江苏开放大学
江苏城市职业学院文件

苏开大（苏城院）〔2022〕30号

关于印发江苏开放大学（江苏城市职业学院）网络与信息安全管理办法（试行）的通知

各部门：

现将《江苏开放大学（江苏城市职业学院）网络与信息安全管理办法（试行）》印发给你们，请遵照执行。

江苏开放大学
（江苏城市职业学院）
2022年5月8日

江苏开放大学（江苏城市职业学院）
网络与信息安全管理办法（试行）

第一章　总　则

第一条　为贯彻落实《中华人民共和国网络安全法》，进一步健全学校网络与信息安全管理体系，落实校园网络与信息安全工作责任制，提升校园网络与信息安全整体水平，保障校园网络正常运行，制定本办法。

第二条　本办法所称网络与信息安全是指江苏开放大学（江苏城市职业学院）校园网内的网络系统和信息系统的安全，包括设备设施安全、系统运行安全和内容数据安全等。

第三条　学校网络与信息安全管理的目标是，完善网络安全技术体系和运行体系，不断提高网络安全保护能力，确保校园网络安全、稳定运行，保障学校信息化建设持续发展。

第四条　学校任何部门和个人都必须遵守《中华人民共和国网络安全法》。使用校园网络系统或信息系统的用户，应接受并配合上级主管部门、公安司法机关或学校的网络安全检查。

第五条　以“谁主管谁负责，谁运营谁负责，谁使用谁负责”为原则，落实网络与信息安全分级责任制；以国家标准《信息系统安全等级保护基本要求》为指导，综合防范、突出重点，保障学校网络与信息安全。

第二章　管理机构与职责

第六条　学校网络安全与信息化建设领导小组负责学校网络与信息安全工作，确定学校网络与信息安全工作的政策方针，审议相关规章制度，提出学校网络与信息安全工作的任务和要求，审定学校网络与信息安全工作计划，组织查处学校网络与信息安全事件。

第七条　学校网络安全与信息化建设领导小组办公室（以下简称网信办），负责学校网络与信息安全具体管理工作。主要职责如下：

（一）根据网络与信息安全实际情况，制定学校网络与信息安全工作计划；

（二）统筹协调和监督管理各部门网络与信息安全工作。审核各部门网络与信息安全管理制度，检查网络与信息安全管理制度落实情况；

（三）组织监测全校网络运行情况，评估网络安全现状，形成全校网络安全报告。负责对学校信息系统进行安全风险检测评估并落实相关改进措施；

（四）组织审核拟在校园网内实施的网络安全方案和方法，对拟部署的网络安全设备和系统的必要性和有效性加以论证；

（五）核定校园网内信息系统安全等级，审核其安全管理制度；

（六）发布有关网络与信息安全的通知、公告；

（七）组织开展经常性的全校网络与信息安全宣传教育、组织开展面向各部门网络安全管理人员的技术培训；

（八）协助公安司法机关查处各种有关网络与信息安全的违纪、违法行为。

第八条 信息化建设处负责学校主干网络和关键信息系统的安全。主要职责如下：

（一）拟订学校主干网络和关键信息系统的安全管理制度。切实落实安全管理制度，保障学校主干网络和关键信息系统的安全；

（二）加强技术人员队伍建设，不断提高防范、应对校园网络安全事件的能力；

（三）为校内其他部门提供网络与信息安全相关技术支持和协助。

第九条 各部门负责本部门的网络与信息安全工作。主要职责如下：

（一）负责本部门所属信息系统和接入网络的安全，包括设备设施安全、系统运行安全和内容数据安全；

（二）认真执行网络与信息安全管理制度，并切实加以落实；

（三）监控本部门所属信息系统的运行状态，及时发现和消除安全隐患。如发现危及全校网络安全的情形或者有害信息，须及时向网信办报告；

（四）组织开展对本部门师生员工的网络与信息安全教育。

第十条 各部门主要负责人是本部门的网络与信息安全第一责任人，对本部门的网络与信息安全负领导责任。

第十一条 各部门负责安排本部门网络安全管理员，承担本部门网络与信息安全的具体工作，并将网络安全管理员信息向网信办报备。

第十二条 各部门网络安全管理员一般应具有相关专业知识背景，在正式上岗前，须参加网络与信息安全培训，掌握网络与信息安全相关技术，了解学校网络与信息安全体系，理解网络与信息安全制度，熟悉本部门网络与信息安全措施。

第三章 网络系统安全

第十三条 学校网络系统分为学校主干网络和部门接入网络两级。

第十四条 学校主干网络由学校统筹建设和管理。信息化建设处负责学校主干网络的线路铺设与维护、设备部署与运维、流量监测与管控，保障学校主干网络的安全畅通。各校区间网络链路应当实现冗余互联，做到核心设备冗余热备。校园网络应当部署相关网络安全设备，实现对网络攻击行为的实时监测和告警，实现对恶意代码的实时检测和防护。

第十五条 校园网络系统对外采用统一出口，实现一体化管理。信息化建设处负责管控校园网络对外的统一出口，负责统一管理所有出口链路的公网 IP 地址。校园网络应该实现多出口链路，所有出口链路需接入防火墙、入侵防御系统等安全设备防护。

第十六条 校园网络系统对内实行按需接入，采取实名管理。信息化建设处负责校园网络的接入管理，接入校园网络的每一个系统和每一件设备都应具有明确的属主。根据工作需要，各部门用于教学和科研的网络可以申请接入学校主干网络。

第十七条 各部门根据工作需要建设内部网络系统。各部门内部网络系统如需接入学校主干网络，须向信息化建设处提供内部网络系统的拓扑结构、系统组成和功能应用等要素，并通过信息化建设处的综合评估，并办理相关手续。

第十八条 在建筑物设计与施工过程中，建设单位就弱电工程部分须征求信息化建设处意见，相关设计方案须经过信息化建设处审核。在建筑物施工完成后，弱电工程部分须由信息化建设处参与工程验收。

第十九条 在维修或拆除涉及校园网络的建筑物，以及维护或开挖涉及校园网络的道路时，须事先通知信息化建设处，以保护校园网络设备设施的安全。

第二十条 加强各楼宇内弱电间的管理，涉及校园网络的弱电间原则上由信息化建设处单独使用。学校自建或与校外合作单位建设的弱电管网由信息化建设处统一管理，任何部门使用弱电管网需提供设计和施工方案，并经信息化建设处审核通过后方可施工。

第二十一条 除信息化建设处外，严禁其他部门或个人以任何方式登录校园网络主干的各类设备，实施修改、设置、删除等

操作。严禁任何施工单位或个人以任何理由损毁校园网络设备设施。

第二十二条 师生员工使用校园网络，采取“实名注册、认证上网”制度。实名上网认证制度由信息化建设处负责实施。

第四章 信息系统安全

第二十三条 学校各信息系统实行安全等级保护。由网信办参照国家标准《信息系统安全等级保护基本要求》，审核确定校园网内各信息系统的安全等级。信息系统不仅包括关键信息系统和各个面向全校的重要业务系统，也包括各级各类应用业务系统，还包括各级各类网站系统。

第二十四条 关键信息系统由学校统筹建设和管理。信息化建设处负责由统一身份认证平台、网站群系统、云计算平台、网上办事大厅等构成的关键信息系统的具体建设和运营工作。

第二十五条 各部门负责所属信息系统的运营，应当按信息系统安全等级保护的要求，制定安全管理制度和操作规程，采取相应的安全保护技术措施，保障信息系统免受干扰、破坏或者未经授权的访问，防止信息系统数据泄露或者被窃取、篡改。相关安全管理制度等须经过网信办审核。

第二十六条 信息系统安全管理制度应当明确安全负责人和各项安全保护责任,应当明确各项安全保护技术措施。

第二十七条 信息系统安全保护技术措施至少包括下列项：

（一）完善系统安全配置，定期进行漏洞扫描、系统加固或

升级；

（二）开启日志审计服务，有效检测、记录系统运行状态；

（三）分类管理数据，对重要数据进行备份、加密处理；

（四）实施用户分类管理，用户账号应能标识系统访问的不同角色，应尽量避免使用系统默认账号，账号只能具有符合用户角色的最小权限；

（五）系统管理员密码应满足强度要求。

第二十八条 信息系统的注册用户应该实名认证，由信息系统的运营者负责实名认证的实施。

第二十九条 在建设阶段须充分考虑信息系统的安全防护。关键信息系统和各部门所属重要信息系统，应当具有支持业务稳定、持续运行的性能，并且安全技术措施必须同步规划、同步建设、同步使用。

第三十条 根据工作需要新建或升级在校园网内运行的信息系统，各部门应事先向网信办提出申请；同时应就信息系统设计方案向信息化建设处征求意见。在上线运行前，信息系统须通过由信息化建设处组织的安全检测，并办理相关手续。

第五章 应急处置

第三十一条 网信办按照规定通报网络与信息安全监测预警信息。各部门根据国家、地方网络安全部门发布的预警信息及时做好相应防范工作，必须按照网信办通报的预警信息，及时做好相应处置工作。

第三十二条 网信办协调信息化建设处和各部门，制定网络与信息安全事件应急预案。网络与信息安全事件应急预案按照事件发生后的危害程度、影响范围等因素对网络与信息安全事件进行分级，并规定相应的应急处置措施。

第三十三条 各部门网络安全管理人员必须熟悉本部门网络与信息安全事件应急处置措施。各部门应当定期开展网络与信息安全事件应急预案演练。

第三十四条 校园网内发生网络与信息安全事件，应当立即启动网络与信息安全事件应急预案，各部门和相关人员须按照应急预案规定进行处置。

第六章 奖 惩

第三十五条 网信办定期开展全校网络与信息安全工作的检查，每年向学校网络安全与信息化建设领导小组汇报各部门网络安全工作汇总信息。对网络与信息安全工作成绩显著的部门和个人，学校给予表彰和奖励；对违反网络与信息安全管理制度、网络与信息安全工作存在不足和隐患且逾期不改的部门，学校给予通报批评。

第三十六条 对拒不执行网络与信息安全管理相关制度、漠视网络与信息安全工作以至造成重大事故和案件的部门，学校将追究该部门主要负责人和直接责任者的责任。对触犯法律的，将移送公安司法机关处理。

第三十七条 对损坏校园网络系统或信息系统设备设施的

个人，学校将视其情节轻重追究责任，如触犯法律应移交公安司法机关处理。

第七章　附　则

第三十八条　对于涉及国家秘密的网络系统或信息系统，按照国家保密工作部门的相关规定和标准进行保护，接受学校保密委员会办公室监督指导。

第三十九条　本办法自发布之日起施行，由学校网络安全与信息化建设领导小组办公室负责解释。

江苏开放大学（江苏城市职业学院）办公室　　2022 年 5 月 8 日印发