上 海 市 浦 东 新 区 教 育 局 文 件

浦教办〔2023〕30 号

关于印发《浦东新区教育局网络与信息安全管理实施办法（修订版）》的通知

各单位：

现将《浦东新区教育局网络与信息安全管理实施办法（修订版）》印发给你们，请认真学习，按照执行。2021 年 10 月 18 日浦教办〔2021〕45 号《浦东新区教育局网络与信息安全管理实施细则（修订版）》停止执行。

特此通知。

上海市浦东新区教育局

2023 年 5 月 8 日

浦东新区教育局网络与信息安全管理实施办法
（修订版）

为进一步提升浦东新区教育单位网络与信息安全防护与保障能力，依据《中华人民共和国网络安全法》《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》等相关法律法规和上级有关要求，制定本办法。本办法适用浦东新区教育局所管辖的各教育事业单位。

第一条 网络接入管理

浦东各教育事业单位均须统一接入浦东教育城域网，统一互联网出口。

各教育事业单位须按浦东教育网络接入标准与规范，配置网络与信息安全相关设施设备，并统一纳入浦东教育网络监控管理体系，同时做好终端接入安全管理。

接入单位的互联网信息系统须使用浦东教育城域网域名，向互联网开放的信息系统须履行公安备案手续，同时做好信息系统的安全等级保护工作。

确有需要建有其他互联网出口的，不得将其他互联网出口用于提供网络服务。

第二条 安全运行管理

各教育事业单位须做好网络安全防护措施，保障单位网络与

信息系统安全运行。

各教育事业单位须落实网络与信息安全责任制，加强信息系统的信息发布审核管理，加强对信息系统的网上互动栏目的监管，确保本单位信息系统的数据安全，每学期至少对本单位的网络和信息安全组织一次自查工作。

教育信息中心对浦东教育城域网进行实时监控，一旦发现接入单位网络与信息系统有异常情况，将采取相关技术手段保障全区教育网络的正常应用；对各教育事业单位的网络与信息系统的安全状况进行定期抽查与检测，对未履行合规性手续、存在高风险安全漏洞的信息系统将采取关闭互联网访问等技术措施。

第三条 应急与保障管理

各教育事业单位须建立网络与信息安全应急预案，一旦发生网络与信息安全重大事件，及时处置并报告教育局信息化办公室。

各教育事业单位须落实专人负责本单位的网络与信息安全管理工作。单位的网络与信息系统安全若采取外包服务的，按有关规定选择专业技术服务公司、签订安全承诺书。网络与信息安全工作纳入对各单位的年度绩效考核、评估和督导范围。

附件：浦东新区教育局网络与信息安全管理实施细则

附件

浦东新区教育局网络与信息安全管理实施细则

目录

第一章　总则

为全面提高浦东教育系统网络与信息安全意识，建立健全浦东教育系统网络与信息安全工作的组织体系、管理规章和责任制度，提高各教育事业单位网络与信息安全管理能力、安全防护水平和安全技术能力，打造浦东新区高速、安全、稳定的教育网络环境，依据《中华人民共和国网络安全法》《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》《中华人民共和国突发事件应对法》《计算机信息网络国际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》《信息安全技术网络安全等级保护基本要求》等有关法律法规的相关要求，结合浦东新区教育信息化实际，制订本管理细则。浦东新区各教育事业单位的网络与各类信息系统的建设、使用和运维，以及网络与信息安全保障的各项工作，适用于本细则。

各教育事业单位的网络与信息安全工作遵循“谁主管谁负责，谁建设谁负责，谁运营谁负责”的原则，严格执行国家网络与信息安全法律法规、政策和标准规范，依照本细则落实本单位的网络与信息安全工作，做到网络与信息安全和信息化工作协调一致、齐头并进，同谋划、同部署、同推进、同实施，内容与技术并重、管理与技术并举。

第二章　职责与分工

浦东新区教育局信息化办公室（以下简称：信息办）负责统筹协调浦东新区教育网络与信息安全工作，研究制定浦东教育网

络与信息安全规划和政策。

浦东新区大数据中心教育局分中心（以下简称：信息中心）负责浦东教育城域网基础设施与区级教育信息化平台的建设与管理，研究制定教育信息化相关技术标准和规范体系，指导各教育单位网络与信息安全建设与管理，对各单位的网络与信息安全运行情况开展技术监测、检测、预警、防护和应急处置工作。

各教育事业单位法人是本单位网络与信息安全的第一责任人，全面负责本单位网络与信息安全工作。各教育事业单位要自主做好本单位的网络与信息安全工作，须设立网络与信息安全管理工作小组，明确网络与信息安全责任主体，建立网络与信息安全制度，并严格落实各项制度与要求。

第三章　网络基础服务管理

浦东教育城域网是由区级数据中心、网络链路以及区内各类教育机构网络所构成的软硬件集成系统，以全区中小学校、幼儿园、职校等教育事业单位为主要组网单位，实现互联网访问、财务管理、视频监控、电子巡考等业务专网，形成多业务承载的浦东教育信息化基础环境。

浦东教育城域网络基础服务主要有：网络接入、域名发布、云资源服务、统一运维平台等。

一、网络接入

浦东新区所有教育事业单位均须统一接入浦东教育城域网，统一互联网出口。各教育事业单位接入、停用或变更教育城域网

均须向信息中心申请及备案。光纤接入和光纤线路租赁费用由各接入单位依照有关资费标准进行支付。

接入单位的内部网络 IP 地址段由信息中心统一进行分配和管理，原则上一家接入单位只分配一个公网 IP。接入单位应严格遵循浦东教育城域网统一规划要求进行内部 IP 地址的配置。

接入单位须配置专用接入交换机、网络防火墙、上网行为审计、防病毒、日志审计等网络安全设备和系统，不具备上述基本网络安全要求的单位一律不允许接入浦东教育城域网。如使用信息系统，须按照信息系统等级保护要求配备 Web 应用防护、防篡改等安全设备和系统。

二、域名发布

信息中心负责浦东教育城域网信息系统的域名发布工作。接入单位可根据实际教育需求向信息中心提出域名发布申请。注销与停用也须向信息中心备案。

接入单位对外发布的信息系统，必须使用浦东教育城域网*. pudong-edu. sh. cn 或*. pdedu. sh. cn 的域名。

三、云资源服务

浦东教育城域网为有合理需求的接入单位提供免费的浦东教育云资源服务，主要包括：云主机、网站群服务等。

各教育事业单位可采用浦东教育云资源服务方式进行单位门户网站建设，信息中心统一部署、统一运维管理，使用单位须负责信息管理。

云资源服务的日常管理由信息中心和使用单位共同负责，信息中心保障云资源的物理安全和网络联通，使用单位须按照浦东教育云资源使用管理要求进行规范使用。

四、网络运维平台

为了高效开展教育网络与信息系统运维和安全管理，建设了浦东教育城域网统一运维管理平台（以下简称“运维平台”，网址：http://ywzx.pdedu.sh.cn/）。

运维平台主要服务内容包括：网络与信息安全通告、应用系统（网站）开通申请、云资源服务申请、网络与信息安全扫描申请等。各教育事业单位须按《浦东教育城域网应用服务指南》进行申请。

接入单位网络管理员应每天登录运维平台关注相关信息，及时处理下发的相关报告与通知。

第四章　信息系统管理

一、信息系统备案

对接入互联网的信息系统，各教育事业单位须履行公安备案和事业单位挂标手续。各教育事业单位使用非教育城域网的互联网信息系统，还须同时履行工业与信息化部的备案手续。

使用移动互联网应用（APP）的单位，须按照市教委相关要求落实 APP 使用者备案工作。

二、信息系统安全等级保护

各教育事业单位应当依据教育部《教育行业信息系统安全等

级保护定级工作指南》《信息安全技术网络安全等级保护基本要求》以及公安部相关文件确定信息系统的安全保护等级，完成等级保护定级备案和测评工作。

各教育事业单位应当根据上海市公安局要求选择具有相关资质的测评机构，按照等保的相关要求对信息系统安全等级状况开展等级测评。经测评信息系统安全状况未达到安全等级保护等级要求的，各教育事业单位应制定方案进行整改，直至通过。

三、信息系统定期登记

各教育事业单位须严格执行信息系统定期（每学期一次）登记制度。各教育事业单位须在运维平台及时更新本单位信息系统的相关信息，确保登记信息的准确性。

四、“双非”与“单非”信息系统要求

“双非”系统是指不使用浦东教育城域网域名和 IP 对外发布的信息系统。“单非”系统是指仅使用浦东教育城域网的域名或 IP 对外发布的信息系统。

接入教育网的各教育事业单位不得使用“双非”或“单非”信息系统。教育局自 2025 年起，对使用“双非”或“单非”信息系统的运维项目信息化项目不再进行备案审批。

第五章　安全运行管理

一、安全防护

各教育事业单位应做好本单位信息系统及各类计算机终端的安全工作。加强落实防范网络攻击、网络侵入、网页被恶意篡

改等技术措施，及时查找和修补系统漏洞，定期做好应用系统及数据备份工作。

须确保各类计算机终端安装防病毒软件，每月及时进行系统的补丁更新和病毒库更新，如发现病毒感染，第一时间断网，避免病毒扩散，并及时进行病毒查杀。

严禁在教育网内使用来历不明、引发病毒传染的软件及文件，对外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

二、信息内容安全

各教育事业单位应建立信息发布审核管理制度，对外发布的信息由本单位相关负责人审核批准后发布，并做好审核记录存档工作。

各教育事业单位的信息系统、APP、微信公众号、微博、重点区域展示屏等发布、转载的信息应当遵守国家的法律、法规、规章和相关政策。不得发布、转载含有危害国家安全和社会稳定的不良信息，以及涉及国家秘密、暴力和色情等内容。

各教育事业单位的信息系统若有网上互动栏目，则应加强对网上互动内容的监管，做好栏目信息安全监控，发现问题应及时处置和上报，确保信息内容安全。

各教育事业单位应当对其收集的用户信息严格保密，并建立健全用户信息保护制度，不得泄露、出售或者非法向他人提供。如涉及第三方服务，需要与服务方签订信息安全协议，明确各主

体的安全职责，确保本单位信息系统的数据安全。

三、安全自查与整改

各教育事业单位应建立健全自查工作机制，组织建立自查工作小组，明确具体工作职责。每学期至少对本单位的网络和信息安全工作进行一次严格的自检自查工作，自查内容和要求包括：

1.网络与信息安全工作的各项制度。各教育事业单位应自查是否落实网络与信息安全工作责任制，建立健全网络与信息安全的各项管理制度，具体包括网络与信息安全管理制度、安全岗位管理制度、系统操作权限管理制度、户外大屏管理制度、安全培训制度、用户管理制度、新服务与新功能安全评估、信息发布审核、个人电子信息安全保护制度、安全事件监测、报告和应急处置制度、用户投诉举报处理等。各项管理制度要明确具体责任人，并由专人严格落实各项工作。

2.信息系统信息内容保密检查。各教育事业单位要高度重视信息系统信息公开保密审查工作，严格执行信息公开保密审查制度，落实保密审查责任。对本单位的信息系统、微博、微信公众号、APP 等系统中发布的信息内容定期检查，检查是否违规刊登、处理、传输敏感信息；对刊登、转载上级的文件和信息要逐一核对原件，检查是否涉密；对涉及招生、考试、学籍、教师、邮件等重要数据信息的信息系统（含网站）定期开展网络安全风险隐患排查和安全加固工作。

3.重要网络设备的规范接入。各教育事业单位要严格自查学

校网络机房中核心网络设备，如防火墙、交换机、上网行为管理、Web 应用防护等设备的接入情况和使用情况，确保核心网络设备在线正常运转。

4.信息系统安全自查整改。各教育事业单位对本单位信息系统及所部署的服务器主机的安全状态、安全防护措施落实情况进行自查，特别对信息系统后门植入、网页篡改、主机漏洞的防范措施情况进行排查，对自查中发现的安全隐患和漏洞，立即予以整改。信息系统如发生升级改版等情况，须在运维平台申请信息系统和主机的安全扫描，经检测安全后再对互联网开放。对新建信息系统，开发过程中要遵循安全规范，在未通过安全扫描、正式运行之前不得对外发布。

5.户外大屏播控主机的安全措施。户外大屏的播控主机须放在安全区域由专人保管，避免无关人员非授权控制显示屏，严禁接入互联网，须设置登录密码，定期对主机的操作系统打补丁和查杀毒，日志留存不少于六个月，发布的信息经相关负责人审核后由专人发布。

6.排查“僵尸”系统、废弃页面。各教育事业单位对发现的“僵尸”系统和废弃页面采取立即下线操作处理。对未开展信息系统备案、未通过安全检测或者无能力完成整改的信息系统，应立刻关闭，待完成备案、整改无漏洞后方能上线。排查不再使用的域名。各教育单位如存在已经不再使用的域名，要及时履行域名注销手续（包括但不限于公安部网站备案注销、事业单位标识

注销、工信部 ICP 备案注销）。

7.各类计算机终端的安全防护措施落实情况。具体包括办公室、多媒体教室、图书馆等区域的各类计算机终端。各类计算机终端须设置操作系统补丁、防病毒软件和病毒库自动升级，定期查杀毒。不允许在计算机终端上私自设置无线热点。

8.日志留存情况。防火墙、上网行为设备、服务器操作系统、应用系统等设备和系统的日志留存须不少于六个月，定期对各类日志进行备份。

9.全面排查弱口令。具体排查内容包括防火墙、上网行为设备、服务器、信息系统、户外大屏播控主机、所有教师用机、班级教室计算机等设备和信息系统的登录口令，设置至少 8 位且包含大小写字母、数字和特殊字符的登录口令。建议登录口令更换周期为三个月，以确保信息的安全。

10.网络安全工作台账。所有的网络与信息安全工作要建立完整、规范的工作台账，各项安全工作要留痕。具体台账内容包括网络拓扑图、计算机电脑与 IP 对应表、机房进出登记日志和使用记录、网络与信息安全日常巡检记录、网站与计算机终端安全自查与整改记录、安全培训开展情况、信息发布审核记录、外包公司运维服务记录等。

第六章　应急与保障管理

一、安全责任制度

各教育事业单位应提高网络与信息安全意识，落实网络与信

息安全负责人员和各项制度。网络与信息安全的日常运行及维护由各单位具体负责，须按照网络运维管理要求做好本单位网络运维工作。

各教育事业单位应将重要活动、重要会议、重大节假日等设为网络与信息安全的重要保障期。重要保障期内，单位主要领导应靠前指挥，重点部门、重要岗位应建立 24 小时值班制度。

二、安全应急预案与处理

网络与信息安全事件是指出现业务中断、系统破坏、数据破坏、信息失窃或泄密等，从而对社会稳定、学校和公众利益等方面造成不良影响以及造成一定程度直接或间接经济损失的事件，如黑客攻击、网站被黑、大规模的病毒发作、网上的有害信息与黄色信息泛滥等。

各教育事业单位应建立重大网络与信息安全事件处置和报告制度，建立网络与信息安全应急预案，明确应急处置流程和权限，落实应急处置技术支撑队伍，应急联系人须保持手机 24 小时畅通，定期开展安全应急演练并做好应急演练记录，提高网络与信息安全应急处置能力。

各教育事业单位应加强监测，一旦发现本单位发生重大网络与信息安全事件的，须立即启动应急预案实施处置，第一时间断网，先消除影响，同时保存好相关日志记录，并在 30 分钟内上报信息中心和浦东公安分局网安支队。

三、安全服务外包

各教育事业单位的网络与信息系统若采取安全服务外包的，按有关规定选择专业技术服务公司，并做好对技术服务公司的管理工作，与外包公司签订安全承诺书，确保代码安全、数据安全。

四、安全宣传培训

各教育事业单位应积极配合“网络安全宣传周”等宣传活动工作，不断加强区教育系统网络安全知识宣传教育，提高网络安全意识，切实维护国家网络安全和人民群众的合法权益。各单位网络与信息安全相关人员需定期进行网络安全法规学习并参与网络安全知识、技术培训。

各教育事业单位每学期至少开展一次以上的知识讲座、论坛、主题班会等形式多样的网络安全宣传教育活动，宣传网络安全知识、强化网络安全意识。

第七章 网络安全监管

一、信息安全专项检查

教育局将不定期进行网络与信息安全专项检查。检查发现信息系统安全保护状态不符合信息安全等级保护有关管理规定和技术标准的、未落实安全自查与整改工作的将会向有关单位发出整改通知。各教育事业单位要根据整改通知要求尽快完成整改，并将整改报告递交至信息办。半年内被相关部门通报 2 次的单位，一年内将不再对该单位提供信息系统互联网开通业务。

二、设备监控

为保障教育城域网整体正常运行，接入单位的接入交换机、网络防火墙和上网行为管理等设备须统一纳入信息中心监控管理体系。接入单位不得私自绕开或关闭网络防火墙，一经发现此类情况，信息中心将采取断开该单位接入教育城域网的措施。

三、安全监测与检测

1.信息中心对接入单位网络运行情况、信息系统的安全运行情况进行日常监测分析，实时监控各单位网络安全运行状况。一旦发现接入单位网络有异常情况，及时采取相关技术手段保障全区教育网络的正常应用。

2.信息中心对接入单位的各类计算机终端（包括服务器、教师和学生用机、移动终端）进行实时安全监测，监测内容包括主机病毒、木马、恶意通讯等主机安全威胁状况。一旦发现主机安全问题，将采取主机隔离教育网的措施，保障教育网主机安全运行。

3.信息中心定期对各教育事业单位的信息系统开展安全检测（区域信息系统每月一次，基层单位信息系统每两月一次），检测报告通过运维平台发送至各单位。相关单位应根据检测报告要求及时进行整改。

4.对监测与检测出的存在高风险安全漏洞、未履行合规性手续的各类信息系统、存在病毒木马的教育网内的主机，将采取以下技术措施：

（1）有高风险安全漏洞的信息系统，一经发现，立即关闭互联网访问功能。

（2）对互联网发布的浦东教育城域网内的信息系统未履行备案相关手续的单位，一经查出，将关闭互联网访问功能。

（3）信息系统出现安全漏洞，整改复查过程中若采用临时页面或非真实部署主机等方式来应付扫描检查行为的，一经发现，一年内将不再为该单位提供信息系统互联网开通业务。

（4）发生严重影响教育网信息安全的事件，例如：信息系统被挂载反动、恐怖、涉毒、涉黄、涉赌页面；发生重要信息泄露；网站、论坛、博客中发布不良言论；单位内主机存在对外恶意攻击行为，影响教育城域网正常运行。如发生以上任一情况，将立即切断该单位浦东教育城域网接入。

四、安全考核评估

网络与信息安全工作纳入各教育单位的年度绩效考核、评估和督导范围。

对网络与信息安全工作中表现突出的集体和个人将给予表彰和奖励，对相关人员的工作量应在各单位的绩效工资中予以体现。对发生网络安全事件、未按要求落实网络与信息安全工作要求、被通报后未及时整改的单位，绩效考核、评估和督导中予以减分，情节严重的，将予以一票否决处理。

对迟报、谎报、瞒报、漏报重大网络安全事件或者在应急管理工作中有失职、渎职行为的，依照有关法律法规对单位和有关

责任人给予处分或者处罚，情节严重的，将由公安部门依法追究民事和刑事责任。

第八章 附则

本管理实施细则如与其他上级文件相关要求有出入，以上级文件要求为准。

本管理实施细则自印发之日起执行。

上海市浦东新区教育局党政办公室　　2023 年 5 月 8 印发

（共印 5 份）