

山东传媒职业学院 网络和信息安全管理办法（试行）

第一章 总 则

第一条 为加强学院网络和信息安全管理，提高网络和信息安全防护能力和水平，保障学院信息化健康发展，根据《中华人民共和国网络安全法》《计算机信息网络国际联网安全保护管理办法》《教育部关于加强教育行业与网络信息安全工作的指导意见》等相关法律法规，结合学院实际，制定本办法。

第二条 依据“谁建设谁负责，谁使用谁负责”的原则，逐级落实网络和信息安全责任，达到明确责任、突出重点、自主防护、保障安全的目标。

第三条 任何部门及个人不得利用学院网络和信息系统泄露国家或学院秘密，危害国家或学院安全，不得侵犯国家、集体和他人的合法权益，不得从事违法犯罪活动。

第二章 适用范围

第四条 为满足教学、科研、办公、管理、后勤服务及生活保障的需要，在校园内建设、运营、维护和使用的计算机网络、物联网、信息系统及相关的信息化基础设施；以学院名义，在互联网上建设、运营、维护和使用的网站及信息系统；以及与以上内容有关的网络和信息安全的监督管理。

第三章 机构与职责

第五条 网络安全和信息化领导小组负责制定网络和信息安全相关政策，研究处理重大网络和信息安全事件，定期召开网络和信息安全会议，统筹指导学院网络和信息安全建设。

第六条 信息网络中心是学院网络和信息安全归口管理部门，负责统筹学院网络和信息安全建设工作。具体职责包括：

- （一）制定网络和信息安全总体规划，并组织实施；
- （二）拟定网络和信息安全管理规章制度，制定信息安全标准规范；
- （三）组织开展信息系统安全等级保护工作；
- （四）负责网络安全应急管理，协调处理与政府信息安全管理部門的关系；
- （五）负责学院信息技术安全防护体系的建设、运行维护、技术指导和服務支持；
- （六）组织信息宣传和教育培训工作；
- （七）负责信息安全监督检查工作；
- （八）学院网络和信息安全的其他工作。

第七条 学院各部门是本部門网络和信息安全工作的责任主体，各部门主要负责人是本单位网络和信息安全工作第一责任人，负责按本办法落实网络和信息安全工作。同时，各部门设置网络和信息安全联络员，负责本部門网络和信息安全具体工作。

第四章 管理规定

第八条 安装网络版杀毒软件，通过部署防病毒策略，对局域网进行全面的病毒防护，加强网络的內网行为管理与网络流量

的控制功能，有效地规范各工作站的上网行为，将病毒隐患降到最低限度。安装防火墙，实现数据流的监控、过滤、记录和报告功能，较好地隔断内部网络与外部网络的连接。

第九条 接入公用数据网的计算机严禁访问非法、淫秽和反动的网站，要确保网络不受外来攻击，防止内部信息的泄露。实施公用数据网接入的计算机必须安装常驻内存的病毒检测软件，并在浏览软件内设置程序下载前的自动警告提示。

第十条 严禁在网上下载、安装软件。以防黑客攻击；如确需下载、安装，必须事先征得网络安全和信息化工作领导小组的同意后，方可从可靠网站以存盘方式将下载软件存放在独立的区域，并对其实施病毒检测，确认安全后，方可安装使用。

第十一条 师生向公用数据网站上发布信息须严格执行信息发布审核制度，逐级审核后方可对外发布，确保信息的准确无误及网络的严肃性，安全性。

第十二条 计算机网络使用人员对工作必须具有高度的责任感，严守保密制度。

第十三条 各部门做好数据的备份工作，预防数据丢失，确保数据完整准确，网络中的共享文件要设定共享密码，只能开放只读权限，以免泄露重要资料。

第十四条 非网络使用人员或与工作无关者，未经批准不得擅自使用网络计算机。凡未经检验的计算机不得并网使用，否则，由此造成的损失由使用者承担，凡未经检测的软磁盘、光盘，严禁在联网计算机上使用。

第十五条 严禁随意更改计算机的 IP 地址及有关网络安全设置。严禁随意搬移、调换、拆装网络计算机或计算机外围设备，确保计算机网络处于良好的工作状态，使用者需保持计算机周围环境卫生清洁，切实做好防盗、防雷、防火、防潮、防尘等工作。

第十六条 校园网络包括校园有线网络和无线网络，涉及光缆、网络机房（含数据中心、汇聚机房、接入机房等）、网络设备、网址域名、IP 地址管理、认证计费、安全防护、网络接入与运维等，由信息网络中心负责建设和运行维护。

第十七条 师生员工登录校园网，实行“实名注册、认证上网”的制度。未经允许，任何部门和个人不得利用校园网及网络设施开展经营活动。

第十八条 各部门要按照国家信息系统安全等级保护制度的相关法律法规、标准规范和要求落实信息系统安全等级保护制度。

第十九条 各业务主管部门为相应业务信息系统（含移动客户端软件）的责任部门，应指定专门人员负责系统的建设、运行维护 and 安全管理，制定信息系统运维和安全管理方案。信息系统原则上由业务主管部门运维，特殊情况可委托信息网络中心运维。

第二十条 各业务信息系统经试运行后，由业务主管部门组织初步验收，出具初步验收报告，并开展信息系统安全保护等级测评，未进行信息系统安全保护等级测评或测评不合格的业务信息系统不得进行竣工验收。

第二十一条 各部门要保留不少于 6 个月的系统维护日志。各部门管理员和个人要妥善保管好账号和密码，采用强密码策略，

定期更新密码，防止密码外泄。

第二十二条 信息系统在立项、建设、上线、运行等阶段应根据学校信息化建设和网络安全管理有关规定同步落实网络安全要求。

第五章 监测预警与应急处置

第二十三条 信息网络中心牵头学院信息系统安全等级保护相关工作，按照信息系统安全等级保护有关制度要求，统筹推进学院各级应用系统和互联网站的信息系统安全等级保护相关工作。

第二十四条 信息网络中心定期组织开展对各部门的信息系统、网站安全状况、安全保护制度及措施的落实情况的检查，并配合上级有关部门开展相关工作。

第二十五条 各部门须按照网络和信息安全事件报告与处置流程的有关规定，做好应急事件处置工作。

第二十六条 各部门须按照安全事件早发现、早报告、早控制、早解决的要求建立本部门信息安全值守制度，制定安全事件应急预案和处置方案，组织应急演练。

第二十七条 信息网络中心牵头联合相关部门对全校各部门网络与信息技术安全工作落实情况进行检查，对安全隐患做出预警，对发现的问题下达限期整改通知书，对网络和信息安全事件进行调查处理。

第二十八条 信息网络中心负责定期组织开展各部门网络和信息安全联络员专业培训。

第六章 附 则

第二十九条 本办法自发布之日起施行，由信息网络中心负责解释。

院内发送：学院领导，院属各部门

山东传媒职业学院办公室

2023 年 12 月 15 日印发

共印 39 份