南宁师范大学文件

南师发〔2019〕88号

关于印发《南宁师范大学网络信息安全管理制度（暂行）》的通知

校内各单位:

经学校同意，现将《南宁师范大学网络信息安全管理制度（暂行）》印发给你们，请遵照执行。

附件：南宁师范大学网络信息安全管理制度（暂行）

南宁师范大学

2019年6月13日

南宁师范大学校长办公室　　2019年6月13日印发

南宁师范大学网络信息安全管理制度（试行）

第一章 总则

第一条 为了保障我校校园网络及信息系统的安全稳定、促进学校信息化健康发展，根据《中华人民共和国网络安全法》及国家相关法律法规并结合我校实际情况，制定本制度。

第二条 网络信息安全是指网络基础设施、网站、信息系统及数据内容等受到保护，保证网络、信息及内容的安全性、完整性、可用性、可控性。

第三条 网络信息安全管理的基本原则是“谁主管谁负责，谁建设谁负责，谁运维谁负责，谁使用谁负责”，明确责任、突出重点、保障安全。

第四条 网络信息安全管理的总体方针是以国家标准《信息系统安全等级保护基本要求》(GB/T 22239-2008)及广西壮族自治区教育厅、广西壮族自治区公安厅《关于广西教育行业网络安全等级保护工作实施意见》（桂教规范[2017]10 号）为指导，预防为主、综合防范。

第五条 网络信息安全管理的目标是建立健全网络信息安全保障体系，提高安全防护能力，确保学校网络信息安全工作规范、有序开展，保障学校信息化可持续发展。

第二章 组织架构

第六条 学校党委网络安全和信息化领导小组是学校网络安全和信息化工作的领导机构，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。

第七条 宣传部、网络信息中心为学校党委网络安全和信息化领导小组的秘书单位，负责学校网络信息安全的日常工作。宣传部具体负责网络信息安全政策宣传、解读，互联网舆情监测、处置等工作，网络信息中心具体负责学校或协助各单位业务信息系统安全建设、测评定级、备案、防护及日常运维工作。

第八条 学校各单位负责本单位网站及应用系统的使用、管理及日常工作。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，同时，各单位须设置网络信息管理员，负责本单位网络信息安全具体工作。

第三章 网络信息安全建设

第九条 各单位在制作网站或信息系统的项目预算时，须包含网络信息安全的专项经费，用于该网站或信息系统的安全建设及运维。

第十条 各单位须明确网站或信息系统是否需要对校外开放，对校外开放的网站或信息系统，须满足国家标准《信息系统安全等级保护基本要求》规定的安全等级要求，参照广西壮族自治区教育厅、广西壮族自治区公安厅《关于广西教育行业网络安全等级保护工作实施意见》（桂教规范[2017]10 号）进行自主定级，各单位需明确其信息安全需求，参考《信息系统安全等级保护定级报告模板》(附件 1)撰写《信息系统安全等级保护定级报告》及填写《信息系统安全等级保护备案表》(附件 2)提交网络信息中心备

案。

第十一条 各单位网站或信息系统在上线前，须开展安全自查工作，提供安全自查报告（格式自拟），并填写《网站及信息系统情况记录表》(附件 3)，由本单位主要负责人签字确认后，提交网络信息中心备案。

第十二条 网络信息中心采用专业技术手段对网站或信息系统进行安全检测。检测未通过的须进行安全整改，直至通过检测，网站或信息系统方可上线运行。

第四章 运行管理

第十三条 各单位须定期对本单位的网站及信息系统开展安全巡检，并做好巡检记录，填写《网站及信息系统巡检记录表》(附件 4)。对校外开放的网站或信息系统，要求每周巡检一次，对校内开放的网站或信息系统，要求每月巡检一次。

第十四条 各单位须制定本单位信息系统密钥管理办法，切勿将具备超级管理权限的账号密码交由他人持有。信息系统密钥口令需具备一定的复杂度并定期更换。信息系统管理操作日志需保存足够的时间跨度，以备翻查。

第十五条 各单位须定期对网站及信息系统进行漏洞修补，包括主机系统漏洞、WEB 应用漏洞、中间件漏洞、数据库漏洞等。

第十六条 学校将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网络信息中心。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。

第十七条 特殊时期，各单位须加强网站及信息系统的安全监管工作，安排专人值守，加强安全巡检，做好安全整改。

第五章 安全事件应急响应

第十八条 安全事件分为紧急事件和普通事件。

第十九条 紧急事件是指：

1、可由校外访问的页面发生篡改或被替换成非法信息的事件，尤其是发生在主页、新闻网站、招生信息网等访问量高的系统或网站的事件。

2、影响学校系统正常运转的攻击事件，如与服务门户、教务系统、财务系统、办公自动化系统相关的攻击事件。

3、可能造成师生隐私信息被窃取、丢失、损坏的漏洞。

4、其它可能对社会公共安全或学校造成危害或不良影响的事件或漏洞。

第二十条 普通事件是指：

1、对校内开放系统或网站的页面发生无害篡改或有隐藏漏洞。

2、影响不大的攻击事件或可能造成中低隐患的漏洞。

3、其他不构成公共危害或社会不良影响的安全事件或漏洞。

第二十一条 网络信息安全事件应急响应流程如下：

1、网络信息中心接到安全事件通报，通过沟通协调，结合技术手段，获取事件截图等相关证据。

2、网络信息中心核实事件类别，发起处理流程。

3、若事件为紧急事件，网络信息中心第一时间向分管信息化工作校领导汇报，同时通报责任单位相关情况及事件证据，并关闭相关网站或信息系统的访问权限，以降低不良影响。若事件为普通事件，则此环节略过。

4、网络信息中心指导分析事件原因，并提供整改建议。

5、责任单位对网站或信息系统进行安全修复，并提交整改报告（格式自拟）。

6、网络信息中心对修复后的网站或信息系统进行安全复查，复查通过后恢复其访问权限。

第二十二条 各单位须制定本单位的网站及信息系统安全应急预案，并定期进行安全应急演练。

第六章　内容安全

第二十三条　任何单位和个人必须遵守《中华人民共和国计算机信息网络国际互联网络管理暂行规定》、国家有关法律法规和学校的有关管理规定，严格执行信息安全保密制度，并对所提供和发布的信息负责。

第二十四条　任何单位和个人不得利用校园网及经学校备案的系统制作、复制、传播下列信息：

1、煽动抗拒、破坏宪法和法律、法规实施的。

2、煽动颠覆国家政权，推翻社会主义制度的。

3、煽动分裂国家、破坏国家统一的。

4、煽动民族仇恨、民族歧视，破坏民族团结的。

5、煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的。

6、捏造或者歪曲事实，散布谣言，扰乱社会秩序的。

7、宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的。

8、公然侮辱他人或者捏造事实诽谤他人的。

9、损害国家荣誉和利益的。

10、以非法民间组织名义组织活动的。

11、其他违反宪法和法律、行政法规的。

第二十五条　需严格遵循内容审核机制，规范信息发布审批流程，加强信息安全监控，防止出现内容篡改等安全事故。

第二十六条　宣传部负责网站内容审查及监管，网络信息中心负责技术支持和保障。

第七章　　附则

第二十七条 涉密网络信息系统的运行安全保护工作不适用本制度所述办法。

第二十八条　依据《中华人民共和国网络安全法》第六章“法律责任”的规定，因网络信息安全导致的事故，由网站或信息系统所属单位和责任人承担相应的经济处罚、民事责任、治安管理处罚或刑事责任。

第二十九条　网络信息失泄密事件按照国家和学校相关法律法规和规章制度处理。

第三十条 本制度自发布之日起施行，由网络信息中心负责解释。