防灾科技学院信息化管理中心

信息中心〔2021〕11 号

关于印发《防灾科技学院信息安全审核和检查管理规定》的通知

学校各部门、各单位：

为规范学校安全检查制度，确保现有安全技术及管理措施的有效性、安全配置与安全策略的一致性、落实安全管理制度的执行情况，特制定《防灾科技学院信息安全审核和检查管理规定》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院信息安全审核和检查管理规定

第一章　总则

第一条　为规范防灾科技学院（以下简称“学院”）安全检查制度，确保现有安全技术及管理措施的有效性、安全配置与安全策略的一致性、落实安全管理制度的执行情况，特制定本规定。

第二条　学院各单位应依照本制度要求执行及配合安全检查工作。

第二章　检查内容和依据

第三条　除外部机构信息安全检查外，学院信息化管理中心依据信息安全管理体系标准要求，结合学院信息安全现状以及内部管理制度中有关信息安全管理的内容，确定学院内部信息安全检查内容。

第四条　学院内部信息安全检查内容应重点关注信息安全检查工作的全面性，应与外部组织的各类信息安全检查侧重点有所不同，以期形成互补，实现对学院信息安全状况的全面了解。内部信息安全检查内容应重点包括组织机构建设与管理体系、规章制度的贯彻执行和监督检查、系统网络安全管理、应用系统开发的安全管理、桌面办公系统的使用和安全管理、运行环境管理、运行值班及技术维护管理、运行安全控制管理以及项目实施安全控制管理等内容。

第三章　检查的方式和周期

第五条 学院内部信息安全检查采取“定期自查与不定期抽查相结合”的方式。定期自查是各部门和服务项目基于本规定的要求周期性地执行信息安全检查，不定期抽查是指由信息化管理中心组织的针对各部门和服务项目的不定期的信息安全检查。

第六条 自查：信息化管理中心负责牵头指导各部门制定“信息安全自查表”，由各部门和组织实施信息安全自查。检查人员将信息安全自查结果提交给信息化管理中心。

第七条 抽查：信息化管理中心原则上半年进行一次抽查，抽查以部门或服务项目为单位。被抽查的部门或服务项目人员应对检查工作给予积极配合。

第八条 外部驱动的信息安全检查：由信息化管理中心负责组织力量接待由外部驱动的信息安全检查，包括公安部等政府相关部门要求的等级保护相关信息安全检查与审计等。各部门需要在信息化管理中心的组织下，由各部门负责人统一协调本部门资源，密切配合外部检查机构完成相关信息安全检查工作。

第九条 信息安全管理体系审查：针对信息安全管理体系本身运行情况，学院每年需要开展针对信息安全管理体系的内部审计工作，该审核的重点是建立的信息安全管理体系的符合性。

第四章 信息安全检查工具及管理

第十条 在确定信息安全检查指标时，以信息安全检查提纲为主要依据，同时可以根据每次检查的性质，参考相关信息安全技术和管理指标，确定本次信息安全检查指标内容。

第十一条 可采取合适的信息安全检查、评估工具对信息系统进行检查，确保信息安全检查的有效性和完整性。信息安全检查工具的采购、实施应符合学院相关采购管理要求，并根据评估工具本身的安全性。

第十二条 内部信息安全检查需获得信息安全管理组的授权，外部信息安全检查需获得信息安全管理者代表的授权，且检查过程中不得违反学院的相关信息安全管理规定要求，尤其是使用信息安全检查、评估工具对信息系统进行评估时，更应遵循对业务影响最小化的原则，严格控制可能带来高风险的信息安全检查方式。对于在线业务系统的评估检查时间应尽量避开业务高峰时期。

第十三条 对于外部组织的各种信息安全检查，最终的检查结果和报告，执总办应妥善保留副本，并确定密级。

第五章 信息安全检查的工作流程

第十四条 针对内部驱动的信息安全自查，由自查人员进行记录检查的结果，填写“信息安全自查表”。

第十五条 针对内部驱动的信息安全抽查，由信息化管理中心负责组织进行信息安全抽查，检查人员进行现场评分并记录检查发现结果。

第十六条 针对内部驱动的信息安全检查，信息安全检查人员与被检查部门确认后，由信息化管理中心向信息安全管理组告知安全检查结果。

第十七条 对于外部驱动的信息安全检查，由信息化管理中心进行记录检查的结果，结合检查方出具的“审核不符合项报告”（如有）向信息安全管理者代表提交检查结果。

第六章 检查的跟踪改进

第十八条 针对内部驱动的信息安全检查结果，被检查部门应对信息安全检查中发现的问题制定“审核问题整改计划”并进行整改，将整改计划和整改结果反馈给信息化管理中心。信息化管理中心应在下次安全检查中针对整改结果进行跟踪。

第十九条 针对外部驱动的信息安全检查结果，信息安全管理委员会督促各部门制定整改计划并执行，将整改结果反馈给外部检查单位。

第七章 附则

第二十条 本规定由信息化管理中心负责解释。

第二十一条 本规定自颁布之日起施行。

附表 1

信息安全自查表														
受检查部门：			检查人：				检查日期：			检查策略：符合情况的，在各项名称下打″√″				
使用人	计算机名称	计算机用途	计算机 IP	防病毒软件名称	病毒库日期	启用防火墙	操作系统补丁日期	屏保设置	密码复杂度	操作系统帐户列表	办公软件安装列表	工作文档目录不存放于系统分区	关闭 U 盘自动运行	备注

防灾科技学院信息化管理中心　　2021 年 10 月 7 日印发