宿州学院文件

校字〔2017〕63号

关于印发《宿州学院网络信息安全管理办法（试行）》的通知

各单位（部门）：

《宿州学院网络信息安全管理办法（试行）》已经2017年10月30日校党委会审议通过，现印发给你们，请认真贯彻执行。

宿州学院

2017年11月13日

宿州学院网络信息安全管理办法（试行）

第一章 总 则

第一条 为加强学校对网络信息安全工作的组织管理，提高网络信息安全防护能力和水平，根据《中华人民共和国网络安全法》（中华人民共和国主席令 第五十三号）、《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）、《信息安全等级保护管理办法》（公通字〔2007〕43号）等国家有关法律、法规对网络信息安全的要求，制定本办法。

第二条 本管理办法所指的网络信息安全，包括网络安全和信息安全两个方面。网络安全是指校园计算机网络的设施设备（包括路由交换、网络传输、服务器、终端、存储介质等）的安全；信息安全是指基于校园计算机网络的各类应用系统以及应用系统承载的数据和内容的安全。

第二章 组织机构与职责

第三条 学校网络信息安全工作由网络安全和信息化建设领导小组统一领导。负责制定学校网络信息安全相关政策，研究处理重大网络信息安全事件，定期召开网络信息安全工作会议，统筹指导学校网络信息安全建设。

第四条 办公室（网络与信息中心）是学校网络信息安全归口

管理、技术支撑单位，负责统筹学校网络信息安全工作。具体职责包括:

（一）制定网络信息安全总体规划，并组织实施;

（二）拟定网络信息安全管理规章制度，组织开展信息安全等级保护工作;

（三）负责学校网络信息安全防护系统的建设、运行维护、技术指导和服务支持;

（四）负责网络信息安全应急管理，协调处理与政府网络信息安全管理部门的关系;

（五）组织网络信息安全宣传和教育培训工作;

（六）学校网络信息安全的其他工作。

第五条 学校各单位负责本单位网络信息安全工作，负责本单位网站等应用系统的建设、管理及安全运维。各单位主要负责人是本单位网络信息安全工作的第一责任人。

各单位应设一名网络信息安全管理员，负责本单位网络信息安全保护措施的落实，对上网人员进行网络信息安全教育和培训，与办公室（网络与信息中心）协同配合，共同做好本单位网络安全运行、管理和维护工作。

第三章 校园计算机网络安全

第六条 校园计算机网络（以下简称校园网）是为学校教学、科研、管理、生活服务的现代化信息基础设施。

第七条 未经批准，任何单位或个人不得将校园网延伸至校外或将校外网络引入至校园内。未经批准，任何数据业务运营商或电信代理商不得擅自进入宿州学院校园内进行工程施工，开展互联网营销业务。

第八条 校园各区域的网络设备，其管理、维护等均由办公室（网络与信息中心）统一负责，未经批准，不得以任何方式试图登录、修改、设置、破坏校园网内的交换机、路由器和服务器等设施。

第九条 办公室（网络与信息中心）负责部署各类防火墙等安全设备，采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十条 校园网用户通过统一上网账号接入校园网络，实行“实名注册、认证上网”制度。校园网用户对自己的上网账号负责，设置足够强度的口令，不得将上网账号转借给他人使用或与他人共用，不得窃取或盗用他人的用户名、口令信息，因账号保管不善造成的信息安全事故由账号本人负责。

第十一条 接入校园网的机房、电子阅览室等一律不准对社会开放，上网人员必须持有校园“一卡通”或凭学生证、工作证等有

效证件登记后，方可上网。机房必须安装管理软件，自动记录上网人员身份和上下网时间、机号、IP 地址等，网络使用记录保存时间不得少于 6 个月。

第十二条 校园网用户必须遵守国家有关法律法规，任何单位及个人不得利用校园网危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体利益和个人的合法权益，不得从事违法犯罪活动。

第四章 信息系统及其数据安全

第十三条 学校按照国家信息系统等级保护制度的相关法律法规、标准规范以及《教育行业信息系统安全等级保护定级工作指南》（教技厅函〔2014〕74 号）要求，落实信息系统安全等级保护制度。

第十四条 各单位（部门）应准确掌握本单位信息系统建设情况，建立信息系统名录，做到底数清、情况明；严格执行本单位信息安全管理措施，切实落实责任，规范建设、运维、使用等各个环节。

第十五条 各单位（部门）应指定专人负责本单位信息系统运行的日常工作，做好用户授权管理，妥善保管好账号和密码。定期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，确保备份数据和备用资源的有效性。

第十六条 办公室（网络与信息中心）负责学校核心信息系统的备份与恢复管理，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，确保备份数据和备用资源的有效性。

第十七条 任何单位和个人，不得私自设立互联网服务器或自建联网的应用系统。根据教学和科研实际工作需求，确实需要建立应用系统的，经批准后方可联网运行。

第十八条 需要开设联网信息服务的单位，须向办公室（网络与信息中心）提出书面申请，经技术评估、备案后方可对外提供服务；服务器必须具有保持日志记录功能，历史记录保存时间不得低于 6 个月。

第十九条 接入互联网的服务器及应用系统，应该采取必要的网络安全防护措施、安装防护软件，并将防护措施报办公室（网络与信息中心）备案。

第二十条 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，包括但不限于各类管理信息系统、教学信息系统、用户服务支持系统以及各类网站产生的数据。

第二十一条 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。

第二十二条 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服务无关的个人信息。按照“谁收集，谁负责”的原则，收集个人信息的单位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，并建立健全相关保护制度。

第二十三条 办公室（网络与信息中心）负责定期对全校的网站及信息系统开展安全检查，检查不合格的网站或信息系统，视其漏洞级别暂停其外网访问，同时通知责任单位限期整改，要求提供整改报告并提交信息化处。经安全复查合格后，方可恢复该网站或信息系统的正常访问。

第五章 终端设备安全

第二十四条 终端设备是指由师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端设备。

第二十五条 终端设备使用人按照“谁使用，谁负责”的原则，对其终端负有保管和安全使用的责任。办公室（网络与信息中心）对终端计算机的安全管理提供技术支持和指导。

第二十六条 终端设备上安装、运行的软件应为正版软件。在终端上使用盗版软件带来的安全和法律责任由终端使用人承担。

第二十七条 终端设备应当设置系统登录账号和密码，登录密码应具有一定强度并定期更改。

第二十八条 终端设备使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第二十九条 终端使用人应做好终端设备的安全防范，如发现终端设备出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处置。

第六章 存储介质安全

第三十条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库等不可移动存储介质，以及移动硬盘、U 盘等等可移动存储介质。

第三十一条 原则上，面向师生服务的存储阵列等大容量介质应托管在学校数据中心机房统一运行、维护和管理。由办公室（网络与信息中心）采取必要技术措施防范数据泄漏风险，保护存储数据安全。

第三十二条 非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。

第三十三条 移动存储介质在接入终端计算机和信息系统前，应当查杀病毒、木马等恶意代码。

第三十四条 介质使用人应注意移动存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第七章 人员安全管理

第三十五条 各单位（部门）应建立健全本单位的岗位信息安全责任制度，明确岗位及人员的信息安全责任。关键岗位的计算机使用和管理人员应签署信息安全与保密协议，明确信息安全与保密要求和责任。

第三十六条 各单位（部门）应加强人员离岗、离职管理，严格规范人员离岗、离职过程，及时终止相关人员的所有访问权限，收回学校提供的软硬件设备，如有必要，需签署安全保密承诺书。

第三十七条 各单位（部门）应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第三十八条 各单位（部门）如有信息系统开发或运维外包服务，应将学校统一制定的网络信息安全与保密协议作为合同附件。明确网络信息安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息和各类电子数据，不得占有服务过程中产生的任何信息资产，不得以服务为由强制要求校方购买、使用指定产品。

第八章 网络信息安全应急管理

第三十九条 办公室（网络与信息中心）负责学校网络信息安全应急工作的具体实施，制定学校网络信息安全事件报告与处置流程，提供安全应急工作的技术支撑和保障。

第四十条 办公室（网络与信息中心）负责定期组织网络信息安全应急演练，评估并适时组织修订网络信息安全应急预案。学校各单位（部门）应组织开展网络信息安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第四十一条 办公室（网络与信息中心）负责组建学校信息安全应急队伍，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第四十二条 学校各单位（部门）应按照学校网络信息安全事件报告与处置流程，做好事发紧急报告与处置、整改等工作。做到安全事件早发现、早报告、早控制、早解决。

第四十三条 学校各单位（部门）及师生员工均有义务及时报告信息安全事件，不得在未授权情况下对外公布或尝试利用所发现的安全漏洞和安全问题。

第九章 网络信息安全教育培训

第四十四条 办公室（网络与信息中心）负责组织学校网络信

息安全宣传和教育培训工作，提高师生员工的安全和防范意识，定期以各种形式组织开展针对师生员工的网络信息安全教育。

第十章 网络信息安全责任追究

第四十五条 学校建立网络信息安全责任追究和倒查机制，玩忽职守、失职渎职造成严重网络信息安全后果的，根据有关规定追究相关部门负责人责任，触犯法律的，移交公安机关处理。

第四十六条 学校各单位（部门）应按照网络信息安全事件报告与处置流程，及时、如实报告并妥善处置网络信息安全事件，瞒报、缓报、处置整改不力造成严重网络信息安全后果的，根据有关规定追究相关部门负责人责任，触犯法律的，移交公安机关处理。

第十一章 其 它

第四十七条 涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准。

第四十八条 本办法在实施中若与国家有关法律、法规有不一致的，以国家法律、法规为准。

第四十九条 本办法自下发之日起实施，由办公室（网络与信息中心）负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

宿州学院办公室　　2017年11月13日印发