四 川 农 业 大 学

信息与教育技术中心文件

信教发〔2022〕 6 号

四川农业大学网络安全工作人员管理细则

第一章 总则

第一条 为进一步加强四川农业大学校内网络安全工作人员和第三方机构工作人员的网络安全管理工作，明确工作人员从录用前、录用后（工作期间）、调岗、离职和离退休等各过程中的网络安全管理要求，结合《网络安全法》等相关法律法规，特制定本细则。

第二条 本细则所称人员是指网络安全相关技术人员。

第三条 本细则所称第三方人员指因从事合作开发、参与项目工程、提供技术支持或服务而涉及的软件开发商、产品供应商、系统集成商、设备维护商和安全服务商等非四川农业大学工作人员。

第二章 校级网络安全工作相关人员职责

第四条 信息与教育技术中心是学校网络安全工作的技术支撑单位，设置校级安全管理员、校级安全审计员、校级

网络管理员等岗位，与学校签订《网络安全岗位承诺书》，其中校级安全管理员为专职。各岗位职责具体如下:

(一) 校级安全管理员

(1) 组织落实网络安全和信息化领导小组安排的各项工作;

(2) 负责学校网络安全类规章制度的起草;

(3) 负责协调处置网络安全威胁预警、事件处置和应急响应工作。

(二) 校级安全审计员

(1) 负责检查、监督网络安全管理制度、安全职责落实情况;

(2) 负责对校级重要信息系统相关的日志进行审计分析;

(3) 负责组织协调校级各相关人员对审计过程中发现的相关问题落实整改;

(4) 定期汇总分析安全日志记录，形成安全审计报告。

(三) 校级网络管理员

(1) 根据校园网总体规划及安全规划，开展校园网网络架构设计;

(2) 根据校园网和信息系统的业务需求及安全要求，进行网络建设;

(3) 具体负责校园网日常运行维护。

第三章 各二级单位安全工作相关人员职责

第五条 网络安全工作应纳入各二级单位常规工作，单位党政主要负责人是本单位网络安全第一责任人，负主要领导责任；主管领导是本单位网络安全直接责任人，全面负责本单位网络安全工作。

第六条 各二级单位应根据本单位网络和信息系统建设情况，设置如下网络安全相关岗位：安全管理员、信息系统负责人、信息系统管理员、信息系统审计员、网络管理员、机房管理员等。具体各岗位职责可参考如下：

(一) 安全管理员

(1) 负责本单位网络安全技术工作，统筹协调本单位网络技术安全工作；

(2) 落实执行学校网络安全工作要求和规章制度，可根据本单位实际情况制定细化的安全管理制度；

(3) 协调本单位机房、网络、信息系统的安全建设和安全运维，负责本单位信息系统信息更新、统筹开展本单位信息系统等级保护工作；

(4) 协调本单位安全漏洞和网络安全事件的应急处置，及时反馈漏洞整改和事件处置情况；

(5) 负责配合学校相关部门组织的网络安全检查；

(6) 组织开展本单位师生员工网络安全意识教育和网络信息素养培训，并向信息与教育技术中心报备。

(二) 信息系统负责人

(1) 根据学校和本单位网络安全工作要求，组织开展所负责系统安全建设和运维;

(2) 负责本信息系统的安全等级保护定级、信息上报与更新;

(3) 负责组织落实系统立项阶段安全方案设计、建设阶段安全开发、上线阶段安全功能测试和运维阶段的安全管理方案、安全操作规程等方案和制度的制定;

(4) 负责系统的安全漏洞修复及安全风险处置，确保信息系统安全运行。

(三) 信息系统管理员

(1) 根据学校和本单位网络安全工作要求，具体落实信息系统安全建设和运维;

(2) 具体负责信息系统安全策略配置、日志记录、数据备份、数据库的管理维护等相关工作;

(3) 落实信息系统的补丁升级、安全漏洞修复、安全风险处置和安全事件应急处理;

(4) 配合开展信息系统相关安全检查、安全审计等工作。

(四) 信息系统审计员

(1) 负责信息系统的安全审计工作，对安全管理方案和安全操作规程实施内部审核，对制度的执行情况进行监督检查，并督促实施整改;

(2) 检查信息系统操作系统、中间件、应用系统、数据库等部分的安全审计功能启用情况，确认以日志的形式记录安全管理方案中规定的操作过程和操作结果工作正常;

(3) 定期完成信息系统审计工作，记录日常审计过程，详细记录可疑事件发生的现象、时间，反馈给信息系统负责人、提出处理意见和建议并监督完成问题处理;

(4) 负责信息系统审计报告的编写和审计资料归档整理。

(五) 网络管理员

(1) 根据校园网络总体规划及安全规划，开展本单位网络建设;

(2) 根据网络和信息系统业务需求及安全要求，开展本单位网络建设;

(3) 负责本单位网络日常运行维护。

(六) 机房管理员

(1) 负责对本单位机房的日常管理，落实学校机房安全管理制度;

(2) 负责机房人员、设备的进出管理;

(3) 负责机房的门禁、电源、空调等设备的日常管理以及防火、防雷、防盗等机房安全和日常维护工作;

(4) 负责对机房各类设备、UPS、消防设施、空调状态、照明等进行巡检记录，及时发现并解决问题。

第七条 网络安全岗位工作人员应签订安全承诺书，并严格履行承诺书中的要求。具体包括：单位党政负责人作为网络安全工作第一责任人应与四川农业大学签订《四川农业大学二级单位网络安全承诺书》；参与信息系统安全相关建设、运维、管理等工作的关键岗位人员，应与本单位签订《网络安全岗位承诺书》；信息系统负责人及信息系统管理员应向信息与教育技术中心提交《信息系统安全承诺书》。

第四章 安全工作人员聘用管理

第八条 人员聘用管理是指学校各二级单位在聘用网络安全相关工作岗位员工前的安全管理要求，主要包括明确安全职责、审核人员信息和签署网络安全承诺书。

第九条 聘用单位应对被聘用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。

第十条 所有安全相关工作岗位员工均需签署《网络安全岗位承诺书》。

第五章 人员转岗和离岗

第十一条 各二级单位应及时终止离岗人员所涉及网络或信息系统的访问权限，变更转岗人员的访问权限。

第十二条 对离岗人员，各二级单位要理清离职交接单的各项交接内容，收回岗位相关身份证件、钥匙、徽章以及为其提供的软硬件设备等，对设备上保留的数据进行安全处理，包括备份需要留 存的数据以及删除不必要的数据。根据

身份变化，调整学校相关信息系统中的人员身份属性和访问权限。

第十三条 各二级单位应注意转岗人员的岗位变化，根据岗位需要，重新签署保密协议。

第六章 网络安全教育和培训

第十四条 学校统筹开展校级网络安全教育和培训，每年根据上级部门要求和工作需要，制定下一年度网络安全教育和培训计划，并落实相关经费。

第十五条 各二级单位应按信息与教育技术中心要求制定本单位网络安全年度培训计划，并及时向信息与教育技术中心报备。

第十六条 新员工在正式上岗前，应由所在二级单位安全管理员组织开展网络安全培训，明确岗位所要求遵守的网络安全管理制度、技术规范以及操作流程。

第十七条 各单位网络安全相关人员应定期参加网络安全培训(每年至少一次),培训内容包括但不限于学校统筹安排的安全培训和校内外其他培训。其中，工作人员参加非学校统筹安排的网络安全培训应向信息与教育技术中心报备培训记录。

第七章 第三方人员管理

第十八条 第三方人员是指因从事合作开发、参与项目工程、提供技术支持或服务而涉及的软件开发商、产品供应

商、系统集成商、设备维护商和安全服务商等非四川农业大学人员。

第十九条 第三方人员现场操作或访问设备需提出申请，填写附件五《第三方人员访问申请表》，申请应明确访问区域、设备或系统的详细信息，需要本单位安全管理员或相关工作负责人审批授权后才能正式访问。

第二十条 第三方人员所在单位应与各二级单位签署第三方保密协议，承诺本单位工作人员对所接触的四川农业大学人员、设备、系统、文档、数据等承担协议约定的保密义务。

第二十一条 第三方人员现场操作或访问设备，安全管理员或相关工作负责人应安排人员全程陪同，应告知有关安全管理规定，不应透露与工作无关的信息，不得任其进行与工作无关的操作。接入重要网络设备和服务器应记录第三方人员操作，事后可追溯。

第二十二条 原则上不允许第三方人员进行远程运维。如因工作需要必须远程运维，须经安全管理员或相关工作负责人审批，在访问结束后应及时关闭访问通道。

第二十三条 应防范第三方人员带来的以下安全风险:

（一）第三方人员物理访问所造成的设备、资料失窃;

（二）第三方人员误操作所导致各种软硬件故障;

（三）第三方人员资料、信息外传所导致的泄密;

（四）第三方人员对计算机系统的滥用和越权访问;

（五）第三方人员给计算机系统、软件留下后门。

第二十四条 未经安全管理员或相关工作负责人同意，禁止第三方人员私自将移动存储介质接入信息系统，移动存储介质必须在接待人的监控下使用。

第二十五条 未经安全管理员或相关工作负责人同意，第三方人员不得在机房内拍照。

第八章 奖惩

第二十六条 学校定期对在网络安全工作中的先进集体和先进个人，给予表扬和奖励；对违章的集体和个人，给予纪律处分。

第二十七条 符合下列条件之一的集体和个人，进行通报表扬并给予奖励:

（一）在网络安全检查、检测手段和方法方面有创新;

（二） 及时发现或者有效消除信息系统重大缺陷和安全隐患;

（三）在紧急情况下保护信息系统安全免遭损失;

（四）在网络安全工作的其他方面做出显著成绩。

第二十八条 有下列情形之一的集体和个人，根据其造成的损害程度，给予必要的批评教育、通报批评、行政处分等处罚。对于违反校规校纪的组织何个人，根据学校规定予以处分。构成犯罪的，依法交由相关国家机关，依法追究刑

事责任:

（一）入侵信息系统;

（二）非法删除、修改、增加、干扰信息系统的功能、数据、程序，造成严重后果;

（三）泄露本单位信息系统安全防护技术、方法、措施、安全产品性能、效果和应用范围，造成后果;

（四）使用已经禁用或者不符合规定的信息系统、安全产品，造成严重安全隐患;

（五）其他危害信息系统安全。

第九章 附 则

第二十九条 本细则自发布之日起施行，由信息与教育技术中心负责解释和修订。

信息与教育技术中心

2022年4月22日