怀远县审计局网络与信息安全防护策略

一、编制目的

实现怀远县审计局网络与信息安全防护和管理，推进各项安全控制措施落实到位，提高整体防护能力和水平，确保网络与信息系统正常运行和安全。

二、编制依据

《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《关于信息安全等级保护建设的实施指导意见》（信息运安〔2009〕27号）、《信息安全技术信息系统安全管理要求》（GB/T20269—2006）、《审计署办公厅关于印发审计机关网络与信息安全信息通报机制暂行规定的通知》（审办计发〔2017〕74号）等相关规定。

三、适用范围

县审计局信息系统资产和信息技术人员的安全管理和指导、网络与信息系统安全策略的制定、安全防护方案的实施以及安全管理措施的选择等。

四、工作原则

坚持统一领导、分级负责、全员参与的原则；坚持科学规划、预防为主、持续改进的原则；坚持依法管理、管理与技术并重、综合防范的原则。

五、安全策略

（一）规划设计安全策略

1.网络与信息系统的规划与设计必须满足安全运行和信

息保密的需要；

2.网络与信息系统建设过程中，必须同步规划、同步设计和同步实施网络与信息安全系统。

（二）物理安全策略

1.机房必须选择在经过防震、防火、防雷击验收合格的办公大楼内部，机房门窗应具备防雨水渗透的能力；

2.机房的位置不能是大楼的地下室、一楼房间或是大楼的顶层，机房的正上方不能是用水量大的房间；

3.进入机房的工作人员必须由安全管理员或机房管理员全程陪同，并进行登记；

4.机房内部必须划分重要设备区、一般设备区、过渡区等区域，对不同区域分别进行管理，区域与区域之间进行物理隔离；

5.机房内部必须部署基础防护系统和设备，如电子门禁系统、监控报警系统、防雷设备、消防灭火系统、防水监控系统、温湿度控制系统、UPS 供电系统和电磁屏蔽等设备。

（三）网络安全策略

1.县审计局接入市局内网必须部署防火墙；

2.主要网络设备除接入交换机以及接入交换机链接工作终端的线路之外，应进行双机热备和双线冗余；

3.整体网络应避免出现流量瓶颈，保证带宽充足；

4.必须严格执行审计转网和互联网物理分离，严禁通过各种方式造成内外网混用；

5.审计专网应进行合理的 IP 地址划分；

6.划分网络带宽，应突出优先级；

7.网络边界处必须部署防火墙、IPS 等安全设备；

8.网络设备必须开启日志审计功能。

（四）主机安全策略

1.登录操作系统和数据库系统的用户，必须进行身份标识和鉴别；

2.操作系统和数据库系统管理用户身份标识不得出现同名用户，口令应有复杂度要求并定期更换；

3.操作系统和数据库系统必须启用登录失败处理功能；

4.对服务器进行远程管理时，必须采取必要措施，防止鉴别信息在网络传输过程中被窃听；

5.为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性，杜绝重名情况；

6.操作系统和数据库必须及时删除多余的、过期的账户，避免共享账户的存在；

7.主机必须开启日志审计功能；

8.主机必须安装防恶意代码产品，并进行统一管理。

（五）应用安全策略

1.应用系统必须在登录时输入用户名和口令，不得使用初始密码长期访问各应用系统；

2.登录应用系统必须进行两种或两种以上的复合身份验证；

3.应用系统中设置的用户都必须是唯一用户，名称不得相同，且不得出现多人使用同一账户的情况；

4.应用系统必须开启登录连接超时自动退出等措施；

5.应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；

6.应用系统必须开启日志审计功能；

7.应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清除内部存储的信息。

（六）数据安全策略

1.业务应用数据和设备配置文档都必须进行备份，以便发生问题时恢复；

2.数据备份至其他设备时，必须使用专门的备份通道，保证数据传输的完整性；

3.数据本机备份时应检测其完整性；

4.数据备份时必须使用专业的备份设备和工具，在数据传输和数据存储时，必须是加密传输和存储；

5.数据进行异地备份时，必须利用通信网络将关键数据定时批量传送至备用场地。

（七）安全管理机构要求

1.设立网络与信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

2.成立网络安全和信息化领导小组，负责人由单位主要领导担任；

3.设立系统管理员、网络管理员、安全管理员等岗位，

明确安全管理机构各个部门和岗位的职责、分工和技能要求；

4.配备专职安全管理员，关键事务岗位应配备多人共同管理；

5.根据岗位的职责，明确授权审批事项、审批部门和审批人等，定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息并记录审批过程，保存审批文档；

6.针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，对重要活动建立逐级审批制度；

7.加强各类管理人员之间、组织内部机构之间、兄弟单位、公安机关、电信公司、供应商、业界专家、专业的安全公司以及网络与信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理网络与信息安全问题；

8.在网络安全和信息化领导小组领导下定期开展安全检查，检查内容包括安全管理责任落实和制度的执行情况、现有安全技术措施的有效性、安全配置与安全策略的一致性、系统日常运行、系统漏洞和数据备份等情况并汇总安全检查数据，形成安全检查报告，对安全检查结果及时整改通报。

（八）安全管理制度要求

1.应制订网络与信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，形成由安全策略、管理制度、操作规程等构成的全面的网络与信息安全管理制度体系；

2.对安全管理活动中的各类管理内容，建立安全管理制度,对管理人员或操作人员执行的日常管理操作,建立操作规程；

3.网络安全和信息化领导小组办公室负责定期组织相关部门人员对安全管理制度体系的合理性和适用性进行审定，对存在不足或需要改进的安全管理制度进行修订。

（九）人员安全管理要求

1.网络与信息系统运维或代维人员应签署保密协议；

2.从事关键岗位的人员，签署岗位安全协议；

3.应严格规范人员离岗管理，及时终止离岗员工的所有访问权限,人员离岗后及时取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；关键岗位人员离岗，须承诺调离后的保密义务，方可离开；

4.定期对各个岗位的人员进行安全技能及安全认知的考核,对关键岗位的人员进行全面、严格的安全审查和技能考核，对考核结果进行记录并保存；

5.对全体人员进行安全意识教育、岗位技能培训和相关安全技术培训,告知相关人员书面规定的安全责任和惩戒措施，对违反违背安全策略和规定的人员进行惩戒；

6．对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，对外部人员访问受控区域前，先提出书面申请，批准后由专人全程陪同或监督，并登记备案。

（十）系统建设管理要求

1.明确网络与信息系统的边界和安全保护等级，以书面

形式说明确定网络与信息系统为某个安全保护等级的方法和理由，并组织相关部门和安全技术专家对网络与信息系统定级结果的合理性和正确性进行论证和审定。

2.根据系统安全保护等级选择基本安全措施，授权专门部门对网络与信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划，并根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件，组织相关部门和有关专家进行合理性和正确性论证审定，经过批准后方可实施。

3.安全产品、密码产品等关键产品和关键软件的采购，应符合国家和上级机关的有关规定。

4.软件开发应保证开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制，制定软件开发管理制度、代码编写安全规范、软件设计的相关方案和使用指南，并在软件安装之前检测软件包中可能存在的恶意代码和后门。

5.授权专门部门负责工程实施过程和测试验收的管理，制定详细的工程实施方案、测试验收相关管理制度，明确说明实施过程的控制方法，并选择第三方测试单位对系统进行安全性测试，出具安全性测试报告；在测试验收过程中详细记录测试验收结果，并形成测试验收报告，组织相关人员对验收报告进行审定和签字确认，制定详细的系统交付清单，对系统运维人员进行技能培训。

6.选择相关资质的测评机构进行等级测评，对测评发现的问题，及时整改；系统发生变更或安全等级发生变化时，应及时进行等级测评或调整安全等级级别，并进行安全改造。

（十一）系统运维管理要求

1.制定安全事件报告和处置管理制度，规定安全事件报告和响应处理程序，确定事件的报告流程、响应和处置的范围、程度以及处理方法等。

2.建立资产安全管理制度，规定网络与信息系统资产管理的责任部门、责任人员,编制并保存网络与信息系统相关的资产清单，根据重要程度对资产进行标识管理和制定相应的管理措施。

3.根据数据的重要性和数据对系统运行的影响程度，制定数据的备份策略和恢复策略，备份策略须指明备份数据放置场所、文件命名规则、介质替换频率和数据离站运输的方法。

4.建立介质安全管理制度，对介质的存放环境、使用、维护、销毁等作出规定；对送出维修或销毁的介质，应首先清除介质中的敏感数据，对保密性较高的存储介质，未经批准不得自行销毁；对重要介质中的数据和软件采取加密存储。

5.指定专门人员负责机房安全，定期对机房供配电、空调、温湿度控制等设施进行维护管理；加强对办公环境的保密性管理，规范办公人员行为，包括工作人员调离办公室应

立即交还该办公室钥匙、工作人员离开座位应确保终端计算机退出登录状态等。

6.建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

7.对系统相关人员进行应急预案培训，每年培训一次；定期对应急预案进行演练，定期审查和根据实际情况更新内容。

8.安全服务商的选择，应符合国家有关规定；选定的安全服务商应签订安全保密协议或服务合同，明确相关责任。