康 复 大 学 文 件

康大校发〔2025〕98号

关于印发《康复大学网络与信息系统安全管理办法（试行）》的通知

各部门、单位：

《康复大学网络与信息系统安全管理办法（试行）》已经学校校长办公会议研究通过，现予以印发，请认真遵照执行。

康复大学

2025年12月24日

康复大学网络与信息系统安全管理办法（试行）

第一章　总则

第一条　为保障学校网络与信息系统安全稳定运行，规范校园网络与信息安全管理工作，促进学校信息化健康可持续发展，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》等相关法律法规要求，结合我校实际，制定本办法。

第二条　本办法适用于所有学校规划建设的非涉密网络与信息系统，以及构建在校园网上的信息系统。涉及国家秘密的网络与信息系统安全管理办法，由学校相关部门另行制定。

第三条　本办法所称网络与信息安全工作是指通过采取必要管理措施或技术手段，防范对网络和信息系统的攻击、侵入、干扰和非法使用等破坏，保障网络相关基础设施、信息系统及数据的完整性、保密性和可用性，使学校网络和信息系统处于稳定可靠的运行状态。

第四条　学校任何部门及个人均应按照国家有关法律法规要求，合法使用校园网络及信息系统，不得有危害校园网络、信息系统及利用校园网络、信息系统侵犯国家与集体利益以及个人合法权益的行为，不得从事违法犯罪活动，不得从事以营利为目的的商业活动。

第五条　网络与信息系统安全须贯穿学校信息化建设始终，

做到同步规划、同步建设和同步运行。

第二章　组织机构与职责

第六条　学校网络安全与信息化工作领导小组是学校网络与信息安全管理的议事决策机构，全面指导学校网络与信息安全工作。网络安全与信息化工作领导小组办公室，负责统筹学校网络与信息安全防护体系的建设、管理与运行维护。

第七条　学校党政管理部门的处级机构，教学科研实体单位的二级学院、研究院，教辅机构，直属单位（以下统称各部门）按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，负责本部门建设、运维、使用的各类网络、信息系统，以及服务器、数据库、堡垒机、VPN、电子显示屏、终端等相关信息化资产的安全。各部门主要负责人为本部门网络与信息安全第一责任人，对本部门网络与信息安全工作负总责。各部门须将网络安全作为安全稳定工作的重要组成部分，纳入重要议事日程，落实网络安全专人负责机制，落实重要时期的网络安全保障机制，建立本部门的网络安全管理制度和应急处置预案。

第八条　各部门信息化建设联络人，负责本部门网络安全的具体工作。人员变动时应及时向信息网络中心备案。

第九条　广大师生作为校园网的使用者、信息化建设的参与者，同时也是网络与信息安全工作的参与者，有责任和义务遵守学校网络与信息系统安全的相关规定，积极参与网络与信息安全

的建设和管理。

第三章　保障及机制

第十条　网络与信息安全工作是学校信息化建设的重要工作，各相关部门应通力合作，在人员、资金、技术、设备等方面提供充足的支持与保障。

学校在经费安排上切实保障网络安全等级保护测评、网络安全监测和检测评估、信息系统安全升级和防护加固、网络安全攻防演练、网络安全教育培训、网络安全事件处置和安全运维等网络安全常规工作预算。

第十一条　按照国家相关法律法规要求，学校及时开展校内网络安全等级保护（以下简称等保）工作。信息网络中心负责等保工作的组织协调，确保学校等保工作按照国家法律法规要求正常开展，各部门应积极配合。

第四章　网络系统安全

第十二条　学校网络系统分为学校主干网络和部门自建网络两级。学校主干网络由数据专网、智能化专网、安防专网、科研专网等四套相互独立的网络组成，未经网络安全与信息化工作领导小组审议通过，任何部门不得改造主干网络的设计和规划。

第十三条　学校主干网络由学校统筹建设和管理。信息网络

中心负责学校主干网络的线路铺设与维护、设备部署与运维、流量监测与管控，保障学校主干网络的安全畅通。校园网络应当部署相关网络安全设备，实现对网络攻击行为的实时监测和告警。

第十四条 学校主干网络的各类设备，其管理、维护等均由信息网络中心统一负责，未经信息网络中心批准，不得以任何方式试图登录、修改、配置校园网内的交换机、路由器和服务器等。严禁任何部门或个人以任何理由损毁校园网络设备设施。

第十五条 校园网络系统对外采用统一出口，实现一体化管理。学校各部门在校园内不得通过其他渠道接入互联网及其他公共信息网络。

信息网络中心负责管控校园网络对外的统一出口，负责统一管理所有出口链路的公网 IP 地址。校园网络实现多出口链路，所有出口链路需通过防火墙等安全设备进行防护。

第十六条 在维修或拆除涉及校园网络的建筑物时，在维护或开挖涉及校园网络的道路时，须事先通知信息网络中心，以保护校园网络设备设施的安全。

第十七条 校园网络接入部门的网络设备须实行账号的分权管理，要求用户权限设置遵循最小授权和权限分割原则，且用户登录、操作等相关活动日志应至少保存 6 个月。设备密码须为 8 位以上，由大小写字母、数字和特殊字符混合组成，并定期更换。严禁使用弱密码、明文密码，且不得以明文形式存储或传输。

第五章　信息系统安全

第十八条　学校信息化项目建设应遵循校内外网络安全相关制度、技术规范、标准流程开展，信息化项目全生命周期内各环节均需要完成相关网络安全建设工作。各信息化项目上线、验收前须通过必要的网络安全检测。

第十九条　各部门与系统供应商、运维服务商、云服务供应商签订的合同中应明确各方安全责任、服务内容、保密义务、知识产权、违约后果等条款，并负责监督其履行情况。对于须使用校外云服务建设的信息化项目，校内项目主管部门在采购文件和合同中应明确要求由云服务供应商负责项目的网络安全建设，并明确约定各自的网络安全责任范围，共同承担网络安全责任。

第二十条　各部门应建立信息系统动态管理清单，标明系统软测情况、源代码、数据字典和技术文档提供情况，以及系统运维情况（包括系统责任人、系统上线时间、保密协议、系统管理员、用户数、数据量、个人信息条数等）。系统责任人负责操作系统、数据库等核心管理权限、安全审计、数据库导入导出、密钥管理、运维账号管理等。

第二十一条　各部门信息化建设中所涉及到的业务数据、个人信息等，须按照国家相关法律法规，采取必要的安全措施进行保护，任何部门及个人不得违法违规采集、存储、使用和处理校内各类个人信息。

第二十二条　对外提供服务的信息系统，原则上须使用域名

作为访问入口。

第二十三条 面向在校师生提供公共服务的信息系统原则上须使用学校统一身份认证。对于仅供校内教职工、学生使用且承载大量重要数据和信息的信息系统，应关闭校外直接访问通道，教职工和学生在校外可使用学校的 VPN 系统，实名认证后访问。

第二十四条 信息系统的注册用户应实名认证，由信息系统的运营者负责实名认证的实施。信息系统的密码设计应严格按照网络安全等级保护要求，密码须为 8 位以上，由大小写字母、数字和特殊字符混合组成，不得以明文形式存储或传输，并支持双因子登录认证方式，重要信息系统密码应设置 12 位以上，定期进行变更。

第二十五条 各部门要保留不少于 6 个月的用户登录、操作等相关活动日志。

第二十六条 信息系统建设部门应定期备份信息系统的重要信息数据，根据数据的重要性和系统运行需要，制定数据的备份和恢复策略与程序等。

第二十七条 对于不符合网络与信息系统安全要求的各类信息系统必须先进行整改，整改完成后方可继续进行建设或继续提供服务。

第二十八条 各部门对信息系统招标时，应按照《信息安全等级保护管理办法》，在系统正式上线前，要求供应商提供网络安全等级保护测评服务（包括定级、备案、建设整改、安全测评、

监督检查等）。等保到期后，提供网络安全等级保护复测服务不少于一次。

第二十九条 信息系统运行维护部门应建立信息系统值守制度，制订应急处置流程，组织专人对信息系统进行监测，发现信息系统运行异常及时处置。

第三十条 对于使用频度不大、阶段性使用的信息系统，信息系统建设部门可采取非工作时间或寒暑假、节假日关闭的方式运行。对于无人管理、无力维护、长期不更新的信息系统，信息系统建设部门应停止系统服务以降低安全风险。

第三十一条 各部门应加强信息系统生命周期管理，在确定信息系统退出运维和服务周期后一周内办理撤销备案手续。

第六章 终端设备安全

第三十二条 终端设备是指由学校师生使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括电脑、智能手机、电视、显示屏、网络打印机及其它联网终端及附属设备。

第三十三条 接入校园网络的每台设备都应具有明确的属主，终端设备使用人按照“谁使用，谁负责”的原则，对其终端设备负有保管和安全使用的责任。

第三十四条 终端计算机设备上安装、运行的软件须为正版软件。在终端计算机上使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第三十五条 终端计算机使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处置。

第七章 安全检测与安全事件处置

第三十六条 各部门应针对所建设和管理的网络与信息系统建立安全管理制度，定期开展网络安全自检自查，及时修补漏洞、升级防病毒软件、查看系统日志，确保系统安全。

第三十七条 信息网络中心建立定期与不定期相结合的安全检测制度，对全校的网站及信息系统开展安全检查。检查不合格的网站或信息系统，视其漏洞级别暂停其外网访问，同时通知责任部门限期整改并提交《网络安全事件和隐患处置情况反馈表》。整改完成并经复查合格后，方可恢复正常访问。对于不积极配合整改的，信息网络中心有权直接对相关的网络及信息系统进行断网、停止服务等应急处理。

第三十八条 信息网络中心建立全天候网络安全监测体系。各部门应根据本部门信息化建设情况制定相应的监控制度，重要安全保障期间应安排人员值守，发现网络安全问题应及时向信息网络中心报告并进行必要的应急处置。

第八章　责任追究

第三十九条　有关部门在收到网络与信息安全限期整改通知书后，整改不力的，学校给予通报批评;玩忽职守、失职、渎职造成严重后果的，依纪依法追究相关人员的责任。

第四十条　各部门应按照学校网络安全事件应急预案及时、如实地报告和妥善处置网络信息安全事件。

第四十一条　师生员工违反网络与信息安全相关管理规定造成不良后果的，视情节轻重，分别由人事管理部门或学生管理部门按相关规定给予批评教育或纪律处分;其中触犯法律的，由相关国家机关依法追究法律责任。

第九章　附则

第四十二条　本办法由信息网络中心负责解释。

第四十三条　本办法自公布之日起施行。

附件：网络安全事件和隐患处置情况反馈表

附件

网络安全事件和隐患处置情况反馈表

<table>
<tr><td colspan="2">*事件名称</td><td colspan="3"></td></tr>
<tr><td colspan="2">*事件类型</td><td></td><td>*危害等级</td><td>低危、中危、高危或紧急</td></tr>
<tr><td colspan="2">*事件描述及原因</td><td colspan="3"></td></tr>
<tr><td colspan="2">*系统名称</td><td></td><td>*系统用途</td><td></td></tr>
<tr><td colspan="2">*域名/URL</td><td></td><td>*校内 IP 地址</td><td></td></tr>
<tr><td colspan="2">*部门名称</td><td colspan="3"></td></tr>
<tr><td colspan="2">*负责人</td><td></td><td>*联系电话</td><td></td></tr>
<tr><td colspan="2">*处置人</td><td></td><td>*联系电话</td><td></td></tr>
<tr><td rowspan="3">总结报告</td><td>*事件处理经过</td><td colspan="3"></td></tr>
<tr><td>*今后防范措施</td><td colspan="3"></td></tr>
<tr><td>*部门承诺</td><td colspan="3">我部门承诺：平时加强安全管理，及时升级系统补丁，堵塞漏洞，确保网络安全与信息安全，如出现问题，愿承担一切后果与责任。</td></tr>
<tr><td colspan="2">*系统是否修复</td><td></td><td>*系统修复时间</td><td></td></tr>
</table>

康复大学党政办公室　　2025年12月26日印发