防灾科技学院信息化管理中心

信息中心〔2021〕21 号

关于印发《防灾科技学院网络安全管理组织机构及职责》的通知

学校各部门、各单位：

为规范学院的网络安全工作，使全体工作人员理解网络安全工作要求，并落实到实际工作中，推动网络安全保障工作的顺利进行，结合学院的实际情况，建立健全网络安全机构职责。特制定《防灾科技学院网络安全管理组织机构及职责》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 12 月 9 日

防灾科技学院网络安全管理组织机构及职责

第一章　总则

第一条　为规范学院的网络安全工作，使全体工作人员理解网络安全工作要求，并落实到实际工作中，推动网络安全保障工作的顺利进行，结合学院的实际情况，建立健全网络安全机构职责，特制定本制度。

第二章　网络安全组织机构

第二条　学院网络安全组织机构由网络安全和信息化领导小组（简称“网络安全领导小组”)和网络安全和信息化领导小组办公室(简称“网络安全办公室”）共同构建。

第三条　网络安全组织的领导层由网络安全领导小组承担，是本单位网络安全管理体系管理机构。网络安全领导小组由学院领导牵头各部门领导组成。小组成员包括：

第四条　组长：学校主要负责人

第五条　副组长：分管办公室校领导

第六条　成员：办公室、党委办公室、党委宣传部(党委统战部)、信息化管理中心、发展与财务处、教务处(学位办公室)、党委学生工作部(学生工作处、学生资助管理中心)、学科与研究生处、团委（大学生艺术活动指导中心)、党委安全工作部（安全工作处)、人事处、资产管理处、基建处、图书馆（档案馆)、高等教育研究所（《防灾科技学院学报》编辑部)、信息工程学院等部门负责人。

第七条 网络安全办公室设在办公室，作为网络安全工作的管理层，负责具体落实领导层决策及日常的安全管理等工作，办公室主任兼任领导小组办公室主任，党委宣传部(党委统战部)、信息化管理中心主要负责人兼任领导小组办公室副主任。由办公室领导担任主任。

第八条 网络安全工作的执行层由信息化管理中心担任，负责技术支撑，负责提供信息系统日常运行维护技术管理工作。

第九条 信息化管理中心应设立安全管理各个方面的负责人岗位，包括安全管理员、安全审计员、系统管理员、网络管理员、数据库管理员、机房管理员等，负责执行系统、网络、数据库和机房的安全管理和运维工作。

第三章 网络安全组织职责

第十条 网络安全领导小组负责领导信息系统安全工作，组织职责如下：

1. 根据国家和行业有关网络安全的政策、法律和法规，确定网络安全工作的总体方向、总体原则和安全工作方法；

2. 根据国家和行业有关网络安全的政策、法律和法规，批准信息系统的安全策略和发展规划；

3. 确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施；

4. 监督安全措施的执行，并对重要安全事件的处理进行决策；

5. 负责跨单位的重大网络安全工作的协调和沟通；

6. 负责网络安全规划和建设的资源保障。

7. 负责对网络安全办公室提交的网络安全保护管理制度进行审核和审批。

第十一条 网络安全办公室负责本单位网络安全管理工作，具体工作职责包括：

1. 负责就信息化和网络安全等重大问题进行调研并向网络安全领导小组提出政策建议；

2. 协调落实并督促检查网络安全领导小组有关决议的执行；

3. 组织起草单位信息化发展战略、总体规划、工作计划及其信息化相关的各类规章制度；

4. 组织审核各部门的信息发展规划，组织协调重大信息化建设项目的立项、论证和验收评估并对项目实施过程进行监督；

5. 参与信息化相关的教育和培训、国内国际合作和交流；

6. 管理监督本单位网络与网络安全，对本单位网络舆情进行监管和通报；

7. 完成网络安全领导小组交代的其他任务。

8. 负责对信息化管理中心提交的网络安全事项进行审批。

第十二条 信息化管理中心负责网络安全的实施工作，具体职责如下：

1. 负责对安全管理活动中的各类管理内容建立安全管理制度，并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；

2. 负责网络安全等级保护相关工作的具体实施，落实网络安全保障工作的各项具体措施，包括安全管理和技术措施；

3. 负责执行网络安全相关技术规范、技术标准和网络安全规章制度；

4. 完成网络安全办公室交办的其他任务。

5. 负责对管理员提交的网络安全工作事项进行审批。

第四章　网络安全岗位职责

第十三条　网络安全主管的岗位职责如下：

1. 组织资源制订本单位网络安全管理制度和技术规范。

2. 领导、组织本单位网络安全管理制度和技术规范的具体实施。

3. 监督、检查本单位网络安全管理工作的落实情况。

4. 定期就网络安全管理的效果和有关重大问题及时向网络安全办公室汇报。

第十四条　安全管理员的岗位职责如下：

1. 负责协助主管安全的领导开展网络安全相关工作；

2. 负责组织实施本单位的网络安全教育和培训；

3. 负责指导协调本单位的网络安全工作，督促开展网络安全工作；

4. 负责网络安全事件的及时上报，并协助相关单位做好安全事件的调查、响应和处理；

5. 负责配合实施内部或外部组织的网络安全检查；

6. 协调网络安全应急响应组织和技术支撑单位；

7. 负责制定信息系统总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况；

8. 对网络、系统、应用、数据库管理员进行安全指导；

9. 定期收集网络安全漏洞和公告信息，告知相关安全运维管理人员。

第十五条 安全审计员的岗位职责如下：

1. 负责依据相关要求制定网络安全检查计划，实施各类网络安全检查；

2. 负责针对检查过程发现的问题，督促责任单位进行整改并验证整改结果；

3. 负责对各类网络安全事件进行独立审核，确保符合网络安全体系方针与策略要求；

4. 定期审计信息系统网络安全策略执行情况，收集信息系统日志和审计记录，并提供审计报告；

5. 对安全、网络、系统、应用、数据库管理员的操作行为进行监督，安全职责落实情况进行检查。

第十六条 系统管理员的安全职责如下：

1. 根据信息系统安全策略定期对系统进行自评估；

2. 依照安全策略对系统进行安全配置和漏洞修补，确保安全补丁保持2个月内最新补丁；

3. 对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告；

4. 在发生系统异常和安全事件时，应能对系统进行应急处置。

第十七条 网络管理员的安全职责如下：

1. 根据信息系统安全策略定期对网络设备、网络架构进行自评估；

2. 依照安全策略对网络设备进行安全配置和漏洞修补；

3. 对网络设备、安全设备进行日常安全运维管理，并定期提交安全运行维护记录或报告；

4. 在发生系统异常和安全事件时，应能对网络设备、安全设备进行应急处置。

第十八条 数据库管理员职责：

1. 负责数据存储与备份管理；

2. 负责 SQL Server 等数据库的管理与维护。

第十九条 机房管理员职责：

1. 负责对机房的日常管理；

2. 负责对机房环境、网络及各系统运行情况进行监控，及时发现并解决问题；

3. 负责机房人员、设备的出入登记管理；

4. 负责组织协调火警、水浸、设备故障等突发事件的分析与处理，跟踪事件处理全过程；

5. 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、防盗等机房安全工作；

6. 负责维护机房卫生环境；

7. 负责落实与机房管理相关的网络安全管理制度。

第五章 网络安全岗位要求

第二十条 信息化管理中心应设立专职的网络安全管理岗位，并由专人负责。

第二十一条 系统管理员、安全审计员和数据库管理员等关键岗位需要配备多人，关键岗位人员配备坚持“权限分散、不得交叉覆盖、最小权限”的原则，安全管理员不可兼任其他管理员。

第二十二条 信息化管理中心根据岗位职责，确定岗位所需要的安全技能，并对所有网络安全岗位人员进行对应的安全技能培训。

第二十三条 网络安全管理、系统安全管理、数据库安全管理以及应用安全管理工作可分别由网络管理员、系统管理员、数据库管理员以及应用管理员执行。

第二十四条 重要业务系统操作人员应在日常工作中认真执行信息系统安全策略和技术安全规范中的各项要求。

第六章 沟通与合作

第二十五条 网络安全领导小组应定期召开例会，指导网络安全策略和制度的实施，解决网络安全工作中的问题，协调单位间、部门间网络安全工作的开展，对实施过程中的问题进行探讨解决。

第二十六条 网络安全管理工作应采取多种沟通方式，有效保障相关工作的落实。主要采取如下协商机制：

1. 会议沟通。对网络安全管理工作中出现的问题进行专题探讨与协商。各种会议须做好会议记录，包括召开时间、地点、参会部门和人员以及会议主题、内容和结果等。

2. 即时沟通。对网络安全管理工作中出现的需要快速响应和决策的事件，通过电话、邮件和即时通讯工具等方式进行非敏感信息的沟通交流；

3. 内部通报。对网络安全管理工作中的成效、经验、问题等内容进行通报，以加强和改进相关网络安全管理工作。

4. 外联沟通。制定有关外联单位联系表（见外联单位联系表），在遇到各种问题的情况下，可以快速联络到相关外联单位有关负责人。联系表需要定期更新，报信息全职能部门备案。

5. 专家咨询。建立外部专家联系名单（见外部专家联系名单）。遇到棘手问题时，可以请相关专家进行协助处理。

6. 外部通报。按照相关部门有关规定，网络安全责任人必须与主管部门或上级部门保持适当的联系，以便及时获取主管部门的政策指导信息，并及时上报各单位的网络安全情况。

第七章　网络安全审核和检查

第二十七条　信息化管理中心根据有关单位要求和相关管理制度，按需组织网络安全管理工作的审核和检查。

第二十八条　各网络安全管理岗位人员根据自身职责配合网络安全管理工作的审核和检查，并对检查过程和结果详实记录。根据检查内容需要填报相关文档(详见安全检查记录单，终端设备情况汇总表)。

第二十九条　相关检查结果由信息化管理中心整理后，经网络安全办公室审核后，报网络安全领导小组。

第三十条　对于检查中发现的问题，由信息化管理中心进行复查。须明确复查的期限和责任。

第三十一条　安全检查包括系统建设和运维部的自查和信息安全工作小组定期执行的安全检查。

第三十二条 信息化管理中心的自查内容应包括业务系统日常运行、系统漏洞和数据备份等情况，自查工作应保留自查结果。自查应至少一个季度组织一次。

第三十三条 信息安全工作小组执行的安全检查内容应包括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、安全管理制度的执行情况和各部门自查结果抽查等。安全检查应至少一年组织一次。

第三十四条 自查和安全检查均应在检查之前形成检查表。

第三十五条 应严格按照检查表实施检查，检查完毕，记录下所有检查结果。

第三十六条 系统建设和运维部应阅读并理解安全检查报告，在信息安全工作小组的指导下对出现的问题进行整改。

第八章 附则

第三十七条 本规定的解释权归网络安全办公室。

第三十八条 本规定自发布之日起施行。

安全检查记录单

单位：　　日期：　年　月　日

审核检查部门					
检查人员					
分管责任人					
序号	检查系统名称	日常运行情况	系统漏洞情况	数据备份情况	确认签字
		□正常 □异常	□无 □有	□正常 □异常	
		□正常 □异常	□无 □有	□正常 □异常	
		□正常 □异常	□无 □有	□正常 □异常	
		□正常 □异常	□无 □有	□正常 □异常	
		□正常 □异常	□无 □有	□正常 □异常	

终端设备情况汇总表

序号	设备类型	品牌型号	使用的操作系统及字处理等软件	资产编号	资产所属单位	房间号	使用人	部署网络	密级
1	台式机							□互联网 □内网	□秘密 □机密 □绝密
2	笔记本								

外联单位联系表

序号	单位名称	合作内容	联系人	联系方式
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

备注：外联单位指各类供应商、业界专家及安全组织等。

外部专家联系名单

序号	姓名	性别	单位名称	职务/职称	联系方式	合作内容
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

防灾科技学院信息化管理中心　　2021年12月9日印发