江西服装学院

网络与信息化管理中心文件

江服网管字〔2017〕4 号

江西服装学院信息安全工作总体方针

第一章 总则

第一条 为加强和规范江西服装学院及各部门信息系统安全工作，提高本单位信息系统整体安全防护水平，实现信息安全的可控、能控、在控，依据国家有关法律、法规的要求，特制定本方针。

第二条 本文档的目的是为江西服装学院信息系统安全管理提供一个总体的策略性架构文件，该文件将指导江西服装学院信息系统的安全管理体系的建立。安全管理体系的建立是为江西服装学院信息系统的安全管理工作提供参照，以实现江西服装学院统一的安全策略管理，提高整体的网络与信息安全水平，确保安全控制措施落实到位，保障网络通信畅通和业务系统的正常运营。

第三条 本文档适用于江西服装学院各部门信息系统资产和信息技术人员的安全管理和指导，适用于指导江西服装学院信息系统安全策略的制定、安全方案的规划和安全建设的实施，适用于江西服装学院安全管理体系中安全管理措施的选择。

第四条 引用标准及参考文件

本文档的编制参照了以下国家的标准和文件:

《中华人民共和国网络安全法》

《中国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 信息系统安全等级保护基本要求》(GB/T 22239-2008)

《信息安全技术 信息系统安全管理要求》(GB/T 20269—2006)

《信息系统等级保护 安全建设技术方案设计要求》(报批稿)

《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429 号)

第二章 方针、目标和原则

第五条 江西服装学院信息系统安全坚持“安全第一、预防

为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行信息系统安全等级保护制度。管理信息网络分为统内网和外网，实现“双机双网”，内网定位为承载涉密数据，外网定位为对外业务网络和访问互联网用户终端网络。内、外网之间实施强逻辑隔离的措施。

第六条 信息系统安全总体目标是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据丢失和失密，防止有害信息在网上传播，防止江西服装学院对外服务中断和由此造成的系统运行事故。

第七条 信息安全工作的总体原则

（1）基于安全需求原则

江西服装学院网络与信息化管理中心，应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全本单位上恰当地平衡安全投入与效果;

（2）主要领导负责原则

主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效;

（3）全员参与原则

信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全;

（4）系统方法原则

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率;

（5）持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性;

（6）依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响;

（7）分权和授权原则

对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限;

（8）选用成熟技术原则

成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先本单位部试点然后逐步推广，以减少或避免可能出现的失误;

（9）分级保护原则

按等级划分标准确定信息系统的安全保护等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护;

（10）管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标;

（11）自主保护和国家监管结合原则

对信息系统安全实行自主保护和国家保护相结合。江西服装学院要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

第八条 在规划和建设信息系统时,信息系统安全防护措施应按照“三同步”原则，与信息系统建设同步规划、同步建设、同步投入运行。

第三章 总体安全策略

第九条 物理安全策略

（1）中心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，机房的窗户需要有防雨水渗透的能力;

（2）中心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）中心机房有相关部门管理，对进出入人员进行登记;

（4)进入中心机房的工作人员必须由机房管理人员全程陪

同;

（5）中心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;

（6）中心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、温湿度控制系统、UPS 供电系统。

第十条 网络安全策略

（1）网络中必须部署路由器、交换机、防火墙、防毒墙、IPS 设备和内网网络管理、补丁分发等系统

（2）网络设备除接入交换机之外，须进行双机热备，除接入交换机链接工作终端的线路外，其他线路必须进行双线冗余;

（3）整体网络不能出现流量瓶颈，保证带宽充足;

（4）各部门必须划分不同网段的 IP 地址;

（5）划分网络带宽，突出优先级;

（6）网络边界处必须部署防火墙、IPS 等安全设备;

（7）网络设备必须开启日志审计功能;

第十一条 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能出现同名用户，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，不能出重名情况；

（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；

第十二条 应用安全策略

（1）应用系统必须在登录时要求输入用户名和口令；

（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，不能名称相同，且不能出现多人使用同一账户的情况；

（4）应用系统必须开启登录失败处理功能；

（5）应用系统必须开启登录连接超时自动退出等措施；

（6）应用系统必须开启身份鉴别、用户身份标识唯一性检

查、用户身份鉴别信息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;

（7）应用系统必须开启日志审计功能;

（8）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，必须清楚内部存储的信息;

第十三条 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，以便发生问题时进行恢复;

（2）数据备份至其他设备上时，必须使用专门的备份数据链路，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，都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。

第四章 附则

第十四条 本办法由江西服装学院网络安全与信息化领导小组办公室负责解释。

第十五条 各单位可根据本办法制定实施细则，报网络与信息化管理中心备案。

第十六条 本办法自印发之日起执行。

网络与信息化管理中心

2017 年 11 月 1 日

江西服装学院网络与信息化管理中心　　2017 年 6 月 10 日印发