上海海洋大学校园网络安全管理规定

(沪海洋〔2018〕23 号　2018 年 10 月 16 日)

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》、《中华人民共和国计算机信息网络国际联网管理暂行规定》，特制定本规定。

一、 组织机构

1． 成立上海海洋大学校园网络安全管理领导小组，该小组由分管校领导和校办、宣传部、保卫处、现代信息与教育技术中心等部门负责人组成，负责制定有关校园网安全管理的制度、措施；召开专项会议；负责贯彻落实上级有关管理部门的政策和规定；负责对校园网的使用和管理进行监督检查。

2． 现代信息与教育技术中心在校园网络安全管理领导小组指导下负责具体的网络安全运行管理工作，并指定专人作为网络安全专管员，负责：(1) 负责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；(2) 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；(3) 及时发布涉及网络及信息安全的通知公告，提供一定的系统安全保障方法及工具，并对各单位的网络安全工作小组的网络信息安全员提供网络安全维护方面的培训及技术指导；(4) 协助宣传部做好网络信息内容的安全管理；(5) 协助保卫处查处利用校园网进行的各种违纪、违法行为。

3． 各学院、各部门安排一名处级负责人为本单位的网络安全第一责任人，在校园网络安全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。同时，各单位设立 1 名网络安全员，具体负责本部门的网络安全工作。

4． 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。(如公务网、财政专网、一卡通专网等)

二、 校园网络公共平台准入和安全管理

1． 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。

2． 校园网络包括校园计算机网络、无线网络、各类专网等。校园网络各建设内容，须符合学校信息化建设总体规划。未经学校校园网络安全管理领导小组审批，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)。

3． 为加强系统集成和共享，各部门购买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)，须符合校园网络的接入标准，立项前应办理审批手续。

三、 网络安全运行

1． 除现代信息与教育技术中心外，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。

2． 各部门新申请接入校园网络，如需网络布线，应先办理审批手续。为确保校园网络安全、便于建成后运行维护，新布线工程完工后应提交施工图和测试报告，并经验收合格后方可接入校园网络。

3． 校园内从事施工、建设时，不得危害校园网络系统的安全。校园网络主结点及二级结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。

4． 未办理入网手续，任何单位和个人不得非法私自将计算机等终端接入校园网络，不得以不真实身份使用网络资源，不得窃取他人帐号、口令使用网络资源, 不得盗用未经合法申请的 IP 地址入网；未经许可，任何单位或个人不得擅自向运行商开通网络或通信服务

5． 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帐户及口令的侦听、盗用活动，不得使用任何非法手段获取他人信息。

6． 由现代信息与教育技术中心采取必要措施，防止“黑客”的攻击，堵塞隐患漏洞，清除互联网中不健康的内容。

7． 校内接入单位应当建立健全网络安全管理制度，建立备案制度，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。

8． 经学校网络安全领导小组批准开设的服务器必须保持日志记录功能，历史记录保持时间不得低于 6 个月。现代信息与教育技术中心按照上海市公安局

的有关规定，不定期地检查各开通服务器的计算机日志。

9． 校园网主、辅节点设备、连接线路及服务器等发生破坏案件后，现代信息与教育技术中心必须及时向校保卫部门及公安机关报告。

四、 信息系统数据安全管理

1． 信息系统数据是指信息系统收集、存储、传输、处理和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、日志记录等。

2． 信息系统数据的所有者是数据安全管理的责任主体，应当落实管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。

3． 信息系统数据收集应遵循“最少够用”原则，不得收集与信息系统业务无关的个人信息。按照“谁收集，谁负责”的原则，收集个人信息的部门是个人信息保护的责任主体，应当对其收集的个人信息严格保密。

4． 现代信息与教育技术中心负责学校关键信息系统的备份与恢复工作，制订备份与恢复计划，根据业务实际需要对重要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。

五、 信息安全管理

1． 网络用户必须遵守《计算机信息网络国际互联网安全保户管理办法》。

2． 校园网及子网站的系统软件、应用软件及信息数据要实施保密措施。信息资源保密等级可分为：1)可向 Internet 公开的；2)可向校内公开的；3)可向本系（单位）公开的；4)可向有关单位或个人公开的；5)仅限于本单位内使用的；6)仅限于个人使用的。

3． 校园网中对外发布信息的 WWW 服务器中的内容必须按照《上海海洋大学校园网站管理办法》的有关规定，由专人负责，审核后方能发布。

4． 未经学校网络安全领导小组允许，任何单位或个人不得开设代理服务器、邮件服务器等，不得在主页上开设交互式栏目，不得设立游戏站点或纯娱乐性站点，一经发现，即从网上隔离，并要追究有关人员的责任。

5． 任何部门和个人使用校园网提供的 INTERNET 服务和电子邮件服务等必须与网络中心签订相应协议。

6． 校园网的所有用户有义务向网络安全管理人员或有关部门报告违法犯罪行为和有害的、不健康的信息，并协助有关部门进行调查。校网络安全小组应不定期检查校园网络信息发布的内容，督促现教中心和各部门对有害信息进行清

除和备份。现教中心建立备案制度，记录来自校园网络内部和外部的可疑行为，记录保存半年以上。

7． 校园网接入单位和用户须遵守知识产权的有关法律法规。

8． 严禁在校园网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用公安部门推荐的杀毒软件检查、杀毒。

六、 安全教育与培训

1． 网络安全教育与培训工作由现代信息与教育技术中心具体负责。

2． 现代信息与教育技术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。

3． 入网单位和个人必须依据有关规定，签订网络安全的有关协议，接受安全教育和培训。

4． 现代信息与教育技术中心负责对各院、部、处级计算机网络安全专管员和网络安全员的安全教育和技术防范培训。

七、 义务与责任

1． 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。

2． 对违反法律、行政法规和有关规定的，由安全保密工作部门和公安机关分别依据职权范围，依据有关法律进行处罚。构成犯罪的，依法追究刑事责任。

3． 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。

4． 如发现互联网泄露国家秘密的情况，现代信息与教育技术中心和用户应立即采取补救措施，并同时向有关部门报告。

5． 违反下列行为之一者，现代信息与教育技术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。

(1) 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。

(2) 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。

(3) 盗用他人帐号或 IP 地址的;

(4) 私自转借、转让用户帐号的;

(5) 故意制作、传播计算机病毒等破坏性程序的;

(6) 不按国家和学校有关规定擅自接纳网络用户的;

(7) 上网信息审查不严, 造成严重后果的;

(8) 使用任何工具破坏网络正常运行或窃取他人信息的。

八、 本规定自公布之日起执行，由现代信息与教育技术中心负责解释。