上 海 海 洋 大 学 文 件

沪海洋〔2023〕39 号

关于修订印发《上海海洋大学校园网络安全管理规定》的通知

各学院（部）、各处室、各直属单位：

为加强学校网络系统安全管理工作，确保校园网的正常运行，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国计算机信息系统安全保护条例》等文件，经 2023 年 12 月 5 日第 33 次校长办公会通过，现将修订后的《上海海洋大学校园网络安全管理规定》予以印发，请遵照执行。

附件：上海海洋大学校园网络安全管理规定

上海海洋大学

2023 年 12 月 28 日

附件

上海海洋大学校园网络安全管理规定

第一章 总则

第一条 为加强学校网络系统安全管理工作,确保校园网的正常运行，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》《计算机信息系统保密管理暂行规定》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国计算机信息网络国际联网管理暂行规定》，特制定本规定。

第二条 校园网络,是指校园范围内连接各种信息系统及信息终端，为广大师生员工提供网络服务的计算机和通信网络，包括校园有线网络、无线网络和各种虚拟专网，包括公务网、财政专网、一卡通专网等。

第三条 信息化管理办公室（以下简称“信息办”）在上海海洋大学网络安全和信息化领导小组（以下简称“网信领导小组”）指导下，负责制定网络安全管理制度。

第四条 现代信息与教育技术中心(以下简称“现教中心”)在网信领导小组指导下负责具体的网络安全运行管理工作，负责：

一、学校网络安全管理工作，制定符合学校实际情况的实施细则，并建立健全网络安全管理的各项措施；

二、做好学校安全及保密教育工作，做好用户信息的管理，保障数据与信息安全；

三、建立健全与各学院、部门网络安全联络员、服务器管理员的网络安全联动机制，及时发布涉及网络及信息安全的通知公告并提供网络安全维护方面的培训及技术指导；

四、协助宣传部做好网络信息内容的安全管理；

五、协助保卫处查处利用校园网进行的各种违纪、违法行为。

第五条 各学院、各部门负责人为本单位的网络安全第一责任人，在网信领导小组领导下对本部门的网络安全负责并按本制度落实网络安全工作。

第六条 各学院、各部门设立一名网络安全联络员，负责协调和执行本部门的网络安全工作，传达上级部门、学校最新安全政策、指导和要求，并监督实施情况。

第七条 服务器管理员是负责所属服务器的日常安全管理的关键角色，需要维护服务器的硬件和软件，确保其处于最新的安全状态。服务器管理员还需要实施访问控制和权限管理，以保护服务器上的数据和应用程序。

第八条 校园网用户应遵守国家法律及校园网络安全规定，不得泄露个人身份信息或敏感数据，并采取适当的措施来保护自己的账户和设备，包括定期更改密码、安装和更新防病毒软件等。

发现异常网络情况或网络安全问题，应积极报告给所在学院、部门网络安全联络员或现教中心，协助维护校园网络的整体安全。

第二章 校园网络公共平台安全管理

第九条 校园网络公共平台是在校园内提供网络连接和网络管理服务的综合平台，主要为网络设备、安全设备、监控设备、声像设备、用户终端提供准入控制、网络连接、地址分配等服务。

第十条 为规范学校校园网络建设，有效实现资源集成和共享，本着“统一规划、统一标准、统一平台”的原则，学校实行校园网络公共平台准入制度。

第十一条 校园网络各建设内容，须符合学校信息化建设总体规划及网络安全要求。未经信息办审批，任何部门和个人不得擅自对外开展通信业务（含短信平台、手机移动通信等）。

第十二条 为加强系统集成和共享，各部门接入校园网络的网上共享设备和系统软件（如服务器、网络交换机、网络存储设备、操作系统、数据库系统等），须符合校园网络安全管理要求。

第三章 网络运行安全

第十三条 除现教中心外，其他单位或个人不得以任何方式试图登入校园网主、辅节点、服务器等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施；不得切断学校、部门或他人网络的连接。

第十四条 各学院、各部门新申请接入校园网络，如需网络布线，应提交方案，由现教中心审核。

第十五条 校园内从事施工、建设时，不得危害校园网络系统的安全。校园网络主节点及二级节点所在单位必须保证节点设备 24 小时正常运行，不得以任何理由关闭有关设备或电源。

第十六条 任何单位和个人不得以不真实身份使用网络资源，不得窃取他人账号、口令使用网络资源,不得盗用未经合法申请的 IP 地址入网；任何单位或个人不得擅自向运营商开通网络或通信服务。

第十七条 对于非必要开放互联网访问的校内信息系统,应通过 VPN 进行访问；开放互联网访问的网站及系统，应按照“谁主管谁负责、谁建设谁负责、谁运行谁负责”的原则，落实网络安全主体责任。

第十八条 任何个人或单位网络使用者不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动，不得使用任何非法手段获取他人信息。

第十九条 各学院、各部门对其管理下接入我校网络的第三方单位，应当加强网络安全管理，落实人员网络准入备案，真实详尽记录各联网计算机的使用者和使用时间，并保留半年以上。

第二十条 接入校园网络服务器必须保持系统日志记录功能，历史记录保持时间不得低于 6 个月。现教中心按照上级主管部门规定，检查各服务器的系统日志。

第二十一条 现教中心负责已申请备份服务的校级数据和信息系统备份与恢复工作，制订备份与恢复计划。各学院、各部

门根据业务需要自行对数据和信息系统进行备份，定期测试备份与恢复计划，并确保备份数据和备用资源的有效性。

第四章 网络设备安全

第二十二条 网络设备主体责任人应定期检查和更新网络设备安全补丁和固件，包括操作系统、网络设备固件、应用软件等。及时应用厂商发布的安全补丁，修复已知的安全漏洞，确保网络设备处于最新的安全状态，防范潜在的网络攻击。

第二十三条 规范网络设备访问权限管理措施，限制只有授权人员能够访问网络设备的配置和管理界面。设立审批机制，对网络设备的配置和管理进行记录和审计，防止未经授权的人员对网络设备进行未授权的访问和操作。

第二十四条 网络设备主体责任人应修复网络设备存在的漏洞，包括但不限于安装厂商发布的安全补丁、更新固件、修改配置等。对于无法修复的网络设备，立即下线并下架，避免存在未修复的安全漏洞，从而降低网络攻击的风险。

第二十五条 网络设备负责人应及时与现教中心联系，对其所负责的不再使用的网络设备进行停用、下线和下架，避免这些设备成为潜在的安全漏洞。

第二十六条 网络设备主体责任人应建立完善的网络设备管理档案，包括网络设备的基本信息、购置和更新记录、安全补丁和固件的更新记录、维护和检修记录等。定期对网络设备管理档案进行审查和更新，确保网络设备管理的全面和规范。

第五章 安全教育与培训

第二十七条 现教中心负责在校园网上设立网络安全知识专栏，发布国家、本市和学校的网络安全管理办法、规定和有关制度。

第二十八条 现教中心负责对各学院、各部门网络安全联络员进行安全教育和技术防范培训。

第六章 义务与责任

第二十九条 入网用户有遵守国家法律、行政法规，严格执行安全保密制度的义务和责任；有举报危害国家安全、泄露国家秘密等违法犯罪行为的义务和责任。

第三十条 对知情不举报者，由于泄密造成危害或重大危害的，要在对泄密者追究责任的同时，依据有关法律、法规和有关规定由相关部门给予相应处罚。

第三十一条 如发现互联网泄露国家秘密的情况，现教中心和用户应立即采取补救措施，并同时向有关部门报告。

第三十二条 违反下列行为之一者，现教中心可向所在单位提出警告，停止其网络使用。如造成损失或影响严重的，由学校保卫处依照有关法律、法规及校纪校规进行处理，情节严重者移交公安机关处理。

一、查阅、复制或传播下列信息： ①煽动抗拒、破坏宪法和国家法律、行政法规实施；②煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；③捏造或者歪曲事实，散布谣言

扰乱社会秩序；④公然侮辱他人或者捏造事实诽谤他人的；⑤宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等；⑥损害学校形象和学校利益的；⑦其他违反宪法和法律、行政法规的。

二、破坏、盗用计算机网络中的信息资源和危害计算机网络安全的活动的；

三、盗用他人账号或 IP 地址的；

四、私自转借、转让用户账号的；

五、故意制作、传播计算机病毒等破坏性程序的；

六、不按国家和学校有关规定擅自接纳网络用户的；

七、上网信息审查不严,造成严重后果的；

八、使用任何工具破坏网络正常运行或窃取他人信息的。

第七章 附则

第三十三条 本规定由信息办负责解释。

第三十四条 本规定自公布之日起执行，原《上海海洋大学校园网入网用户守则》《上海海洋大学校园通信网络管理办法》《上海海洋大学校园网络安全管理规定》同时废止。

上海海洋大学办公室 2023 年 12 月 28 日印发