南昌航空大学

校保密字〔2016〕6 号

南昌航空大学
涉密计算机及信息系统安全策略文件

1 概述

涉密计算机及信息系统安全策略文件属于顶层的管理文档，是学校网络与信息安全保障工作的出发点和核心，是学校计算机与信息系统安全管理和技术措施实施的指导性文件。是我校计算机和信息系统全体管理和使用人员必须遵循的信息安全行为准则。由保密办公室联合现代教育技术于信息中心制订，经校保密委员会审批发布，并组织学校相关人员学习与贯彻。

涉密计算机及信息系统涉及到存储、传输、处理国家秘密，必须保证其安全。因此，必须从技术、管理、运行等方面制订确保涉密计算机和信息系统持续可靠运行的安全策略，做好安全保障。

我校计算机及信息管理系统管理分为涉密计算机管理、非涉密内部计算机管理、互联网信息系统及计算机管理三个

层次。

涉及国家秘密的信息必须由相应等级的**涉密计算机**处理，实行物理隔离管理，由学校保密管理部门安装专用的防护及审计系统，只能由我校涉密人员使用，由所属保密要害部位涉密人员管理。涉密计算机信息数据必须被保护以防止被泄露、破坏或修改。

非涉密内部计算机应与互联网隔离，配置保密管理措施，只能通过指定的移动存储介质传输，储存技术文档、软件等涉及学校的内部信息。上述信息必须定期备份，以免被破坏和非授权修改。

互联网信息系统及计算机主要处理来自于外部资源的普通信息，同样在信息安全防护上进行安全考虑。

2 策略

本策略文件主要包括：物理安全策略、运行管理策略、信息安全策略、备份与恢复策略、应急计划和相应策略、计算机病毒与恶意代码防护策略、身份鉴别策略、访问控制策略、信息完整性保护策略、安全审计策略。

物理安全策略

计算机信息和其他用于存储、处理或传输信息的物理设施，例如硬件、磁介质、电缆等，对于物理破坏来说是易受攻击的，同时也不可能完全消除这些风险。因此，应该将这些信息及物理设施放置于适当的环境中并在物理上给予保护使之免受安全威胁和环境危害。

- 应该对计算机介质进行控制，如果必要的话需要进行物理保护。可移动的计算机应该受控;

- 设备应放置在合适的位置或加强保护，将被如水或火破坏、干扰或非授权访问的风险降低到可接受的程度;
- 对设备应该进行保护，以免受电源故障或其他电力异常的损害;
- 对计算机和设备环境应该进行监控，必要的话要检查环境的影响因素，如温度和湿度是否超过正常界限;
- 对设备应该按照生产商的说明进行有序的维护;

运行管理策略

为避免信息遭受人为过失、窃取、欺骗、滥用的风险，应当识别计算机及信息系统内部每项工作的信息安全职责并补充相关的程序文件。学校全体相关人员都应该了解计算机及系统的网络与信息安全需求。

- 信息设备和存储介质应当具有标识、涉密的应当标明密级，非密的应当标明用途;
- 涉密计算机应当实行物理隔离;
- 涉密计算机操作人员应保留操作日志记录。包括:系统开机和关机时间；系统应用错误和采取的纠正措施;
- 禁止使用非涉密的计算机和存储介质存储和处理涉密信息;
- 未经保密办审批，禁止对计算机系统格式化或重装系统;
- 涉密人员不得擅自更改和卸载正在使用中的计算机安全防护及审计软件或硬件，必须事先通过保密办的审批;
- 当涉密人员调离涉密岗位时应该移交所掌握的涉密

计算机及涉密载体;

信息安全策略

为保护存储计算机的数据信息的安全性、完整性、可用性，保护系统中的信息免受恶意的或偶然的篡改、伪造和窃取，有效控制内部泄密的途径和防范来自外部的破坏，制订以下安全措施。

- 设置屏幕保护，涉密计算机要求设置保护时间为 1 分种，恢复时有密码保护;
- 涉密计算机禁止安装多启动操作系统，只能安装一个操作系统;
- 及时安装操作系统、数据库、应用程序的升级补丁;
- 拆除涉密计算机中具有无线联网功能的硬件模块;
- 涉密计算机应配备电磁泄露发射防护装置;
- 需要向涉密计算机中输入信息时，只能采用读取一次性写入的光盘或者使用保密技术防护专用系统（三合一）提供的单导盒输入普通移动介质（U 盘）内的信息资料。

备份与恢复策略

计算机及信息系统数据备份与恢复的基本措施包括:

- 建立有效的备份与恢复机制;
- 定期检测自动备份系统是否正常工作;
- 明确备份的操作人员职责、工作流程和工作审批制度;
- 建立完善的备份工作操作技术文档;
- 针对建立的备份与恢复机制进行演习;
- 对备份的类型和恢复的方式进行明确的定义;

- 妥善保管备份介质;

应急计划和相应策略

应该制订和实施应急计划和响应管理程序，将预防和恢复控制措施相结合，将安全故障造成的影响降低到可以接受的水平。

- 考虑突发事件的可能性和影响;
- 了解中断信息系统服务可能对业务造成的影响，并确定信息处理设施的业务目标;
- 定期对应急计划和响应程序进行检查和必要的演练，确保其始终有效;
- 适当的对技术人员进行培训，让他们了解包括危机管理在内的应急程序;
- 必须建立有效的信息反馈渠道，以便于一旦发现安全威胁、事件和故障，能及时向有关领导报告;

计算机病毒与恶意代码防护策略

病毒防范包括预防和检查病毒（包括实时扫描/过滤和定期检查），主要内容包括:

- 控制病毒入侵途径;
- 安装可靠的防病毒软件;
- 对系统进行实时检测和过滤;
- 定期杀毒;
- 及时更新病毒库;
- 防病毒软件的安装和使用由计算机管理责任人执行;

身份鉴别策略

每台涉密计算机都应该指定专门的使用和负责人，如非

工作需要，原则上禁止他人登录使用。为保证计算机不被他人违规使用，制订以下措施:

- 采用有效的口令保护机制，包括: 规定口令的长度、有效期、口令规则。保障用户登录和口令的安全;
- 用户选择和使用密码时应参考良好的安全惯例
- 严格设置对重要服务器、网络设备的访问权限;
- 严格控制可以对重要服务器、网络设备进行访问的人员;
- 严格控制可以物理接触重要设备的人员;

访问控制策略

为了保护计算机系统中信息不被非授权的访问、操作或被破坏、必须对信息系统实行控制访问。

- 计算机活动应可以被追踪到人;
- 应使用有效的访问系统来鉴别用户;
- 特殊权限的分配应被安全地控制;
- 用户应确保无人看管的设备受到了适当的安全保护;
- 应根据系统的重要性制订监控系统的使用规程;
- 必须维护监控系统安全事件的审计跟踪记录;

信息完整性保护策略

由于我校计算机和信息系统采用三层管理模式，不排除连接到外部网络，计算机和信息系统的运行必须使用可控且安全的方式来管理，网络软件、数据和服务的完整性和可用性必须受到保护。

应当制订管理和操作所有计算机和网络所必须的职责和规程，来指导正确的和安全的操作，这些规程包括:

- 数据文件处理规程，包括验证网络传输的数据;
- 对所有计划好的系统开发、维护和测试工作的变更管理规程;
- 为意外事件准备的错误处理和和意外事件处理规程;
- 问题管理规程，包括记录所有网络问题和解决办法;
- 为所有新的或变更的硬件或软件，制订包括性能、可用性、可靠性、可恢复性和错误处理能力等方面的测试/评估规程;
- 日常管理活动，例如启动和关闭规程，数据备份，设备维护，计算机和网络管理，安全方法或需求;

安全审计策略

计算机及信息系统的信息安全审计活动和风险评估应当定期执行。特别是系统建设前或系统进行重大变更之前，必须进行风险评估工作。

涉密计算机安全审计应当 3 个月进行一次，并形成文档化的安全审计报告。

信息安全风险评估应当至少 1 年一次，可由学校自己组织进行或委托有信息系统风险评估资质的第三方机构进行。信息安全风险评估必须形成文档化的风险评估报告。