华南理工大学文件

华南工网信〔2022〕2 号

关于印发《华南理工大学网络安全管理办法（试行）》的通知

各院（系）、校直属各单位、机关各部门:

为进一步做好学校网络安全管理工作，根据《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）、《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）、《中华人民共和国个人信息保护法》（中华人民共和国主席令第九十一号）和《关键信息基础设施安全保护条例》（中华人民共和国国务院令第 745 号）等相关法律法规要求，学校结合实际，研究制定了《华南理工大学网络安全管理办法（试行）》，经 2022 年第四次校长办公会议审

议通过，现予以印发，自 2022 年 9 月 26 日起实施，请遵照执行。

华 南 理 工 大 学

2022 年 9 月 21 日

华南理工大学网络安全管理办法
（试行）

第一章　总 则

第一条　为进一步做好学校网络安全建设与管理工作，保障数据安全和信息系统持续稳定、可靠运行，根据《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）、《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）、《中华人民共和国个人信息保护法》（中华人民共和国主席令第九十一号）和《关键信息基础设施安全保护条例》（中华人民共和国国务院令第745号）等相关法律法规要求，结合学校实际，特制定本办法。

第二条　本办法所称网络安全工作，是指为保障学校建设、运行、维护或管理的校园网基础设施、数据中心、信息系统、移动互联网应用程序、网站、数据等信息资产的完整性、保密性和可用性而开展的相关管理和技术工作。

第三条　本办法所指网络安全不包括涉密信息系统安全，其管理由学校另行规定。

第二章　网络安全管理的组织与保障

第四条　学校网络安全和信息化领导小组是学校网络安全管理的议事决策机构。主要职责是:

（一）组织协调学校网络安全和信息化发展与管理方面的重大事项，统筹部署学校网络安全和信息化工作。

（二）审定网络安全相关规定，组织校内网络安全考核工作等。

网络安全和信息化领导小组日常工作由领导小组办公室（以下简称“网信办”）负责。

第五条 信息化办公室是网络安全工作归口管理单位。主要职责是:

（一）负责学校网络安全规划、推进、监督和教育培训等工作，协调网络安全事件的处置。

（二）组织协调各单位统一开展信息系统网络安全等级保护（以下简称“等保”）定级、备案和测评工作。

（三）组织开展学校关键信息基础设施安全保护工作。

第六条 信息网络工程研究中心（以下简称“网络中心”）是网络安全技术支撑单位，负责学校网络安全防护体系的建设、运行维护、技术指导和服务支持。

第七条 各二级单位主要负责人是本单位网络安全第一责任人，主管网络安全工作的负责人为直接责任人。各二级单位主要职责是:

（一）指定在岗在编的专职人员担任信息化联络员，负责处理、协调本单位网络安全具体工作，包括及时开展校内信息系统等保工作，参与关键信息基础设施识别认定、检测评估等工作，积极参与并做好网络安全宣传推广等。

（二）按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，遵循学校的管理规范和技术标准，建立本单位网络安全管理制度。

（三）组织实施本单位建设、运维、使用的信息系统和内部网络的安全工作，及时开展校内网络安全等保工作。信息系统建设单位是信息系统网络安全等级保护及测评整改的责任主体，应全力配合等保测评工作，积极参与关键信息基础设施识别认定、检测评估等，并按照要求进行网络安全加固。

（四）监督承担本单位信息系统和内部网络建设和服务的校外单位做好相关的网络安全工作。

第八条 学校教职工和学生作为校园网络的使用者，应遵守学校网络安全相关规定，积极参与网络安全的建设和管理，依法处理和保护个人信息。

第九条 学校在网络安全等保测评、系统升级加固、评估监测、事件处置、宣传培训和安全运维等方面安排专项资金以确保相关工作顺利开展，各单位新增信息化项目应包含网络安全专项预算。

第三章 校园网基础设施的安全

第十条 校园网指校园计算机网络，主要用于学校教学、科研、管理和服务等各项业务，严禁任何单位和个人利用校园网及相关基础设施开展各类未经许可的活动。校园网及相关基础设施由信息化办公室负责统一规划，由网络中心负责建设、管理、维护和防护，

并提供互联网的统一接入。任何单位及个人不得擅自建设、更改、损毁和挪用校园网设施，不得私自接入其他网络，不得私自提供给校外人员使用。

第十一条 校园网接入实行登记备案制，网络使用实行实名制。校内用户通过实名登记后方可按照入网要求使用校园网，未经登记不得以任何方式私自接入校园网，严禁盗用其他用户账号信息使用校园网。

第十二条 未经信息化办公室审核同意，信息化专业系统的业务专网中的任何设备不得私自接入校园网、互联网，校园网的任何设备也不得私自接入业务专网。

第十三条 校园网 IP 地址不得面向校园网外提供互联网服务。如在教学、科研上确有特殊需求，IP 地址需对外开放服务（限于非信息发布类服务）的，须经信息化办公室审批同意后方可开放，由 IP 使用单位承担相应的网络安全责任。

第十四条 各单位负责本单位所安装使用的网络打印机、电子显示屏、门禁、水电控制器等物联终端及其控制系统的安全防护，及时向信息化办公室登记安装使用情况，并加强安全监管，落实防范措施，确保运行安全。

第十五条 校园网用户应文明上网，做好上网终端安全防护，依法保护个人信息安全，发现网络安全事件应及时上报。校园网用户的上网行为不得危害学校网络安全和正常秩序，严禁利用校园网从事任何无授权的扫描、渗透、破坏、信息窃取等网络攻击活动。

第十六条 终端设备使用者应做好终端设备的安全防范，终端设备上安装、运行的软件须为正版软件，使用盗版软件带来的安全和法律责任由终端设备使用者承担。

第四章 信息系统和数据安全

第十七条 学校信息化项目建设应遵循学校网络安全相关制度、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完成相关网络安全建设工作，落实等保要求。信息系统上线、验收前，须完成校内登记，通过必要的网络安全检测和测评。学校信息化项目建设过程中，不符合网络安全要求的信息化项目须进行整改，整改完成后方可继续建设或提供服务。

第十八条 学校和各单位建设和管理的信息系统原则上应部署在学校的数据中心并使用学校 IP 地址及域名；涉及学校基础数据、教职工和学生个人信息或敏感信息的信息系统，不得部署在校外；未经信息化办公室审批同意，严禁使用境外数据中心（包括云服务）。

特殊用途信息系统须经信息化办公室审批同意方可使用非学校域名或在非校园网环境建设。

非学校域名或在非校园网环境建设的信息系统，与学校教学、科研、管理和服务等各项业务无关的信息系统，以及未经信息化办公室审批的信息系统，原则上不得使用校名、校徽、域名等学校标识，所有网络安全责任由该系统校内相关单位（包括系统建设单位、

使用单位、宣传推广单位等）及参与人员承担。

第十九条 面向在校师生的校内各信息系统应集成到学校统一门户中，其用户登录须使用学校统一身份认证。各单位的移动互联网应用程序原则上应基于学校统一的移动门户和入口进行建设、运行和服务。移动互联网应用程序应按照教育行政管理部门、公安部门有关要求履行备案程序，并进行等保测评。

第二十条 信息化数据资源是学校的公共资源和战略资源，各单位应严格遵守国家相关法律法规，并按照学校信息化数据资源相关管理规定，建立数据分类分级保护制度，制定重要数据目录，对重要数据做好定期完整备份和实时增量备份，确保重要数据资源不被破坏、篡改和泄露，并定期进行数据安全风险评估。与学校共享数据库对接的业务系统，应加强对共享数据的安全管理。

第二十一条 信息系统应完善日志功能，按国家相关规定记录并保存管理员和用户登录/退出、信息修改和关键操作、系统运行和维护等日志。

第二十二条 信息化建设中所涉及到的个人信息，须按照国家相关法律法规和学校个人信息保护相关规定进行严格保护，任何单位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。

第二十三条 各单位的网站原则上应基于学校网站群平台进行建设。网络中心负责网站群平台建设和运维安全，各单位负责本单位网站管理账号和内容安全。

第二十四条 各单位使用学校公务电子邮箱，教职工、学生使

用学校个人电子邮箱应遵守学校电子邮箱管理等相关规章制度，并对使用其电子邮箱账号开展的所有活动负责，禁止使用电子邮箱传播恶意程序和不良信息，禁止使用电子邮箱存储、处理、传输涉密信息。

第二十五条 各信息系统应加强账户安全管理，杜绝使用弱密码、默认密码和通用密码，杜绝僵尸账号。

第五章 网络安全监测预警与应急处置

第二十六条 学校授权网络中心对校内各类信息系统、网络和其他相关设备开展网络安全检测工作。信息化办公室可根据检测结果启动校内网络安全事件处置流程或发布安全预警。

第二十七条 网络中心负责学校网络安全相关的各类安全情报搜集和分析，信息化办公室结合校内信息化建设实际情况对校内开展网络安全预警。相关单位及人员应根据预警信息，落实网络安全自查及问题修复，避免预警相关安全问题的发生。

第二十八条 校内网络安全事件的处理由信息化办公室负责协调并由网络中心负责实施。安全事件相关单位及人员应认真落实网络安全事件处置相关工作。为避免扩大网络安全事件的不良影响，在发生重大网络安全事件等紧急情况下，网络中心可直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第二十九条 信息化办公室负责组织校内网络安全事件应急演练，相关单位应通力配合，通过演练提高校内网络安全事件处置

能力。

第三十条 各二级单位应根据本单位信息化建设情况制定相应的监控与值守制度和网络安全事件报告流程，发现网络安全问题应及时向网络中心报告并进行必要的应急处置，不得在未经学校同意的情况下对外公布、测试或利用所发现的安全漏洞或安全隐患。

第三十一条 各二级单位应对所属信息系统（网站）进行安全监测，安排专人定时巡检和备份数据，保证网络状态、安全事件等相关日志留存 180 天以上，并采取必要的安全措施，严防黑客入侵、数据被篡改、信息泄露等事件发生。

第三十二条 学校制定学校网络安全应急预案，明确相关单位在网络安全应急响应过程中的工作职责，定期开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。各二级单位成立本单位网络安全应急响应小组，在信息化办公室指导下制定本单位的网络安全应急预案，并报信息化办公室备案，定期开展相应的宣传、教育和培训。

第六章 考核评价与责任追究

第三十三条 学校将网络安全工作纳入各单位发展考核指标体系，将网络安全责任制落实情况作为对各单位、单位领导班子和领导干部综合考核评价的重要内容。网信办负责组织校内网络安全考核工作。

第三十四条 对于违反网络安全相关法律法规和学校相关规

章制度的单位和个人，经网信办查实，学校将视情节轻重发出网络安全整改通知书，给予限期整改、封停账号或端口、暂停或者中止网络与信息化服务、通报批评、纪律处分等处理。对于违反法律、法规的，学校还将依法配合公安、网信、通信管理等部门进行处理。

第三十五条 各二级单位在收到网络安全整改通知书后，应按要求限期整改。对于整改不力的，由网信办给予通报批评并责令改正；瞒报、缓报网络安全事件的，由网信办对相关单位责任人进行约谈并通报批评；对于玩忽职守、失职渎职造成严重后果的，学校将依法依规追究相关人员的责任。

第七章 附 则

第三十六条 学校原有其他涉及网络安全的相关规定，如与本办法不一致，以本办法为准。各单位可参照本办法制定相应的实施细则。

第三十七条 本办法自 2022 年 9 月 26 日起实施，由学校负责解释，具体工作由信息化办公室、网络中心承担。

华南理工大学办公室 主动公开 2022 年 9 月 26 日印发