** | **控制措施** |
|  | 设备死机 | 高 | 提前进行数据备份，制定恢复策略 |
| 控制台审计 | 误操作引起系统崩溃或数据丢失、损坏 | 高 | 规范审计流程； 严格选择测评师；  甲方进行全程监控；  制定可能的恢复计划； |
| 网络流量和主机资源  占用 | 低 | 避开业务高峰 |
| 应用测评 | 产生非法数据，致使系  统不能正常工作 | 中 | 做好系统备份和恢复措施 |
| 异常输入（畸形数据、  极限测试）导致系统崩溃 | 高 | 做好系统备份和恢复措施签署《现场测评授权书》 |
| 测评痕迹 | 木马、内容篡改等 | 高 | 对测评痕迹进行清理 |

被测评单位已知悉测评风险告知书内容，了解测评过程中可能面临的安全风险，已做好相关安全防护措施，并积极配合测评工作。

# 被测评单位签字： XX

**日期： 2020 年 11 月 5 日**