华东师范大学网络安全管理办法

第一章 总 则

第一条 为规范学校网络安全管理,提高网络安全防护能力和水平，保障学校各项事业健康有序发展，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》《信息安全等级保护管理办法》《信息安全技术网络安全等级保护基本要求》《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》等国家有关政策、法规及指导性文件，结合学校实际，特制定本管理办法。

第二条 网络安全工作关系到学校安全和广大师生切身利益，关系到学校教学、科研和管理各项工作的稳定运行，在学校统筹安全与发展工作中具有重要地位。应加强党对学校网络安全工作的领导，发挥党委的政治核心作用，严格落实主体责任，努力形成党委统一领导、党政齐抓共管、有关部门各负其责的网络安全工作格局。

第三条 校内各级党组织要强化政治责任，建立“主要负责人负总责，直接负责人牵头抓”的网络安全领导责任制。按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”和“属地管理，逐级负责”的原则，学校党委负责指导和监管全校网络安全工作，各相关机构、各部处在职能范围内负责网络安全监督管理工作，各二级单位党组织对本单位网络安全工作负主体责任，落实网络安全

各项任务。

第二章 组织机构及职责分工

第四条 学校网络安全与信息化领导小组(以下简称网信领导小组）是学校网络安全工作的领导机构，学校党委书记和校长担任网信领导小组组长,分管宣传和信息化的校领导担任副组长。主要承担以下网络安全职责:

（一）贯彻落实上级部门关于网络安全的决策部署，贯彻落实网络安全法律法规和政策文件，明确学校网络安全发展战略、总体布局、制度规范、重大政策和工作要点;

（二）贯彻落实党委领导下的网络安全决策机制，定期组织召开专题会议部署网络安全工作，听取网络安全工作汇报，研究网络安全重大问题，审议网络安全重大项目;

（三）统筹协调全校网络安全保护和重大事件处置工作，督促各级单位落实网络安全政策规定,组织开展网络安全信息通报,组织领导网络安全检查和评价考核工作;

（四） 向上一级网信领导小组及时报告网络安全重大事项。

第五条 学校网络安全与信息化管理办公室(以下简称网信办）为学校网络安全工作的管理部门。主要承担以下网络安全职责:

（一）负责网信领导小组日常事务工作，在网信领导小组领导下统筹协调网络安全推进工作;

（二）贯彻落实上级部门和网信领导小组关于网络安全工作

的重大决策、总体部署和工作要求，组织开展网络安全重大问题调研并向网信领导小组提出工作建议;

（三）负责制订网络安全政策文件，建立网络安全制度，建立完善校园网络安全综合治理体系和协同工作机制;

（四）负责指导、监督、检查网络安全重点任务落实，推进实施各单位网络安全责任制考核评价工作;

（五）负责建立网络安全专家咨询机制，监测、研判网络安全重大风险，及时向网信领导小组报告网络安全信息;

（六）负责校园网络内容安全管理和网络舆情工作;

（七）负责组织开展网络安全宣传教育活动;

（八）负责制订网络安全年度工作要点，进行工作总结;

（九）承担网信领导小组交办的其他网络安全工作事项。

第六条 学校信息化治理办公室（以下简称信息办）作为网络技术安全工作的负责部门。主要承担以下网络安全职责:

（一）作为网络安全协调机制单位，负责落实网络技术安全管理保障和建设工作;

（二）协助拟订网络技术安全政策措施和规章制度，指导各单位落实各项技术安全工作，建立保障有力的网络技术安全建设和管理支撑队伍;

（三）全面实施网络安全等级保护制度，对关键信息基础设施实行重点保护，建立健全校园网络技术安全保障体系;

（四）开展全校网络技术安全监测预警和信息通报工作，发现威胁及时通报相关单位并跟踪核查修复情况，协助实施网络技

术安全责任制考核评价工作;

（五）制定网络技术安全事件应急预案和处置机制，发生安全事件及时报告、及时处置;

（六）指导监督各单位落实重要时期的各项网络技术安全保障要求;

（七）实施网信领导小组交办的其他网络安全工作事项。

第七条 二级单位党组织主要承担以下网络安全职责:

（一）及时传达和认真贯彻学校网络安全工作的决策部署和工作要求，贯彻落实网络安全法律法规和政策文件。

（二）统筹本单位的网络安全建设和管理工作。建立健全网络安全责任制和相关制度规范，落实网络安全管理和防护措施，并将网络安全责任要求落实到本单位各内设机构。

（三）将网络安全工作纳入领导班子重要议事日程，建立健全二级单位党组织领导下的网络安全决策机制，落实相关人力、财力、物力的支持和保障，制定网络安全工作规划，确保网络安全各项任务落实到位。

（四）落实网络安全工作队伍。明确由本单位党政主要负责人担任网络安全第一责任人，由主管网络安全的领导班子成员担任网络安全直接责任人，由具体分管网络安全的工作人员担任网络安全联络员，各类信息系统（网站）和新媒体账号等由在职教职员工担任管理员，重要系统、平台的管理员应建立工作补位机制，确保相关人员具备第一时间应急响应能力。

（五）落实网络安全清查工作。及时向网信办报送本单位网

络安全工作队伍通讯录，向信息办报送信息资产清单，向党委宣传部报备本单位新媒体公众账号清单。

（六）落实网络安全等级保护制度。依法完成所属信息资产的网络安全等级保护定级备案、等级测评、安全建设等工作。

（七）开展网络安全自查工作。定期组织针对本单位信息系统的安全巡查，对负有主体责任的网络发布内容进行适时跟踪和把关，建立网络安全工作台账。

（八）做好网络安全应急响应工作。配合学校开展本单位网络安全保护和重大事件处理工作，制定网络安全应急预案并定期组织应急演练，发生重大网络安全事件，网络安全负责人应一线指挥，第一时间报告学校信息办、网信办及相关职能部处，并第一时间做好应对处置。

（九）及时汇总并向网信办报告网络安全重大事项。

第三章 网络及信息系统安全

第八条 校园网及相关基础设施由学校统一规划、建设、管理，并提供统一网络出口。校内各单位及个人不得擅自建设、更改、损毁、挪用校园网设施，不得私接外网出口，不得私自提供给校外人员使用。

第九条 校园网接入实行登记备案制，使用网络实行实名制。校内用户必须通过学校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接校园网。严禁盗用其他用户

上网信息使用校园网。

第十条 校园网主要服务于学校教学、科研、管理、服务等业务工作，用户不得将校园网用于其他用途。严禁任何单位和个人利用校园网络及相关基础设施开展各类未经许可的其它活动。

第十一条 校园网用户应文明上网，规范网络行为，并做好个人网络信息安全维护。校园网用户的上网行为不得危害到学校整体网络信息安全，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等互联网攻击活动。

第十二条 校园网 IP 地址或域名未经许可不得对外提供互联网服务。若需要 IP 地址或域名对外开放服务，应经信息办、网信办审批后方可开放，建设单位承担全部网络安全责任。

第十三条 校园网提供统一的域名解析服务，任何单位及个人不得私自架设域名服务器，对外提供域名解析服务。

第十四条 各单位负责本单位安装使用的网络打印机、电子显示屏等物联终端及其控制系统的安全防护，应掌握使用情况、落实防范措施、加强安全监管、确保运行安全。

第十五条 终端计算机使用人应做好终端计算机的安全防范，终端计算机上安装、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计算机使用人承担。

第十六条 各单位和教职工、学生使用学校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、传输涉密信息和工作敏感信息。

为确保邮箱安全，学校将定期冻结或收回长时间未使用的邮箱。

第十七条 学校信息系统必须符合国家、地方和学校等各级单位有关网络安全的法律法规和制度要求。对于不符合网络安全要求的信息系统必须先进行整改，整改完成后方可提供服务。

第十八条 未经信息办、网信办审批备案的信息系统不属于学校信息资产，不得使用学校相关信息化资源，不得使用校名、校徽等学校标识，一切网络安全责任由系统建设、使用单位或个人承担。

第十九条 IP 地址或域名需对外开放的应用服务，应按照国家法律法规要求开展相应网络安全等级保护（以下简称安全等保）工作。信息办负责校内信息系统安全等保工作的组织协调，各单位负责本单位主管信息系统安全等保工作的具体落实。

第二十条 面向互联网开放的信息系统每年须由其责任单位提交网络安全自查报告。如发生安全事故被上级部门通报，学校将第一时间关停其互联网服务。待通过安全等保测评，或迁移至已通过安全等保的学校网站群平台等系统后，方可继续对外开放。

第二十一条 各单位应强化供应链安全管理，采用安全规范、质量和售后服务优良的软硬件产品并选择服务优质、资质和信誉良好的服务厂商承建信息系统建设项目，优先选用具有自主核心技术以及安全性达到要求的国产化产品。

第二十二条 各单位应加强信息技术外包服务的安全管理，对外包服务全流程实行严格监督和管理，确保外包服务的连续性和安全性。

第二十三条 各单位应加强信息资产管理，规范信息资产的新增购置、日常运维和更新替代，形成信息资产清单，有效保障信息资产安全。

第二十四条 新建信息系统项目立项时应将安全运维与安全等保测评费用纳入预算。新建信息系统项目中的人员、经费、采购、合同、建设、验收、运维等各环节中都需包含网络安全相关说明。

第二十五条 新建信息系统项目验收前必须通过必要的安全检测，未通过检测不得验收。新建信息系统如需面向互联网开放，必须通过安全等保测评。

第二十六条 各单位应加强源代码安全管理，在信息系统上线运行前或者发生重大变化时须进行系统源代码安全审查。

第二十七条 各单位信息系统建设须引入严格的版本控制系统，若发生系统小版本更新，须第一时间提交信息办开展相关安全检测。系统各类日志留存时间不少于6个月。

第二十八条 各单位门户网站及其它各类文章发布类信息系统，应统一基于学校网站群平台进行建设。信息办负责网站群平台的建设、管理和运维，提供建站技术支持，各单位负责网站的规范运行和内容安全。

第二十九条 原则上各单位不得再建设使用校外IP地址或校外域名提供学校相关服务的系统。对于现使用校外IP地址或校外域名提供学校相关服务的系统须每年进行审查，如有不符合网络安全规定者限期迁至校内或关停。相关责任单位应落实安全等保

要求，或将系统迁移纳入学校统一管理。

第三十条 各单位的移动互联网应用程序应经信息办审核后单独备案，按照教育部、公安部有关要求履行备案程序，经等保测评和安全评估方可上线。大范围采集个人信息的移动互联网应用程序应通过移动应用个人信息安全认证。超过半年未更新移动互联网应用程序应予以关停。

第三十一条 各单位应加强信息系统的数据安全，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。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。未经批准，严禁使用境外数据中心存储数据。

第三十二条 各单位应按照国家有关法律法规的规定严格保护学校师生个人信息，不得违规采集、存储、使用和处理校内各类个人信息。

第三十三条 各类信息系统使用者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。关键岗位的信息系统使用和管理人员应签订网络安全保密协议。离岗、离职人员的访问权限应及时予以终止。

第三十四条 各类信息系统均应向信息办、网信办提交备案，备案信息发生变化须及时提交更新，不再使用的信息系统应按照相关流程进行注销。

第四章 监测预警与应急处置

第三十五条 校内网络安全事件的处理由信息办负责组织实施，按照学校网络安全事件报告与处置流程进行分级、分类处理。为避免安全事件不良影响扩大，信息办有权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。

第三十六条 信息办负责组建校内网络安全应急响应组织，制定相应的应急响应流程、规范。

第三十七条 各单位应根据本单位情况制定相应的网络安全监测与值守制度，发现网络安全问题应及时进行处理，并及时向信息办报告。重要时期，各单位应严格执行 7×24 小时值守和领导带班制度，保持通讯联络通畅。

第三十八条 网络安全事件处理后，由信息办与相关单位共同进行责任认定，并根据本办法第五章规定对责任人、责任单位进行处理。

第五章 学习与培训

第三十九条 各单位需组织本单位全体教职工学习《中华人民共和国网络安全法》《计算机信息网络国际互联网安全保护管理办法》《中华人民共和国计算机信息系统安全保护条例》等规章制度，提高本单位教职工维护网络安全的警惕性和自觉性。

第四十条 各单位应积极配合网信办的工作，自觉参加网信办组织的校内外培训活动。

第四十一条 各单位每年需安排每位在职人员完成不少于 4

个学时有关网络安全的学习与培训任务，并纳入教职工政治理论学习统筹管理。其中，集中学习、研讨 1 学时，自主学习 3 学时及以上。

第四十二条 各单位组织的网络安全学习与培训可采取线下和线上等多种形式：既可组织线下的网络安全法规的学习，进行网络安全知识和技术的培训；也可依托网络资源组织线上学习，听取专题报告、开展线上专题研讨等。

第四十三条 各单位需指定专人对学习和培训进行通知和管理，并负责记录本单位的学习和培训情况台账。

第六章 奖励与处罚

第四十四条 学校将网络安全工作纳入学校发展考核指标体系，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。

第四十五条 各单位在收到网络安全整改通知书后，应按要求限期整改，整改不力的，给予通报批评并责令改正；瞒报、缓报网络安全事件的，对相关单位责任人进行约谈并通报批评；玩忽职守、失职渎职造成严重后果的，严肃追究相关人员的责任。

第四十六条 对于违反本管理办法及相关网络安全制度的单位和个人，经信息办、网信办查实，可对其暂停或终止一切网络与信息化服务，并根据安全事件的影响程度提交相关职能部门或网信领导小组商讨处理意见。

第四十七条 对于违反法律、法规，造成国家、学校和个人

损失的，学校将依法配合公安、网信等主管部门进行处理。

第七章 附 则

第四十八条 本管理办法为校内网络安全建设的基本规定，校内其他网络安全相关规定应以本管理办法为依据，如有相悖之处以本管理办法为准。

第四十九条 本管理办法由网信办、信息办负责解释。

第五十条 本管理办法自发布之日起施行。