长沙民政职业技术学院文件

民院发〔2023〕59号

关于印发《长沙民政职业技术学院网络安全管理办法（试行）》的通知

各院、部、中心、处、室：

现将《长沙民政职业技术学院网络安全管理办法（试行）》印发给你们，请认真贯彻执行。

特此通知。

长沙民政职业技术学院

2023年12月27日

发：各院、部、中心、处、室。

长沙民政职业技术学院党政办公室　　2023年12月31日印发

长沙民政职业技术学院
网络安全管理办法（试行）

第一章 总则

第一条 为加强我校网络安全管理，确保网络安全各项工作落实到位，依据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络安全技术网络安全等级保护基本要求》（GB/T 22239-2019）和《信息安全技术应用软件安全编程指南》（GB/T 38674-2020）等相关法律法规，特制定本办法。

第二条 本办法所指网络安全管理主要包括数据中心机房管理、云平台管理、信息系统管理、VPN 管理、应急管理、责任追究等。

第三条 按照“谁建设谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络安全体系。全校师生和第三方运维服务提供商应依照本办法要求及学校相关标准规范履行网络安全责任和义务。

第二章 管理机构及职责

第四条 网络安全与信息化领导小组作为网络安全管理工作的领导和决策机构，负责统一领导、统一谋划、统一部署学校网络安全工作；统筹制定网络安全发展战略、宏观规划和重大政策；对网络安全重大事项、重点项目和政策性问题等进行研究决策。领导网络安全事件应急管理和处置。

第五条 信息处是网络安全工作的执行机构，负责统筹、规划全校网络安全建设及管理；负责学校网络安全技术指导、网络安全

监管巡察、值班值守、应急处置、业务培训等工作；配合学校宣传部门开展舆情监控，协助提供舆情管理技术支持。

第六条 管理机构成员单位作为网络安全工作的协同部门，其具体职责如下。

（一） 党政办公室负责全校各部门网络安全工作信息沟通；负责上级部门网络安全和信息化文件的传达、管理、保密等相关工作。

（二）宣传统战部负责网站、官微等内容安全；负责网络舆情管理处置；负责开展网上疏导和正面宣传。

（三） 教务处负责组织、协调上级部门网络安全竞赛，负责推动教育教学及管理中的网络安全与信息化工作。

（四）学生工作部负责学生网络文明和网络安全的教育与管理；负责对学生网络安全违纪行为进行处理。

（五）保卫部负责网络与信息安全相关的保卫；负责与国家司法机关和安全部门联络、沟通、协调网络安全问题。

第七条 各部门是部门网络安全工作的责任主体，部门负责人是本部门网络安全工作第一责任人，负责按本办法落实网络安全管理工作。并指定专人担任网络安全员，负责本部门的网络安全工作，确保每项网络安全工作落实到位。

第三章 数据中心机房管理

第八条 数据中心机房管理（以下简称为机房）包括图书馆和大运馆数据中心机房场地及 IT 设施的管理。

第九条 信息处负责机房的整体规划、设计、建设和运维。负责机房环境、UPS 电源、消防、视频监控、空调和新风系统等设施

日常巡检。负责对视频监控系统录制的人员活动录像存档，并至少保留 180 天。

第十条 非信息处人员进入机房，须遵守如下原则：

（一）须事先提出申请（见附件一），记录进出机房的日期、时间、事由、批准人等事项，信息处核实同意后方可进行，非本校人员进入机房须由学校申请人陪同进入。

（二）进入人员只能携带工作相关的工具，不得携带易燃、易爆、腐蚀性、强电磁、辐射性和流体性物质。

（三）进入人员只能操作其运维任务相关的设备和系统，不得随意插拔电源和网络，不得操作、改变和移动其他设备，禁止拍照。

（四）进入人员在运维任务完成后，须将运维设备和系统恢复原样，不得复制、传输数据中心机房的资料、文档和配置参数等，检查并关闭灯光和门禁。

第十一条 设备进出数据中心机房，须遵守如下原则：

（一）对进出机房的各类设备实行严格准入准出制度，详细记录设备的进出情况，记录内容包括设备名称、编号、功能、（原）安装位置、安装或拆除日期、操作人、批准人等信息。

（二） 设备进入机房后，应根据机房管理员的安排进行安装、加电、连网，不得擅自接入设备。

（三） 机房管理员为每台进入设备建立标签，标明设备的名称、编号、功能、负责人等主要信息。

（四）设备计划移出机房时，须在机房管理员的指导下断电、断网、拆除，不得擅自移出设备。

第十二条 **对**机房进行日常维护时，机房管理员须遵守如下原

则：

（一）保持机房内整齐干净，不得存放与系统运行无关的物品，不得存放各类易燃易爆物品。

（二）定期巡查机房内各类设备的运行情况，发现问题应及时处理。

（三）定期检查 UPS 后备电池的性能参数（检查周期原则上不大于两个月）。如果发现电池参数异常，应及时更换。电池更换时应整组进行，不应单独更换个别电池。

（四）定期检查各类消防设施，对过期或失效灭火器应及时更换。

（五）定期检查空调系统运行状态，并对室内机滤网和室外机散热器进行清扫或更换。

（六）定期检查机房照明系统工作情况，发现问题及时修复。

第十三条 机房供电发生故障且恢复时间超出 UPS 电池供电时间时，设备和信息系统负责人尽快以正常方式关闭设备和信息系统，避免造成设备损坏或数据丢失。

第十四条 当机房内温度传感器报警和烟雾传感器报警时，机房管理员应尽快到达现场，检查异常的原因并进行相应处置。

第十五条 违反机房管理原则的，信息处有权禁止其进入机房，并将其设备下架。

第四章 云平台管理

第十六条 云平台管理是指对我校建设的超融合私有云平台的管理。由服务器、存储及基础软件等组成，为全校提供云资源服务。

第十七条 信息处负责云平台的整体设计、规划、建设和运维，

负责云平台安全策略与配置。

第十八条 云平台资源需要申请才能使用。各部门可根据教学、科研、管理和服务需求，在网上办事大厅申请使用云平台资源（申请表见附件二），信息处根据申请生成虚拟服务器。虚拟服务器内部安全由申请部门负责。

第十九条 使用云平台资源，申请部门须遵守如下安全原则：

（一）安全策略管理。根据业务需求和系统安全分析制定虚拟服务器的访问控制策略，控制分配信息系统、文件及服务的访问权限。定期进行漏洞扫描，并形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别等方面。及时修补发现的安全漏洞。

（二）安全防护管理。不得以虚拟服务器为跳板，扫描、攻击其他设备和系统。使用信息处安装的防火墙或杀毒软件，定期对服务器系统、杀毒软件等进行升级和更新，并进行病毒清查，禁止随意使用U盘等移动存储介质。

（三）补丁管理。应关注部署的信息系统及其相关组件（操作系统、数据库、中间件、第三方组件）可能存在的漏洞，及时关注安全漏洞预警。确保补丁程序来源可靠，建议从厂商官方网站下载。对于支持校验的补丁程序，必须先校验可靠性，防止下载被恶意篡改后的补丁程序。重要系统升级补丁前，应制定升级方案和恢复方案，对系统重要文件进行备份。

（四） 账号安全。密码设置做到长度不得少于8个字符，至少包含英文小写字母、英文大写字母、数字和特殊字符中的三类。

（五）部署内容管理。不得使用虚拟服务器从事法律法规和学校禁止的活动，包括但不限于私自开设代理服务器，使用P2P软件、

黑客扫描软件和恶意病毒等；不得部署 BBS 论坛形式的软件，不得发布含有色情、赌博、反动内容等不良信息以及发送垃圾邮件；不得安装与业务系统无关的软件，不得安装存在版权问题的软件；不得下载和使用未经测试和来历不明的软件。

（六）配置管理。不得随意更改分配的服务器 IP 地址，不得关闭和卸载防火墙和杀毒软件。不得更改已经配置好的安全规则（包括操作系统、防火墙和杀毒软件）。

第二十条 使用部门必须有完整的备份计划，并按照备份计划备份服务器操作系统、业务系统等所有文件、数据和日志，日志保存 6 个月以上，每次备份完成后立即将备份内容迁出服务器，如因不可抗拒因素造成文件、数据和日志损失，相关责任由申请部门承担。

第二十一条 违反云平台管理安全原则的，信息处有权停止和注销其云平台资源。

第五章 信息系统管理

第二十二条 信息系统管理是指运行在我校云平台的信息系统，依据《网络安全技术网络安全等级保护基本要求》（GB/T 22239-2019）开展信息系统全生命周期安全管理。

第二十三条 信息处负责统筹学校信息系统安全管理，组织开展信息系统台账管理，定级、等级测评，备案、建设整改、安全自查、监督检查工作。

第二十四条 信息系统在立项阶段应确定安全保护等级，由信息处对建设方案进行安全论证和等级评审。根据国家网络安全等级保护要求提出初步定级建议，并指导建设部门形成安全建设方案。

第二十五条 信息系统建设部门应根据初步定级结果，在建设阶段同步落实安全保护措施，要求开发方遵循安全建设方案，所开发系统应满足身份认证、访问控制、安全审计、输入验证、数据保密性等安全要求，符合《信息安全技术应用软件安全编程指南》（GB/T 38674-2020）要求。

第二十六条 信息系统在上线运行前，信息处对其进行安全风险评估，评估报告参照信息系统等级保护对应级别相关要求，涵盖差距分析、漏洞扫描、渗透测试等方面，确保已实现系统安全功能、不存在高风险漏洞。信息系统业务无法在网上办事大厅集成，且通过信息处论证确实需要互联网访问的，建设部门根据需求在网上办事大厅申请使用互联网 IP 地址。

第二十七条 信息系统可由建设部门自行或委托第三方运维服务提供商维护。涉及重要业务或大量师生信息的核心信息系统以及安全等级第二级以上（含第二级）的信息系统，原则上应由信息处进行网络安全维护。

第二十八条 第三方运维服务提供商需要与建设部门签订网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何信息资产， 不得以服务为由强制要求学校购买、使用指定产品。

第二十九条 信息处将运行的信息系统的其纳入安全资产管理，使用安全态势感知系统进行实时监控。信息系统发生应用层面变更（如功能模块调整、版本升级等），基础设施层面变更时（如调整网络策略、变更对外开放端口和服务、变更访问控制策略、系

统迁移等），须提前向信息处报备。变更可能影响学校师生服务和管理活动时，信息系统管理部门提前通知可能涉及的学校各二级部门、教师和学生。重大变更应事先制定变更方案，做好系统和数据备份，明确回退程序。系统变更对服务造成影响的，应立即采取措施解决问题或采用恢复、回退等方式，降低影响、恢复服务。

第三十条 信息系统退出使用时，信息系统管理部门提前向信息处报备。第三方运维服务提供商停止系统的日常服务与运维，关停信息系统的互联网访问服务。信息处回收信息系统所用的 IP 地址和云平台的计算、存储、网络等资源，退出安全资产管理，删除态势感知系统等安全设备相关安全规则和策略。

第六章 VPN 管理

第三十一条 VPN 管理是指对我校 VPN 资源的管理，为全校提供校外访问校内资源服务。

第三十二条 信息处负责 VPN 的的整体设计、规划、建设和运维。

第三十三条 VPN 资源需要申请才能使用。各部门可根据教学、科研、管理和服务需求，在网上办事大厅申请使用 VPN 资源（申请表见附件三），信息处根据申请生成 VPN 账号并配置访问资源范围，VPN 账号申请人即为 VPN 账号管理员。

第三十四条 使用 VPN，须遵守如下安全原则：

（一）VPN 账号采用实名制管理，仅限申请部门及账号管理员使用，禁止将 VPN 账号以任何形式交由他人使用或借用他人账号。

（二）VPN 账号只能用于学校的教育教学、科研、管理和服务，不得将其用于商业及其他用途，不得利用 VPN 服务获得的校内资源

牟利。

（三） 确保用于登陆 VPN 终端的安全性，不得以任何理由攻击、干扰其他用户的正常使用和网络的正常运行。

第三十五条 VPN 管理员离职、调岗或者 VPN 账号访问资源范围发生变化时，信息处将注销其分配的账号。

第三十六条 违反 VPN 安全原则的，信息处有权停止和注销其账号。

第七章 应急管理

第三十七条 应急管理是指建立健全网络安全事件应急保障和恢复工作机制，提高应对突发网络与信息安全事件的组织指挥和应急处置能力，保证应急指挥调度工作迅速、高效、有序进行，保障信息系统安全运行，保障信息的合法性、完整性、准确性，保障网络、计算机、相关配套设备设施及系统运行环境的安全。

第三十八条 在网络安全与信息化领导小组领导下，实施网络安全应急管理。

（一）网络安全与信息化领导小组负责应急管理体系、管理办法和预案的评审和确定；负责应急预案启动和终止命令的下达和授权；负责应急实施过程中的决策和授权；负责对故障处置或演练后预案变更的最终评审和确认。

（二）党政办公室负责处置指挥和资源协调，协调各部门应急工作；负责应急处置情况、故障升级等相关信息的确认；负责汇报应急处置的进展情况；负责在应急过程中，策略的调整和应急指挥；负责组织并协调应急现场的各种资源。

（三）信息处负责按照现场应急指挥的指令，严格执行相应的

应急处置方案；负责将现场故障处理情况汇报和更新；在实施应急措施过程中，协调应急技术支持；故障解决后总结、归纳应急工作的经验和教训，完善相关应急预案；负责制定、修改、优化应急预案中应急场景的具体处置方案；负责组织应急预案的检查和评审工作。

第三十九条 网络安全事件根据其产生原因、表现形式，可划分有害程序事件、人为攻击事件、信息破坏事件、信息内容安全事件、设备设施故障事件和灾害性事件等六类。

第四十条 影响程度是指网络安全事件所影响的信息系统的重要程度。本预案中信息系统的重要程度是依据信息系统的安全保护定级等级来确定，安全保护等级定级为二级的为重要信息系统，安全保护等级定级为一级的一般信息系统。

第四十一条 严重程度是指事件对信息系统的破坏程度，以及利用信息网络发布、传播的信息内容对国家安全、社会稳定和公共利益的危害程度。对信息系统的破坏程度分为特别严重破坏、严重破坏和一般破坏。特别严重破坏指造成信息系统瘫痪或信息受到特别严重破坏；严重破坏指造成信息系统主要功能受损或信息受到严重破坏；一般破坏指造成信息系统性能下降或信息受到一般破坏。

第四十二条 网络安全事件根据其影响程度、严重程度、影响范围和可控性，将应急管理网络安全事件分为四级：由高到低划分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）四个级别。

（一）Ⅰ级（特别重大）：发生以下任一种网络安全事件，且不能在短时间内恢复。

1、重要信息系统受到特别严重破坏；

2、对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害的网络与信息安全事件。

（二）II级（重大）：发生以下任一种网络安全事件，且不能在短时间内恢复。

1、重要信息系统受到严重破坏；

2、对社会秩序和公共利益造成严重损害，或者对国家安全造成损害的网络安全事件。

（三）III级（较大）：发生以下任一种网络安全事件，且不能在短时间内恢复。

1、较大突发公共事件引发的，有可能造成学校网络通信故障的情况。

2、对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全的网络安全事件。

（四）IV级（一般）：发生以下任一种网络安全事件，且不能在短时间内恢复。

1、一般突发公共事件引发的，局部网络通信故障的情况。

2、其他对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益的网络安全事件。

第四十三条 应急管理分为预警发布、应急处置、后期处置三个部分。

（一）预警发布。预警信息来源于网络态势感知平台监测、上级机构或其他职能部门通报的网络安全事件信息，预警信息由网络

安全与信息化领导小组统一发布。

（二）应急处置。包括响应分级、信息报送、即时处置、事件研判、应急响应和应急结束。

1、响应分级。应急响应级别分为四级：Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级，分别对应Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级网络安全事件。

2、信息报送。网络与信息安全事件发生后，事发部门会同信息处进行初步判断，对于Ⅳ级网络安全事件，必须在2小时内向网络安全与信息化领导小组口头报告；接到Ⅲ级网络与信息安全事件报告后1小时内，应向网络安全与信息化领导小组书面报告；Ⅱ级或Ⅰ级网络与信息安全事件应立即向网络安全与信息化领导小组报告，经网络安全与信息化领导小组同意后，上报上级网络安全主管部门。

3、即时处置。网络安全事件发生后，事发部门会同信息处必须在第一时间实施即时处置，控制事态发展。在开展即时处置的同时，及时汇总信息并迅速报告网络安全与信息化领导小组。

4、事件研判。紧急情况或故障发生时，事发部门和人员发现问题后，应先详细记录该事件的信息，了解事件可能造成的损失、影响以及现场控制情况。在汇总相关信息的基础上，及时判断事件性质，分析事件已经造成的损失和预计损失、事件的严重程度和扩散性等情况，会同信息处判定事件级别。

5、应急响应。对于判定为Ⅱ级及Ⅰ级的网络安全事件，网络安全与信息化领导小组确定应急响应级别，并与党政办公室、信息处及事发部门成立应急网络安全应急处置指挥部，启动相应应急响应预案。对于判定为Ⅳ级和Ⅲ级的网络与信息安全事件，事发部门

会同信息处确定应急响应级别，启动相应应急响应预案，并向网络安全与信息化领导小组报告有关情况。

6、应急结束。Ⅰ级和Ⅱ级网络安全事件，在应急处置工作结束或相关危险因素消除，网络安全与信息化领导小组确认后，终止应急响应，转入常态管理。Ⅲ级和Ⅳ级网络安全事件，在应急处置工作结束或相关危险因素消除后，转入常态管理，并向网络安全与信息化领导小组报告。

（三）后期处置。包括责任追究、事件备案与归档以及恢复重建。

1、责任追究。应急处置工作结束后，信息处联合保卫部对事件进行调查，分析产生原因，确定责任人。具体处理办法见第八章《责任追究》。

2、事件备案与归档。应急处置工作结束后，由信息处协助事发部门将事件处置的过程和结果报网络安全与信息化领导小组备案。

3、恢复重建。信息处协助事发部门制订重建和恢复计划，迅速采取各种有效措施，恢复网络与信息系统的正常运行。并对在故障发生前半小时内所进行过的业务操作进行检查，认真核对业务数据是否正确或有无丢失，不正确或有丢失的应马上更正或补录，确保数据的正确和完整。

第八章 责任追究

第四十四条 信息处实时对数据中心机房、云平台托管虚拟服务器、信息系统、接入校园网的个人电脑和手机等进行网络安全监测。发现问题，立即整改，在规定限期整改不力的，信息处有权关

停设备、系统、网络和账号。拒不改正导致发生网络安全事件的，Ⅰ级、Ⅱ级都由保卫部移交国家司法机关和安全部门处理，Ⅲ级和Ⅳ级由学校按照相关规定处理。

第四十五条 委托第三方运维服务提供商进行运维的，应按照网络安全与保密协议，严格实施网络完全管理。委托部门承担主体责任，发生违反网络安全管理和法律法规的情况，由委托部门依据网络安全与保密协议追究其责任，学校追究委托部门责任。

第四十六条 师生员工由其所属或管理部门承担主体责任，发生违反网络安全管理和法律法规的情况，由所属或管理部门对其在年度考核中进行处罚，学校追究所属或管理部门责任。

第九章 附则

第四十七条 本办法适用于长沙民政职业技术学院网络安全的管理。

第四十八条 本办法自发布之日起施行，由信息处负责解释。

附件一

长沙民政职业技术学院数据中心机房出入申请表

<table>
<tr><td rowspan="4">出入人员基本信息</td><td>出入机房人员</td><td colspan="3"></td></tr>
<tr><td>所属单位或部门</td><td colspan="3"></td></tr>
<tr><td>联系电话</td><td colspan="3"></td></tr>
<tr><td>身份证号
（校外人员需提交身份证号及复印件）</td><td colspan="3"></td></tr>
<tr><td rowspan="2">出入事由</td><td>事由</td><td colspan="3"></td></tr>
<tr><td>开始时间</td><td></td><td>结束时间</td><td></td></tr>
<tr><td colspan="2">管理员审核意见</td><td colspan="3"></td></tr>
<tr><td colspan="2">申请部门负责人意见</td><td colspan="3"></td></tr>
<tr><td colspan="2">信息处部门负责人意见</td><td colspan="3"></td></tr>
</table>

附件二

长沙民政职业技术学院虚拟服务器托管申请表

申请时间	
申请部门	
服务器配置	
服务器托管起止日期	
操作系统类型	
服务器信息安全保障	
服务器用途	
服务器信息安全保障	
服务器用途	
服务器提供的信息服务类型	
服务访问范围	
网站域名	
网站 ICP 备案信息	
VPN 帐号需开放端口	
第三方维保服务商	
申请部门设备责任人	
管理员审核意见	
申请部门负责人意见	
信息处部门负责人意见	

附件三

长沙民政职业技术学院 VPN 用户申请表

申请时间	
申请部门	
需开通的 IP 及端口	
用户数量	
用途	
申请部门设备责任人	
管理员审核意见	
申请部门负责人意见	
信息处部门负责人意见	