安徽信息工程学院网络安全管理办法

第一章 总则

第一条 为保障安徽信息工程学院计算机网络设备、信息和运行环境的安全，依据《中华人民共和国网络安全法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》等法规，制定本办法。

第二条 学校对校园网站实行分级管理。由宣传部负责校园网站统一规划、管理、监督和考核；网站开发技术单位负责提供统一的网站构建技术平台、网站运行的技术支持及日常维护。二级单位负责校园网站内容发布、审核及下属网站的形式、运行。

第三条 各单位、部门需对本单位师生进行信息安全和网络安全教育。

第四条 安徽信息工程学院计算机网络用户须遵守国家有关网络安全法规，须接受国家有关部门及学校智慧校园建设办公室依法进行的网络安全监督检查，有义务向智慧校园建设办公室和有关部门报告违法上网行为。

第二章 计算机网络管理

第五条 外网的开通和使用，实行方便工作和保障安全相结合原则。申请访问外网的方式可采用如下方式：

登录信息门户在“业务流转中心”填写安徽信息工程院校园网 VPN 申请，经学院、部门领导同意，报智慧校园建设办公室审核，办理开通事宜。

第六条 校内资源未经审批禁止外部网络访问，如需外部网络访问，须在信息门户业务流转中心填写安徽信息工程学院资源端口开放申请，并报智慧校园建设办公室审批。此端口开放后，智慧校园建设办公室会定期对业务系统进行检查，检查反馈问题使用单位应配合整改，若因使用单位整改不到位产生的安全问题由申请单位安全负责人负责。

第七条 任何单位和个人不得擅自安装、拆卸或改变主要网络设备，不得未经批准擅自更改计算机系统设置国际互联网，施工不得危害计算机网络系统安全。

第八条 上网人员要自觉接受身份认证和 IP 绑定技术对个人上网活动的安全监督检查，严禁擅自改动分配的 IP 地址。

第九条 网络教室、网络机房等接入校园网的环境，不对社会开放。

第十条 涉密及特殊岗位用户计算机应根据学校要求安装保密部门认可的违规上互联网监控软件。

第十一条 严禁在内部专网计算机上使用无线网卡、键盘、鼠标、蓝牙等一切无线设备，连接手机、相机、USB 存储介质等一切非授权的可存储或连接其他网络的外置设备。

第十二条 严禁在校园网及其连网计算机上浏览反动、淫秽等国家明文禁止的信息。

第十三条 内网安全与应用支撑平台的建设，实行内网用户、资源的统一注册管理，并为单位信息系统的安全和安全域防护提供身份鉴别、授权管理、便捷防护等公共安全技术手段。

第十四条 网络管理员负责网络拓扑图的绘制。若网络结构发生变化要及时更新拓扑图，确保网络拓扑图完整、真实。

第十五条 任何人不得擅自改变网络拓扑结构、网络设备布局、服务器和路由器配置以及网络参数。

第三章 信息安全管理

第十六条 校园网内办公计算机须启用屏幕保护程序并设置恢复密码，应用系统应设置密码并定期修改，屏幕保护的闲置时间设置为 10 分钟以内，密码长度不少于 8 位，由字母、数字和特殊字符混合组成。

第十七条 校园网内办公计算机不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。对便携式和移动式设备需提前进行杀毒，确认安全后方可接入网络。

第十八条 系统管理员不得泄露应用系统中用户的帐号、口令和信息数据，需对校园各网络设备、服务器、应用系统的账号口令进行定期更新，周期为三个月。

第十九条 对有涉密要求的计算机应接入互联网，应采取双布线双用户终端，双布线单用户终端，物理隔离卡的方式进行物理隔离，严禁在外网计算机上处理涉密文件和敏感工作信息。

第四章 数据安全

第二十条 内网信息系统利用公网（PSTN、ISDN、ADSL、DDN、X. 25、帧中继、ATM、SDH 等）进行远程传输时，必须使用 VPN 技术。

第二十一条 内外网因工作需要数据进行交换时，必须采用符合国家保密部门要求的方式（如：刻录光盘）或设备（如：保密部门认可的安全移动存储介质管理系统）。

第二十二条 不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

第二十三条 内外网网络之间要实行物理隔离。如需进行数据交换时，应使用符合国家政策和保密部门认可的安全产品或技术措施进行数据传输。

第五章 运维安全

第二十四条 网络管理专员负责全校网络及信息的安全工作，及时汇报网络安全事故，解决突发事件和问题。

第二十五条 补丁升级系统、防病毒系统、漏洞扫描系统、网页防篡改系统、存储备份系统、容灾系统统一部署，建立与应用相适应的安全策略，全面加强主机和应用系统安全。

第二十六条 在互联网发布的应用系统须使用网页防篡改技术或专用安全设备进行保护，以便受到破坏时能及时恢复。

第二十七条 内网进行分级、分层、分域管理，对内网信息系统及相关的局域网（业务专网）划分为独立可管理和控制的安全域。不同的安全域应采取相应的安全策略和保护手段。应在数据

中心网络边界部署防火墙、审计系统、IPS/IDS 等安全设备；重要的业务应用服务器区部署单独的防火墙进行保护。

第二十八条 在互联网发布的应用系统须经过有资质的专业信息安全公司或第三方技术机构的安全测评，确保网站的安全性。

第二十九条 任何人不得擅自进入计算机系统更改系统信息和用户数据。

第三十条 任何人不得利用计算机技术侵害用户合法权益，不得制作和传播有害信息。

第三十一条 信息系统核心设备采取冗余措施(包括线路及设备冗余)，确保网络正常运行。

第三十二条 网络、安全设备的管理须采用安全的方式(如加密、SSH 等)，严格控制可访问该设备的地址和网段。

第三十三条 网络系统(服务器、网络设备)须定期进行漏洞扫描，及时修补已发现的安全漏洞。

第三十四条 根据设备厂商提供的更新软件对网络设备和安全设备进行升级，在升级之前需对重要文件的配置进行备份。

第三十五条 定期对重要的网络、安全设备进行巡检，确保重要设施工作正常，并填写相关记录表单归档保存。若在巡检中发现问题要及时上报处理。

第三十六条 校园网须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

第三十七条 部署专用网络审计设备，记录网络访问日志，日志保存期不低于 60 天，且应保证无一天以上的中断。

第六章 附 则

第三十八条 本办法由安徽信息工程学院智慧校园建设办公室负责解释。

第三十九条 本办法自发布之日起施行。