上海建设管理职业技术学院

沪建管职院〔2023〕124号

关于印发《上海建设管理职业技术学院校园网络安全管理办法（试行）》的通知

各部门、中心，各二级学院（部）：

经党委会、院长办公会审议通过，现将《上海建设管理职业技术学院校园网络安全管理办法（试行）》印发给你们，请认真学习，贯彻执行。

上海建设管理职业技术学院

2023年8月10日

上海建设管理职业技术学院校园网络安全管理办法（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》，加强学院网络安全管理，完善网络安全工作机制，提高网络安全防护能力和水平，创建良好的校园网络环境，根据相关法律法规和文件精神，结合学院实际，特制定本办法。

第二条 学院各部门或个人以学院或学院部门、组织、团体名义建设、运营、维护和使用校园网络和信息化基础设施、电子显示屏、应用系统（含教学资源）、网络、论坛、互联网新媒体等网络信息平台，以及学院网络安全的监督管理，适用本办法。

第三条 按照“谁主管、谁负责，谁使用、谁负责，谁运维、谁负责”的基本原则，学院各部门、全体师生员工应依照本办法要求及相关标准规范履行网络与信息安全的义务和责任。

第二章 网络安全责任体系与职责

第四条 学院网络安全与信息化领导小组负责统一领导、统一谋划、统一部署全校网络安全工作，统筹制定网络安全发展战略、宏观规划和重大决策，研究解决网络安全重要问题；学院党政主要负责人是学院网络安全第一责任人；分管院领导是学院网

络安全直接领导责任人。

第五条 学院网络安全管理执行机构由宣传处、图文信息中心和安全保卫处组成,负责学院网络安全的专业化和常态化管理。

（一）宣传处负责全院网络意识形态管理；指导、协调、督促各部门加强网络信息内容管理；监督、监测和处理违法违规及不良网络信息内容；监控、收集、疏导学院网络舆情。

（二）图文信息中心负责统筹协调网络安全工作和相关指导、监督管理工作，制定学院网络安全管理制度和规程；负责学院网络安全技术防护体系的建设、运行维护、技术指导和服务支持。

（三）安全保卫处负责协调全院网络安全事件的侦测查处;与公安机关的沟通、联系；一旦发生网络安全事件，按照学院流程上报公安机关等主管单位。

第六条 学院各部门是本部门网络安全和信息化工作的责任主体；二级学院党政负责人是本学院网络安全的第一责任人；各职能部门或教辅单位主要负责人是本单位网络安全工作的第一责任人;各部门分管负责人是本单位网络安全工作直接领导责任人;各部门网络安全管理人员是本单位信息系统（网络新媒体）安全的直接责任人。

第七条 校园网用户作为校园网的使用者、学院信息化建设的参与者，同样也是网络安全的参与者，须遵守学院网络安全的相关规定，积极参与网络安全的建设和管理。

第三章 校园网络基础设施安全

第八条 校园网络与互联网及其他公共信息网络实行逻辑隔离，统一出口、统一管理和统一防护。

学院各部门未经学院允许不得擅自将校园网络与校外网络或互联网建立专线连接;不得在校园内擅自铺设管线或通讯设备。

任何单位和个人未经学院允许不得利用校园网络及设施开展经营性活动。

第九条 学院各部门和个人有义务保护校园网络基础设施，不得损坏或擅自改动，发现校园网络基础设施的破坏行为或事件应及时通知图文信息中心。

各部门楼宇进行修缮、改扩建、重建，校内道路施工等，涉及网络基础设施、地下通讯管线的，工程主管部门和施工单位应提前通知图文信息中心，并在施工过程中采取必要的保护措施。

第十条 弱电间是学院各楼宇楼层弱点系统布线的集中汇聚场所，非管理人员未经许可或授权不得进入弱电间、操作弱电间内设备。强电线路等与弱电无关的业务不得使用弱点管网，禁止将弱电间内的电源引出挪作它用。各部门需要使用弱点管网设施的，须经图文信息中心审批，校外单位还须签订相关协议，并服从学院管理。

第十一条 外部网络线缆进入校园，须经后勤保障处、图文信息中心审批，并提供管线图纸，按国家相关专业标准和学院相关规定进行施工，不影响校园环境及学院原有的网络系统，接受学

院相关管理部门监督管理。

第十二条 校园无线网络是有线网络的补充和延伸。未经学院许可，任何单位或个人不得擅自在校内建设无线网络或提供无线网络服务，也不得擅自同意校外无线网络服务提供商在校园内从事无线网络安装、经营业务。

第四章 校园网络运行安全

第十三条 学院注册域名为 shjgzy.cn，学院内各部门建设信息系统须按相关规定向图文信息中心申请使用学院二级以下各级域名。

第十四条 校园网络 IP 地址由图文信息中心负责统一管理和分配。入网单位和个人应履行审批手续并使用分配的 IP 地址接入校园网，禁止挪用他人 IP 地址或私自设置 IP 地址。

第十五条 校园网络应落实访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等网络边界防护措施，合理划分安全区域，确保有防护、有数据、有痕迹。

第十六条 校园网络按照国家网络安全管理规定，记录并妥善保管用户个人信息和上网日志信息，不得泄露、篡改、毁损，未经许可不得提供给第三方。根据法律有关规定，或者行政、司法机构要求提供的除外。

第五章 校园网用户安全管理

第十七条 学院师生员工接入校园网络，实行“实名制注册、认证上网”制度。用户须办理入网手续并签署信息安全承诺书，对所管理的账号、密码保密，并按要求规范管理，不得共用账号，自觉约束、规范自身网络行为。如出现出借账号、他人盗用账号造成的违法后果的，账号所有者负有管理责任。

短期来访人员上网手续由接待部门负责核实后申请办理；学生入网在新生入学时统一办理。

学院各部门应加强人员离岗、离职管理，及时终止相关人员的网络或系统访问权限，回收学院提供的软硬件信息设备和相关账号权限。

第十八条 校园网用户应文明上网，规范网络行为，做好个人网络信息安全维护，并对自己向网络所提供的信息负责。校园网用户的上网行为不得危害学院网络信息安全，不得利用校园从事任何未经授权的探测、破坏、信息窃取等互联网攻击活动。不得利用计算机从事非法和违规活动，不得制作、查阅、复制和传播不良、不实信息。

校园网用户有义务向学院和有关部门举报网络违法犯罪行为和有害信息侵入情况，接受并配合学院及国家有关部门依法进行的监督检查。

第六章 信息系统建设及安全管理

第十九条 信息系统实行等级备案制度，备案信息包括但不

限于信息系统名称、主办/主管单位、责任人、技术管理员、服务器存放信息、数据库类型、开发商、域名、IP 地址、开放端口、运行有效期等。信息系统主管部门应在信息系统立项时向图文信息中心登记备案，并在建设、运维的过程中及时更新备案信息。

第二十条 各部门新建信息系统应当按照网络安全等级保护制度的要求实施等保定级、测评、备案、整改等工作。原则上提供互联网访问的信息系统及重点业务管理系统定级应不低于二级。系统主管部门应在系统规划、建设、运维中同步规划安全等级保护相关内容。图文信息中心做好网络安全等级保护相关的组织、指导工作。

第二十一条 信息系统要实施全生命周期安全管控，从系统规划设计阶段同步介入，融入网络安全内容，同步建设，同步实施。

（一）立项论证阶段：要有网络安全专项论证，明确系统使用范围，确定网络安全保护等级，预留网络安全预算和资源。论证须由网信办出具网络安全意见。

（二）采购阶段：项目采购需求文件应由网络安全专门章节，满足网信办提出的网络安全技术要求、运维服务要求、应急响应和处置要求、信息保密要求等。

（三）验收阶段：建设单位应向网信办提出网络安全专项验收申请，根据有关规定和合同要求，提交相关网络安全测评报告。图文信息中心组织对系统进行软件测评，测评通过后方可校内上

线试运行。

（四）运行阶段：信息系统主管部门应为系统配备专业技术维护服务，负责信息系统的安全配置、软件更新、数据备份、日志记录、防病毒、防攻击、安全检查、安全隐患整改、安全事件应急与处置等，严格落实和执行学院关于网络安全管理的各项制度。

（五）终结阶段：废弃网络或信息系统须妥善处置，信息系统主管部门应终结系统运行，回收网络资源并及时到图文信息中心或通信管理部门办理注销手续。

第二十二条 学院内各部门原则上不再单独购买服务器和建设服务器机房，计算和存储需求应申请使用学院统一提供的云服务资源，并遵守学院云平台使用规定。如确有单独采购服务器需求，须在采购项目立项阶段提出，经专家论证通过后进行采购。服务器提供服务前，须按相关规定申请使用校园 IP 地址和学院二级域名，并做好安全防护工作。

第二十三条 信息系统校内上线前应指定网络安全管理员，明确网络安全维护模式和维护单位，并通过图文信息中心的安全检测，系统主管单位网络安全工作第一责任人及网络安全管理员签署网络安全责任书。学院重点系统还须通过有安全检测资质的第三方评测机构的检测。

第二十四条 信息系统需要开放互联网访问的，应同时满足以下条件且经院领导批准：

（一）符合校内上线要求并已连续稳定运行一个月以上;

（二）在公安机关完成网络安全等级保护二级及以上等级备案，符合备案等级的技术和管理要求，通过等级保护测评机构测评;

（三）具有运维服务单位且服务内容满足学院要求;

（四）实行只开放指定功能的分离部署，禁止管理后台提供互联网访问;

（五）通过图文信息中心组织的网络安全测试。

第二十五条 按照“谁经手，谁使用，谁管理，谁负责”的原则,各部门应采取措施保证信息数据安全,防止数据泄漏和丢失。未经学院批准,任何单位和个人不得向他人或校外单位提供数据。

第二十六条 信息系统网络安全管理员应强化网络安全责任意识，定期参加网络安全教育培训，履行信息系统的网络安全管理职责。系统管理人员、具有敏感信息权限的关键岗位人员应签订信息安全与保密协议，明确信息安全与保密要求和责任。信息系统由校外公司建设及运维的，该公司须签署保密协议。相关人员（含校外运维人员）工作期间获得和知晓的保密信息以及从该保密信息中得到的信息数据均应保密。

第七章 信息内容安全管理

第二十七条 学院各部门开设网站、互联网新媒体由学院宣传处归口管理。

第二十八条 网站、互联网新媒体开设单位应妥善保管管理员账号密码，及时进行内容更新，严格信息内容审查，做好数据维护、数据备份和归档工作，及时关停、注销不再使用的僵尸网站或账号。

第二十九条 学院统一建设网站群平台，学院各部门宣传类网站原则上全部纳入网站群平台，统一管理、统一防护、统一检测。图文信息中心负责网站群系统平台的安全运行维护，网站内容由开设单位管理维护。

第三十条 信息内容安全由信息发布单位负责，严格执行信息发布保密审查制度，坚持“上网信息不涉密、涉密信息不上网”原则。网站、互联网新媒体的开设单位应建立完善的信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员，加强相关人员权限管理，明确审核与发布程序，保存相关操作记录，制定应急处置流程，组织专人对上网发布内容进行检测，发现运行异常及时报告和处置。

第三十一条 信息系统、网站、互联网新媒体具有评论、留言等用户生成内容交互式栏目或功能的，主管部门应向学院宣传处报备，建立用户生成内容审查机制，确保内容先审查后展示；对于第三方平台不支持筛选的，要主动监测内容，及时处理不恰当的内容。

第三十二条 公共区域电子显示屏本地控制电脑及其相关设备实行专机专用，不得私自接入互联网，非管理人员未经许可或

授权不得擅自操作相关设备。

第八章 网络安全检查监督

第三十三条 图文信息中心联同安全保卫处，对各部门落实网络安全管理责任、执行各项管理制度的情况进行定期检查与不定期抽查。根据分类管理要求，具体制定检查的范围、内容、方式、频率、通报形式、处置方式、整改要求等。

第三十四条 图文信息中心不定期对学院内信息系统安全性进行检测，对存在安全隐患的信息系统，向其主管部门提供安全检测报告，提出整改要求。相关部门接到报告后应立即组织人员进行整改、修复和加固，并将整改情况报图文信息中心。对无法达到整改要求的，应暂停信息系统运行。

第三十五条 信息系统存在以下情形之一的，图文信息中心立即关停其互联网访问服务，并视影响范围和后果关停其校内访问服务。待整改完成后由信息系统主管单位提出恢复申请，经图文信息中心测评通过后予以恢复。

（一）发生网络安全事件的;

（二）未落实安全责任制和网络安全负责人的;

（三）未履行校内有关网络信息安全审查程序的;

（四）无有效运维服务支持的;

（五）存在中高危安全隐患或漏洞的;

（六）存在弱口令的;

（七）具有信息发布功能却无信息内容审核机制的;

（八）未按照规定留存网络日志六个月以上的;

（九）年访问量在1000人次以下，内容180天以上未更新或不维护的;

（十）网络安全管理多次无故不参加安全培训的;

（十一）未履行法律、法规规定的其他安全保护义务的。

第九章 网络安全应急管理

第三十六条 根据网络安全事件的分类及信息系统的特点，各部门须有针对性地制定服务相关法规和业务范围的网络安全事件应急处置预案。预案内容应具有规范性、可操作性和有效性，预案内容应包括:

（一）应急组织机构、人员分工及其工作职责、联系方式;

（二）报告时限要求与报告程序;

（三）应急处置方案和程序;

（四）后期处置方案;

（五）应急保障措施。

第三十七条 校内各部门应按照学院网络安全事件报告处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第三十八条 校内各部门或师生员工均有义务及时向学院相

关部门报告网络安全事件，未经授权不得对外公布事件情况，不得利用所发现的安全漏洞实施违法违纪行为。

第十章 网络安全工作考核

第三十九条 网络安全和信息化建设与管理工作情况纳入学院考核、评价、绩效分配等制度，并在年度考核中实行网络安全和信息化工作一票否决制。各部门要高度重视网络安全和信息化建设工作，将信息化工作纳入本部门工作，严格落实主体责任，建立相应的内部考核评价制度并严格执行。

第四十条 学院和各部门应建立健全责任追究制度。学院相关管理部门对未按规定履行安全职责、违反安全管理制度的单位和个人，可根据情况作以下处理:

（一）警告、责令限期整改、给予通报批评;

（二）停止网络使用;

（三）根据学院有关文件规定给予相应的行政和纪律处分;

（四）对导致重大安全事故、造成严重后果的，学院向公安部门报告，由有关部门依法追究其法律责任。

第十一章 附则

第四十一条 本办法下列用语的含义:

（一）校园网络，是指校园范围内由学院建设、运营、管理的，连接各种信息系统及信息终端的计算机网络，包括校园有线

网络、无线网络和各种虚拟专网。

（二）校园网络基础设施，是指构建校园网和校园网运行所必需的相关设施,包括校园范围内和各校区之间的各类通信管线，楼宇内网络综合布线系统、信息插座，弱电间、弱电管线、网络机房、网络机柜、配线架、跳线，以及无线网络热带你、接入设备、路由器、交换机等各类网络设备、运维管理平台等软硬件配置资源。

（三）信息系统，是指由计算机及其相关的配套的软硬件设施构成的，按照一定的应用目的和规则对信息进行采集、加工、存储、传输、检索等处理的系统，通常由服务器、操作系统、数据库、应用系统等组成，包括：公共基础服务平台、跨部门信息系统、业务部门管理信息系统、各类网站、教学资源系统、教学服务平台等。

（四）互联网新媒体，是指包括博客、微博、微信公众号、即时通讯工具、网络直播和其他移动客户端等在内的，采用第三方开放平台，向用户提供信息和服务的传播形态。

第四十二条 涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准，由学院保密办公室监督指导。

第四十三条 本办法自印发之日起施行，由宣传处、图文信息中心负责解释。

上海建设管理职业技术学院办公室　　2023年8月11日印发

（共印3份）