**网络与信息安全问卷调查表**

单位名称：\_\_\_\_\_\_\_\_\_\_\_\_\_ 部门名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

填表人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 联系电话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1．本单位是否与网络和信息系统同步规划、建设、投入使用网络与信息安全设施？

□是 □否

2．本单位信息系统安全保护等级确定为（若有多个系统，需分别填报说明）？

□一级 □二级 □三级 □四级 □五级 □未定级

3．本单位是否已经制定、实行网络与信息安全管理制度？

□已经制定并严格实行 □正在规划并逐步实行

□已经制定，但并没有实行 □暂无这方面的规划

4．本单位设置了哪些安全管理岗位？（多选）

□系统管理员 □安全管理员 □网络管理员 □其他

5．本单位在网络与信息安全方面采取了以下哪些管理和技术措施？（多选）

□数据备份 □数字证书 □身份鉴别 □访问控制 □防火墙

□入侵防范 □漏洞扫描 □防病毒 □加密 □抗抵赖

□安全审计 □系统安全加固 □制定安全管理规章制度

□定期进行安全风险评估 □制定应急处置预案和措施 □其他

6．本单位在物理安全方面做了以下哪些防护？（多选）

□机房设置在具有防震、防风和防雨等能力的建筑内

□机房出入口有专人值守，控制、鉴别和记录进入的人员

□重要区域配置了电子门禁系统，控制、鉴别和记录进入的人员

□机房安装了必要的防盗报警设施

□机房设置了避雷装置

□机房设置了交流电源地线

□机房设置了灭火设备和火灾自动报警系统

□机房关键设备采用了必要的接地防静电措施

□机房设置了温、湿度自动调节设施

□机房供电线路上配置了稳压器和过电压防护设备

□机房提供备用电力供应系统，满足关键设备在断电情况下的正常运行要求

□机房对关键设备和磁介质实施电磁屏蔽

□其他

7．本单位是否在用户身份认证方面使用了密码技术和密码产品？

 □是 □否

如果是，使用了何种密码技术和产品

8．本单位是否在网络和信息系统访问控制方面使用了密码技术和密码产品？

 □是 □否

如果是，使用了何种密码技术和产品

9．本单位是否在数据保护方面使用了密码技术和密码产品？

 □是 □否

 如果是，使用了何种密码技术和产品

10．本单位是否在可信服务方面使用了密码技术和密码产品？

 □是 □否

如果是，使用了何种密码技术和产品

11．本单位是否在安全审计方面使用了密码技术和密码产品？

 □是 □否

 如果是，使用了何种密码技术和产品

12．本单位是否在电子文件生成、传输、存储等环节采用了密码技术和密码产品进行安全防护？

 □是 □否

如果是，使用了何种密码技术和产品

13．本单位是否对用户进行基于数字证书的身份鉴别？

□是 □否

14．本单位是否能够对信息内容进行过滤？

 □是 □否

15．本单位是否对网络设备运行状况、网络流量、用户行为等进行日志记录？

□是 □否

16．本单位是否能够对非授权设备私自连接内部网络的行为进行检查？（若否，跳过下一个问题）

□是 □否

17．如果是，是否能够准确确定位置，并对其进行有效阻断？

□是 □否

18．本单位是否能够对网络边界处或主机的恶意代码进行检测和清除？

□是 □否

19．若是，系统能否实现防恶意代码的统一管理？（若否，跳过下一个问题）

□能 □否

20．当对服务器进行远程管理时，能否防止鉴别信息在网络传输过程中被窃听？

□能 □否

如果采取了相应的措施，则采取的措施是：

21．本单位是否对重要的信息资源设置敏感标记？

□是 □否

22．本单位数据备份采取的方式有哪些？

□本地备份 □异地备份 □其他

23．本单位是否具备数据恢复措施？

□是 □否

24．在设计网络的拓扑结构时是否采用冗余技术？

□是 □否

25．本单位提供的硬件冗余包括哪些硬件？（多选）

□网络设备 □通信线路 □服务器 □存储 □无 □其他

26．本单位安全审计的内容包括？（多选）

□重要用户行为 □系统资源的异常使用

□重要系统命令的使用 □其他

27．本单位是否发生过网络与信息安全事件？（若否，跳过下一个问题）

□没有 □1次 □2次 □3次 □其他 次

28．本单位曾经发生的网络与信息安全事件类型？（多选）

□网络窃密/泄密 □窃取信息或知识产权 □主干网络中断

□垃圾邮件 □网络/系统或数据遭到破坏 □网络欺诈、网络钓鱼

□出现病毒、蠕虫、木马及间谍软件等 □网页被篡改

□遭到端口扫描、网络攻击或未授权使用网络 □机房发生火灾等事故

□内部人员破坏或滥用网络资源 □其他

29．本单位能够对网络边界处的哪些攻击行为进行监视？（多选）

□端口扫描 □木马后门攻击 □拒绝服务攻击

□强力攻击 □缓冲区溢出攻击 □IP碎片攻击

□网络蠕虫攻击 □其他

30．本单位如何发现网络与信息安全事件？（多选）

□事后分析发现 □网络安全产品告警发现

□通过技术监测发现 □意外发现

□有关部门通知或他人告知 □其他

31．本单位网络与信息安全存在的问题？（多选）

□安全意识和观念薄弱 □网络安全管理人员不足，缺乏培训 □缺乏安全管理制度或制度不落实 □网络安全保护资金投入不足

□缺乏与网络安全主管部门沟通 □网络安全产品不能满足要求 □其他

32．本单位采购的哪些安全产品实现了国产化？哪些安全产品未实现国产化？未实现的原因是什么（列表说明）？

33．本单位的哪些数据库、重要信息资源、重要网络与信息系统需要进行重点安全防护？防护到怎样的程度？预测未来5年内的网络流量和用户数量情况等（列表说明）

34．本单位在网络与信息安全方面还制定了哪些行政管理的制度、办法等？

35．本单位在网络与信息安全方面还需说明的其他情况：

36. 本单位对省政务信息中心网络与信息安全规划、建设、管理等方面的建议

37. 本单位对省灾备中心规划、建设、管理等方面的建议：