管理员	蒋小波
类别	6
级别	对外公开

南宁学院

信息安全管理制度汇编

【2019】

编制：南宁学院网络安全与信息化领导小组办公室

审核：南宁学院网络安全与信息化领导小组

目录

第一章 信息安全管理制度总则 3
一、 总则 3
二、 总体方针 3
三、 总体目标 3
四、 信息安全工作总体原则 3
五、 信息安全工作总体策略 5
六、 信息安全管理制度制定和发布 6
七、 信息安全管理制度评审和修订 6
八、 引用标准及参考文件 6
九、 适用范围 7
第二章 安全管理机构 8
一、 目的 8
二、 组织机构 8
三、 重要岗位工作职责 9
四、 授权和审批 12
五、 沟通和合作 14
六、 审核和检查 14
第三章 人员安全管理 16
一、 人员录用 16
二、 人员 AB 岗制度 16
三、 人员调岗与离岗 16
四、 人员考核与惩罚 17
五、 安全意识和教育培训 17
六、 外部人员管理 18
第四章 系统建设管理 20
一、 系统定级 20
二、 安全方案设计和审定 20
三、 产品采购和使用 21
四、 软件自开发 21
五、 外包软件开发 21
六、 工程实施 22
七、 测试验收 22
八、 系统交付 22
九、 安全服务商选择 23
第五章 南宁学院中心机房管理制度 23
一、 一般规定 23
二、 日常管理规定 23
三、 办公环境管理 24
第六章 网络信息中心资产和设备管理制度 26
一、 资产和设备管理 26
二、 介质管理 26
第七章 网站安全管理制度 27
一、 网站建设 27

二、 网站编辑和管理 27
三、 网站监控 28
第八章 网络安全管理制度 29
一、 网络安全规划 29
二、 网络接入和安全管理 29
三、 网络安全审计 33
四、 网络设备管理 33
五、 网络安全检查 34
第九章 信息系统安全管理制度 35
一、 信息系统建设和管理的工作及责任划分 35
二、 信息系统安装及接入 35
三、 信息系统变更 36
四、 各信息系统及其依赖环境的配置及安全管理 38
五、 信息系统安全审计 39
六、 数据容灾备份 40
第十章 病毒及恶意代码防范管理制度 41
一、 病毒及恶意代码防范的日常管理 41
二、 病毒及恶意代码的查杀与处理 41
第十一章 信息安全事件管理制度 43
一、 信息安全事件的定义和范围 43
二、 信息安全事件的监控和处理 43
三、 信息安全事件监督和总结管理 44
第十二章 信息安全应急管理制度 45
一、 突发事件分类 45
二、 职责 45
三、 事件分级 45
四、 信息与网络安全突发事件处理原则 46
五、 监督管理 47
第十三章 附 则 48
1. 本标准由网络信息中心负责解释。 48
2. 本标准自颁布之日起实行。 48

第一章 信息安全管理制度总则

一、总则

为加强和规范信息系统安全管理工作，提高信息系统整体安全防护水平，实现信息系统的可控、能控、在控，依据国家有关法律、法规的要求，制定本文档。

本文档的目的是为本学校信息系统安全管理提供一个总体的策略性架构文件，指导信息系统安全管理体系的建立，实现信息系统统一的安全策略管理，提高整体的网络与信息安全水平，确保安全控制措施落实到位，保障网络通信畅通和业务系统的正常运行。

二、总体方针

信息系统安全坚持 “安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、 能控、在控。依照“分区、分级、分域”的总体安全防护策略，执行信息系统安全管理制度。

三、总体目标

信息系统安全总体目标是确保信息系统持续、稳定、可靠运行，确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据损失，防止有害信息在网上传播，防止系统服务中断和由此造成的系统运行事故。

四、信息安全工作总体原则

1. 基于安全需求原则

按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上平衡信息系统安全设备投入及安全防护效果。

2. 主要领导负责原则

主要领导应确立统一的信息安全保障的宗旨和政策，提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理牵头部门与各分院、处、室的工作关系，并确保其落实、有效。

3. 全员参与原则

信息系统所有相关管理人员（包括各分院、处、室）应遵循信息系统的相关安全管理规定，共同保障信息系统安全。

4. 系统方法原则

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率。

5. 持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

6. 依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

7. 选用成熟技术原则

成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误。

8. 分级保护原则

按等级划分标准确定信息系统的安全保护等级，实行分级保护。

9. 管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，

采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

10. 自保护和国家监管结合原则

对信息系统安全实行自保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

五、信息安全工作总体策略

1. 按照国家等级保护相关要求，确定信息系统安全等级，根据不同的安全等级实施分等级保护。

2. 定期对信息安全管理体系进行评审，并实施相应的预防和纠正措施，保证信息安全管理体系持续的适宜性、有效性。

3. 建立安全管理组织机构，明确相关岗位及职责，建立健全的信息安全管理责任制，使得各项安全管理责任落实到个人。

4. 加强所有人员（包括内部人员，以及各类外来人员）的安全管理，明确岗位安全职责，制定针对违规的惩戒措施，落实人员在岗和离岗时的安全控制，与重要岗位人员签署保密协议。

5. 规范信息系统和设备的调配、日常操作、管理维护规程，制定文档化规范，降低和避免因无操作引发信息安全事件的可能性。

6. 加强信息安全日常管理，包括口令管理、无人值守设备管理、屏幕保护等，促使每位管理人员的日常工作符合信息安全制度要求。

7. 对重要信息及信息系统进行备份，确保备份信息的保密性、完整性、可用性。

8. 通过正式的信息安全技能、知识培训，以不仅限于培训会议的信息安全教育活动形式，不断加强人员安全意识，提高人员安全知识和技能。

9. 采用技术和管理两方面的控制措施，加强对信息系统外网的安全控制，不断提高网络的安全性和稳定性。对外网与互联网进行逻辑隔离。通过实施网络

访问控制等技术防范措施，对接入进行严格审批。

10. 在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。

11. 对所适用的国家信息安全相关法律法规进行定期的识别、记录和更新，并对信息安全管理现状与法律法规的符合性进行检查，确保各项信息安全工作符合国家信息安全相关法律法规要求。

六、信息安全管理制度制定和发布

1. 在网络安全与信息化领导小组的总体负责和监督下，组织人员制定安全管理制度。

2. 组织信息化建设相关人员通过内部评审对安全管理制度进行论证和审定。

3. 安全管理制度应经过学校网络安全与信息化领导小组审定后，按照一定的程序和途径以文件形式发布。

七、信息安全管理制度评审和修订

由网络信息中心主管定期组织相关管理人员对制度的适用情况进行检查和评审，对不合适的地方进行修订，在学校网络安全与信息化领导小组审定后及时更换新版。

八、引用标准及参考文件

本文档的编制参照了以下国家的标准和文件：

- 《中华人民共和国计算机信息系统安全保护条例》
- 《关于信息安全等级保护建设的实施指导意见》（信息运安(2009)27 号）
- 《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）
- 《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）
- 《信息系统等级保护 安全建设技术方案设计要求》（报批稿 ）

- 《信息安全技术　信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息安全技术　网络基础安全技术要求》（GB/T20270-2006）
- 《关于开展信息安全等级保护安全建设整改工作的指异意见》（公信交[2009]1429 号）

九、适用范围

本文档适用南宁学院信息系统、信息系统技术实施及管理人员的安全管理和指导，适用于信息系统安全建设和运维过程。

第二章 安全管理机构

一、目的

为规范南宁学院信息安全管理工作，建立自上而下的信息安全工作管理体系，需建立健全相应的组织管理体系，以推动信息安全工作的开展和信息系统的安全管理。

二、组织机构

学院设立的信息安全工作管理组织机构分两级主管领导。第一级主管领导是网络安全与信息化领导小组，作为本院信息安全工作的最高决策机构；第二级主管机构为网络安全与信息化领导小组办公室，即学院网络信息中心（以下别称包括“网络中心”、“信息中心”、“中心”、“网络安全与信息化领导小组办公室”），作为本校信息系统、信息安全、数字化校园建设、管理的牵头部门。

1. 网络安全与信息化领导小组负责研究重大事件，落实方针政策和制定总体策略等，主要职责包括：

(1) 根据国家和行业有关信息安全的政策、法律和法规，批准学院信息安全总体策略规划、管理规范和技术标准。

(2) 确定学院信息安全有关部门的工作职责，指导、监督信息安全工作。

(3) 网络安全与信息化领导小组下设网络安全与信息化领导小组办公室，网络安全与信息化领导小组办公室分设应急小组。网络安全与信息化领导小组办公室主任由网络信息中心主任担任，应急小组组长可由网络信息中心主任兼任或指定具有相应能力的人员担任。

(4) 网络安全与信息化领导小组办公室各岗位包括网络安全与信息化领导小组办公室主任、网络安全与信息化领导小组办公室副主任、安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员，应急小组由应急小组组长、应急小组副组长、应急联络员组成。

3.网络安全与信息化领导小组办公室负责统筹和实施校园数字化、信息化、信息安全建设工作，主要职责包括：

(1) 负责贯彻执行网络安全与信息化领导小组的决议，协调和规范学院信息安全工作。

(2) 根据网络安全与信息化领导小组的工作部署，对信息安全工作进行具体安排、实施。

(3) 组织对重大的信息安全工作制度和技术操作策略进行审查，并监督执行。

(4) 组织信息安全工作检查，分析信息安全总体状况，提出分析报告和安全风险的防范对策。

(5) 及时向网络安全与信息化领导小组和有关部门报告信息安全事件，出具信息安全事件报告说明情况。

(6) 跟踪先进的信息安全技术，组织信息安全知识的培训和宣传工作。

(7) 依据国家相关政策，对信息系统实行分等级保护工作的实施，统筹信息系统的定级、备案、测评、整改、运维的工作。

4.应急小组主要职责包括：

(1) 审定学院网络与信息系统的安全应急策略及应急预案。

(2) 决定相应应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统。

(3) 定期组织信息安全应急策略和应急预案的测试和演练。

三、重要岗位工作职责

1. 网络安全与信息化领导小组办公室主任、副主任主要职责包括：

(1) 根据信息化建设的总体目标，负责信息系统的安全管理体系建设，包括：制度建设、技术保障和操作规范等各方面的逐步建成。

(2) 负责制订信息系统安全规划，并在实施过程中逐步完善。

(3) 负责信息系统运行安全保障工作的管理、组织、实施和监督。

(4) 负责信息系统安全工作进行指导、检查并进行情况通报。

(5) 负责协调、督促各信息系统管理人员的信息安全工作，参与信息系统工程建设中的安全规划，监督安全措施的执行。

(6) 负责灾难备份系统及相关设施的完善及日常管理工作。

(7) 负责组织信息安全教育活动，对内部人员进行信息系统安全管理的教育、

培训，提高本院内部人员的信息系统安全意识。

(8) 负责对信息安全状况的定期检查；当出现安全事件时，对发生的安全事件及时上报，并配合相关的调查和纠正工作。

(9) 负责与外部安全机构（如：安全服务商）的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持。

2. 应急小组组长、副组长主要职责包括：

(1) 负责组织审定学院网络与信息系统的安全应急策略及应急预案。

(2) 决定相应应急预案的启动，组织应急联络员进行现场指挥。

(3) 定期组织应急预案演练。

(4) 负责接受各二级分院、处、室的信息系统紧急信息安全事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出信息安全事件防范措施。

3. 安全管理员主要职责包括：

(1) 负责信息系统的安全相关事务，协助监督安全制度的执行、修改等。

(2) 负责制订信息系统安全规划，并在实施过程中逐步完善。

(3) 负责制定安全设备或系统的文档化的操作和维护规程。

(4) 负责执行普通项目流程对接和普通审批的管理，并向主任进行工作汇报。

(5) 负责对安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。

(6) 负责组织实施安全设备或系统各类事故（故障）的应急处理。

(7) 负责协助领导安排安全培训，负责协助负责制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识。

(8) 负责制定安全检查计划，定期检查。包括检查职责、检查周期、检查范围、检查内容、检查报告的编制、检查整改、检查通报等内容。对信息系统安全检查并进行情况通报。对记录进行收集、整理、归档。

(9) 当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作。

(10) 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根

据指令立即采取安全措施启动相关处理程序。

4. 安全审计员主要职责包括：

(1) 审计员负责定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等。

(2) 按照相关策略和要求进行安全检查，并妥善保存相关的安全检查执行记录。

(3) 定期检查系统管理员和系统操作员的活动日志。

(4) 负责记录、分析故障日志，对所有可疑或经确认的入侵行为或入侵企图需及时汇报并采取相应的响应措施。

(5) 定期查看数据库系统的运行日志和审计日志。

5. 网络管理员主要职责包括：

(1) 负责网络的运行管理，实施网络安全策略和安全运行细则。

(2) 安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行。

(3) 监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向信息安全人员报告安全事件。

(4) 对操作网络管理功能的其他人员进行安全监督。

6. 系统管理员主要职责包括：

(1) 负责系统的运行管理，实施系统安全运行细则。

(2) 严格用户权限管理，维护系统安全正常运行。

(3) 认真记录系统安全事项，及时向安全管理员报告安全事件。

(4) 对进行系统操作的其他人员予以安全监督。

7. 数据库管理员主要职责包括：

(1) 对账户进行管理监控工作。

(2) 确保数据库的正常运行。

(3) 及时发现并解决后台问题与隐患。

(4) 进行系统性能调整和优化。

(5) 备份策略的规划与实施等。

8. 应急联络员工作职责包括：

(1) 参与安全应急策略、应急预案的制定、审定、测试和演练。

(2) 负责配合小组组长、副组长开展信息系统紧急事件应急预案的启动。

(3) 负责及时接收各二级分院、处、室的信息系统紧急事件报告，分析情况，根据事件严重程度采取相应处理措施，上报小组负责人。

9. 网络信息中心实行轮值管理，要求关键岗位人员掌握网络管理、系统管理、数据库管理等技能。

四、授权和审批

1. 内部授权程序

(1) 根据网络安全与信息化领导小组的主要职责，网络安全与信息化领导小组办公室由网络安全与信息化领导小组授权后生效。网络安全与信息化领导小组办公室直接对网络安全与信息化领导小组负责。

(2) 根据网络安全与信息化领导小组办公室的主要职责，信息安全各安全岗位的负责人员由网络安全与信息化领导小组办公室授权后生效。各信息安全岗位管理人员对网络安全与信息化领导小组办公室负责。

(3) 根据网络安全与信息化领导小组办公室的主要职责，各院、处、室提出的信息系统建设、设备购置等需求的经办人员由各业务单元的相关部门提由网络安全与信息化领导小组办公室授权后生效，各院、处、室对网络安全与信息化领导小组办公室负责。

2. 外包运维人员审批程序

(1) 外包运维人员对信息系统每个环节的参与均需要网络信息中心主管的审批，或者由网络信息中心主管授权网络安全与信息化领导小组办公室组员进行相关审批。

(2) 对于没有经过正式授权的，临时的、紧急的、需要即时审批的信息系统维护需求，可由网络信息中心主管电话审批同意，但过后需要补充审批记录。

3. 变更审批办法

(1) 变更分类与审批的一般原则

- 信息系统变更主要分两大类别：标准变更和紧急变更。

- 变更的发起人为各院、处、室信息系统管理人员、系统管理人员或系统运维外包厂商人员。
- 两类变更的审批办法和流程基本一致，原则是需要有效识别各类系统变更的风险，并严格按照审批程序有效规避风险、落实相关责任方。

(2) 变更审批流程

- 变更由上述变更发起人发起，根据变更的具体内容填写相关的变更管理表单。
- 变更审批的第一级部门是信息系统直接使用部门（即各院、处、室等），因为不直接牵涉到信息系统的变更，该部分变更由该部门审批，最后一个审批人须是该部门的部门领导或者更高一级的主管领导，具体由该部门自行决定。
- 变更审批的第二级审批部门是网络信息中心，由网络信息中心安排专人评估变更的风险和可行性，评估结果可行后，由网络信息中心主管审批，网络信息中心主管审批后交由系统运维人员具体实施，完成系统变更。
- 可能会涉及到系统内核的变更，在变更实施时影响系统运行的稳定性。此类变更一般由系统管理员发起，要求系统管理员在发起变更的同时需要就本次变更的潜在风险和风险规避措施进行描述后报请网络信息中心主管进行审批，信息中心主管审批后由系统管理员进行具体实施，完成系统变更。

4. 设备采购审批

设备的采购过程按照学院相关规定执行，牵涉到信息中心部门审批的环节，均需要有网络信息中心主任签字审批认可。

5. 其他审批办法

(1) 物理访问、系统接入等其他对信息系统的访问和修改操作，均由网络信息中心主管或网络信息中心主管授权的信息中心其他人员负责审批并监督后续的访问过程。

(2) 重要操作，如业务系统功能上的重大调整、重大升级变更、网络架构大的调整，均需要由网络信息中心主管召集相关人员论证后初审，初审的结果报网络安全与信息化领导小组做最后审批后进行。

五、沟通和合作

1. 网络安全与信息化领导小组和相关负责人员、管理人员、相关企事业单位、系统集成商等应就信息系统的管理及安全防护问题紧密沟通与合作。

2. 信息安全工作主管领导应不定期召开交流和协调会议，共同协助处理信息安全问题，确保安全工作的顺利实施。

3. 信息安全工作主管领导可每半年组织相关部门和人员召开安全工作会议，协调安全工作的顺利实施。

4. 信息安全工作主管领导可经常举行一些与其他兄弟单位、公安局的沟通交流会，以便在发生信息安全事件时能够得到及时的支持和帮助。

5. 将信息系统相关集成商、运营商等合作单位的关键信息汇总并记录。

6. 对各类会议，包括交流会、协调会议、安全评审等进行记录。

六、审核和检查

1. 网络安全与信息化领导小组应监督、指导安全审核和安全检查工作，督促执行。

2. 网络安全与信息化领导小组定期（每年）进行全面的信息安全检查，其内容包括现有技术措施的有效性、安全配置与安全策略的一致性的核查，安全管理制度的执行情况等。

3. 网络安全与信息化领导小组应定期召开信息安全会议，审核网络安全与信息化领导小组办公室和应急小组的相关记录和报告，规划下阶段安全计划。

4. 网络安全与信息化领导小组办公室应制定安全检查表格，配合网络安全与信息化领导小组实施安全检查，记录汇总安全检查数据，编写安全自查报告。

5. 安全管理员应定期（每季度）组织进行安全检查，各相关管理人员应配合完成。

6. 安全审计员应定期（每季度）进行安全审查，各相关管理人员应配合完成。

7. 相关部门和人员应积极主动配合安全审查和检查工作，对发现的问题应及时改进。

8. 网络管理员、系统管理员、数据库管理员、应急联络员等相关信息系统管理人员应定期针对管理的相关工作（包括网络、设备、日常管理等）进行安全检查，并报网络安全与信息化领导小组办公室审核检查结果，并根据网络安全与信息化领导小组办公室提出的安全建议进行改进。

9. 所有信息安全审核和安全检查工作都应记录并存档。

第三章 人员安全管理

一、人员录用

1. 人员录用办法依照学院人事处相关规定进行录用。

2. 为保证被录用人员具备基本的专业技术水平和安全管理知识，在人员正式上岗前，对被录用人进行专业技术水平考核和安全管理知识考核。

3. 应对被录用人所具备的与岗位相关的技术技能进行考核。

4. 应对被录用人说明其角色和职责，并进行针对性的岗位培训。

5. 被录用人应签署岗位安全协议及保密协议，约束自身行为规范、防止系统中的核心信息和相关重要信息的泄漏。

二、人员 AB 岗制度

1. 为提高办事效率，进一步完善工作程序，特制订人员 AB 岗制度。

2. 此 AB 岗工作制是针对网络与教育技术中心各管理员在处理相关工作时，对应岗位的管理员不在，规定相应的人员代行处理的一种工作制度。

3. A 岗或 B 岗管理员因休假、学习、因公外出等原因离岗时，必须提前半天至一天向 B 岗或 A 岗管理员做好工作交代，因特殊原因不能及时交代的，B 岗或 A 岗管理员应当主动顶岗；B 岗或 A 岗管理员在顶岗期间要同时做好本岗和 A 岗或 B 岗主要工作，并同时兼有 A 岗或 B 岗的职责权利，对执行 A 岗或 B 岗的工作结果负有相应责任。

4. AB 岗对应工作人员应互相学习和传授业务、操作技能，加强联系，及时交流、了解相互之间的工作业务，在一方外出时要保证工作的衔接。

三、人员调岗与离岗

5. 人员离岗办法依照学院人事处相关规定办理离职手续。

6. 对于因各种原因即将离岗的员工，应立即终止其与系统相关的所有访问权限。

7. 即将离职的系统管理员，应将管理设备的口令和密码上交，后续管理员应在第一时间进行口令和密码的修改工作。

8. 应立即取回即将离职员工的各种与系统和单位相关的身份证件、钥匙、徽章等以及机构提供的软、硬件设备和其他介质。

9. 若管理人员申请调走，报告经单位批准前，应对重要的管理工作提前交接，把密码、钥匙、注意的问题等交接给单位指定人员。

四、人员考核与惩罚

1. 为确保系统各个方面的管理人员意识到信息安全威胁和隐患，并在正常工作时遵守信息安全方针，网络安全与信息化领导小组办公室定期对各个岗位的人员进行安全技能及安全认知的培训和考核，这种培训与考核有时候要扩大到有关的第三方管理人员。

2. 对与系统各个方面相关的管理人员应该进行身份审查、岗位职责审查、权限和责任审查、保密审查等；对其他关键人员应该进行身份审查、岗位职责审查等，以确保系统的安全运行和管理。

3. 对违背安全策略和规定的人员进行惩戒。对违规的单位内部员工，情节较轻的，进行批评并要求其进行书面检讨；情节较重的，由相关部门追究其行政责任。对于违规的第三方管理人员，情节较轻的，责令其改正，并告知其项目负责人和该学院相关负责人；情节较重的，由相关部门追究其行政责任。

五、安全意识和教育培训

1. 信息安全教育培训计划由网络信息中心根据年度工作计划作出安排。

2. 可指定专人定期组织信息安全教育学习。

3. 信息系统相关管理人员应积极主动地参加网络信息中心组织的信息安全教育学习活动。

4. 有选择地参加其它行业和部门举办的专业培训，鼓励参加其它业务交流和学习培训。

5. 支持、鼓励各管理人员结合日常工作自学。

6. 信息安全教育

(1) 定期组织学院工作人员认真学习网络安全、计算机信息网络安全保护等知识，不断提高工作人员的安全意识和技能。

(2) 负责对全体教师进行安全教育和培训。

(3) 可邀请安全专家、安全集成商等对管理人员进行信息安全方面的培训，提高操作员的防范能力。

7. 职业道德教育

(1) 工作人员要严格遵守工作规程和工作制度。

(2) 不得制造，发布虚假信息，向非相关人员提供有关数据资料。

(3) 不得利用计算机信息系统的漏洞偷窃资料，进行诈骗和转移资金。

(4) 不得制造和传播计算机病毒。

8. 计算机技术教育

(1) 操作员必须在指定计算机或指定终端上进行操作。

(2) 机房管理员，程序维护员，操作员必须实行岗位分离，不得串岗，越岗。

(3) 不得越权运行程序，不得查阅无关参数。

(4) 发现操作异常，应立即向相关管理员报告。

9. 培训方法

(1) 结合专业实际情况，指派有关人员参加学习。

(2) 有计划有针对性，指派人员到外地或外单位进修学习。

(3) 举办专题讲座或培训会，聘请有关专家进行讲课。

(4) 自订学习计划，参加学习。

六、外部人员管理

1. 基本安全管理

(1) 未经学院相关负责人的审核审批的情况下，禁止外部人员了解和查阅学院的敏感、重要和商业秘密信息。

(2) 外部人员如因业务需要查阅学院敏感资料或访问学院网络和信息系统资源，必须经过相关负责人批准并详细登记。

(3) 外部人员进出关键区域的进出应填写规定的表格，经负责人签字确认后，

由内部人员的全程陪同，方可进入。

2. 外部人员物理访问控制

(1) 外部人员进出学院时，应遵守学院相关外部人员管理制度。

(2) 业务洽谈和技术交流应当在接待室、会议室或培训教室内进行，商务会见、教育科研等正式洽谈和重大项目的会谈应当在专门的会议室进行，不得在办公区域内进行。

(3) 外部人员进入机房、设备间等重要区域时，应遵从《南宁学院中心机房管理制度》等相关办法。

3. 外部人员信息系统使用控制

(1) 网络中心机房设备的配置只能由中心专门负责的工作人员完成。

(2) 禁止外部人员远程访问。

(3) 在购置网络设备需测试时，厂家设备由厂方或集成商技术人员操作，核心区域（包括核心交换机、重要服务器等）的配置由网络信息中心操作。

(4) 学校的设备配置只能由网络中心人员配置，特殊情况需经过网络信息中心主管审批。

- 必须填写外部人员系统操作审批表。
- 必须在中心人员的全程陪同下操作。
- 未经网络中心主管允许，不得使用光盘、硬盘、U 盘等介质接入系统，并禁止任何拷贝行为。
- 进入系统需要中心人员输入账号密码。
- 保存操作记录。

第四章 系统建设管理

一、系统定级

1. 根据信息系统的整体规划和设计运行需要，按照《信息系统安全等级保护定级指南》对相应系统进行定级。

2. 开展信息系统等级保护工作初期，明确定义和确定信息系统的安全保护等级属性，如实填写定级报告及备案表。

3. 信息系统的定级结果应经过网络安全与信息化领导小组办公室的审定，上报南宁市网络安全保卫支队备案并获得备案证明，再开展后续等级保护工作。

二、安全方案设计和审定

1. 根据系统的安全等级保护级别选择安全设备和安全措施。

2. 编写系统安全设计方案，内容包括但不限于系统的安全保护要求和策略、安全措施等。

3. 根据相应的系统安全设计方案，编写信息系统详细安全设计方案。

4. 网络信息中心主管组织相关人员（及安全技术专家）对安全设计方案的合理性和正确性进行论证和审定。

5. 在项目正式开始实施之前，应由网络信息中心主管（及安全技术专家）批准安全设计方案，再上交至网络安全与信息化领导小组，经批准后方可实施。

6. 安全性论证应着重对项目的安全需求分析、安全对策以及总体安全方案进行成本-效益、合理性、可行性和有效性分析，给出明确的结论：

- 适当
- 不合适（否决）
- 需作复议

7. 对论证结论为“需作复议”的项目，须对有关内容进行必要的补充或者修改后，再次提交复审。

8. 项目安全立项

- 申请流程至审批通过后，项目审批单位将对项目进行立项。

- 网络安全与信息化领导小组办公室负责对整个项目进度的把控。
- 网络安全与信息化领导小组办公室负责项目的整体统筹，包括信息系统安全建设、监督厂商或集成商的实施、信息系统建设完成或测评整改结束后的管理。

9. 立项的项目，如采用引进、合作开发或者外包开发等形式，则需与第三方签订安全保密协议。

三、产品采购和使用

1. 设备和产品的采购和管理遵照学院相关部门的采购、管理制度。
2. 采用符合国家的有关规定和信息安全等级保护对应等级的相关标准保的产品（包括网络产品、安全产品等）。
3. 采用符合国家密码主管部门要求的密码产品。

四、软件自开发

内部人员可根据需求进行软件开发，自行搭建开发环境且禁止使用实际环境进行开发和测试，开发成果可呈交至信息中心主任，提供相关设计、实施文档及使用指南等文件，由主任及部门人员共同测试、评定，最终结果由主任向上级领导汇报，作为信息系统变更事件处理。

五、外包软件开发

1. 与软件开发单位签署软件开发协议，明确代码质量要求、知识产权的归属和安全方面的要求。
2. 要求开发方提供软件质量测试报告。
3. 在软件安装之前和应用系统正式上线之前，相关管理人员负责检测软件包中可能存在的恶意代码。
4. 要求软件设计开发单位提供软件的源代码以及相关设计、实施的文档和使用指南。

5. 要求软件开发单位针对软件的安装、使用和注意事项进行相关培训。

六、工程实施

1. 项目开始实施之前，应与工程实施单位签订与安全相关的协议，以约束工程实施单位的行为和工程实施的质量。

2. 在项目实施的过程中，网络信息中心负责工程实施整个过程的管理。

七、测试验收

1. 系统建设完成之后，网络信息应组织人员对系统进行软件运行测试、系统应用测试、系统安全性测试等，同时编写测试方案，填写测试报告。

2. 在测试验收前，实施单位向网络信息中心提出验收申请，网络信息中心主管对系统测试报告和验收报告进行审定，并通知学院资产管理部门和纪检部门，协同验收。

3. 在测试验收时，参与系统验收的人员应以双方签订的合同及前期的系统建设相关方案为标准进行验收，并保存验收报告。

4. 根据学院相关规定，学院资产管理部门派遣人员参与验收，负责对交付清单中所交接的设备进行清点、核对。

5. 根据学院相关规定，学院纪检部门派遣人员参与验收，负责监督验收工作的严谨性、公正性。

八、系统交付

1. 完成系统验收工作后，工程实施单位提供系统交付清单，包括所有的设备、软件及相关文档。

2. 系统交付后，组织工程实施单位对中心管理人员的相关培训工作。

3. 系统交付后，相应管理人员应对工程实施单位、系统建设方提交的系统相关技术文档、操作手册等进行熟读并妥善保存。

4. 系统交付后，工程实施单位仍按照服务承诺，在一定期限内及时对系统运行维护提供技术支持。

九、安全服务商选择

1. 选择符合国家信息安全相关规定的安全服务商。
2. 选择提供技术支持和服务承诺的服务商。
3. 直接合作时，双方签订安全服务合同，合同内明确约定相关责任。

第五章 南宁学院中心机房管理制度

一、一般规定

1. 防雷：按国家的规定对机房的设备进行接地。每年要按国家的规定对防雷设施及设备接地进行检测。
2. 防火：需按国家的规定在计算机机房进行设置消防设施。设施每年要按国家规定进行检测。
3. 防水：要经常检查机房的防漏水情况，空调、门窗及屋顶。
4. 防盗：严格机房进出管理，门禁要 24*7 小时工作，严格执行进出机房的登记制度、严格执行进出机房不得携带其他物品的规定。
5. 防虫害：经常检查机房的顶棚上和地板下的封闭情况，不得在机房内在放食品，不得在机房内堆放杂物。

二、日常管理规定

1. 严禁非机房工作人员进入机房，特殊情况需填写机房出入登记表后方可进入。
2. 严禁非中心工作人员上机操作。
3. 进入机房人员应遵守机房管理制度。
4. 进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流

体物质等对设备正常运行构成威胁的物品。

5. 严禁将其它与机房工作无关的物品带入机房。

6. 机房要保持清洁、卫生，定期打扫，由专人负责管理和维护(包括温度、湿度、电力系统、网络设备等)，每天查看、维护、管理。

7. 不定期对机房内设置的消防器材、监控设备进行检查，以保证其有效性。定期检查排插安全，防漏电。

8. 值班人员必须认真、如实、详细填写机房出入登记表，详记来人、事件、处理经过等，以备后查。

9. 中心机房内严禁吸烟、喝水、吃食物、嬉戏，保持机房安静。

10. 中心机房设备间玻璃门实行常规性上锁封闭，除必要的设备调试和安装维护外，不得开锁进入。

三、办公环境管理

1. 上班着装整洁得体。

2. 员工应严格遵守办公环境管理要求。

3. 公共办公区域内禁止吸烟，保持防火、防盗安全意识。

4. 标识统一规范，不随意张贴，各类物品摆放整齐、有序，功能布局清晰。

5. 所有区域应保持清洁卫生，遵守环境体系要求，节约能源纸张，垃圾分类投放。

6. 不在办公区进行接待，设专门的接待室或使用会议室接待来访人员。

7. 工作时间不做与工作无关的事。

8. 办公设备属学院财产，主要包括办公桌椅、电脑及电脑的各种组件、电脑软件、网络设备、打印机、复印机、扫描仪、存储柜等。

9. 办公设备分配到个人后，使用人须自觉妥善放置和保管，并爱护使用。

10. 未经允许，不得随意挪用他人或公用办公设备。

11. 爱护公共设备设施，按规定正确使用，不浪费或故意损坏，使用人未能合理使用而造成设备损坏的则需照学院相关处置办法处理。

12. 借用公用办公设备须及时归还，如有丢失或损坏，由借用人负责照价赔偿。

13. 设备使用人须配合办公设备管理员的工作。

14. 工作人员离开座位时退出登陆状态，桌面没有敏感信息文件。

15. 离开办公室应注意关闭电脑、电灯、空调、打印机等设备电源，并检查门窗是否关闭上锁。

16. 工作人员调离办公室应立即交还该办公室钥匙。

第六章 网络信息中心资产和设备管理制度

一、资产和设备管理

1. 网络信息中心资产和设备的管理责任人为信息中心主管。

2. 学院设立专门的资产管理部门，信息中心的资产设备遵照该部门的相关制度办理立项报批、采购、验收、入库、登记、报账、领用等手续。

3. 网络信息中心的资产和设备报损、报废等处置行为遵照资产管理部门的相关制度和流程处理。

4. 资产和设备维修

(1) 管理人员应根据设备的实际使用情况、日常管理中发现的问题对设备进行预防性维修。

(2) 管理人员按照生产厂商推荐的方式对设备定期进行保养，发现设备存在隐患时，及时向资产管理部门报修，落实设备维修工作。

(3) 维修完成后，管理人员和相关负责人负责进行质量验收，验收通过方可投入使用。

5. 中心信息资产重要程度分为对外公开信息、对内公开信息、内部敏感信息，相应的权限及存储方式详见《信息资产分类标准表》。

二、介质管理

1. 介质包括单位计算机系统相关业务的电子信息输出、存放的电子介质、物理介质、可移动和不可移动的磁盘、光盘、硬盘、磁盘阵列等。

2. 所有的介质须登记在册，填写介质清单，标明介质名称、类型、用途、责任人等信息。

3. 介质的安装、使用、转移、维修和销毁须经过信息中心主管的批准。

4. 仅允许中心工作人员领用介质，禁止第三方使用。

5. 定期盘点，保存盘点记录。

第七章 网站安全管理制度

一、网站建设

1. 网络中心是学校各类网站建设的牵头部门，总体负责学校各类网站的建设和技术支持工作，各二级学院、处、室或活动办等需建立开设网站的应向网络中心报备，由网络中心牵头落实或在网络中心的要求和指导下自行建设。

2. 需建设的新网站或进行改版建设的网站，不论是由网络中心具体落实还是使用单位自行建设，均须采用”php+mysql”的网站技术架构，并经网络中心对新建网站安全检测通过后方可上线运行。

二、网站编辑和管理

1. 网站日常编辑工作由各网站使用单位指定信息员负责，如无特殊情况，除学校主站外，各二级学院网站、处室部门网站只设立一个管理员账号，由网站使用单位指定 1 人专项负责，网站账号专人专用，网站编辑专人专管，指定的网站编辑人员不得将账号转告他人代为操作。

2. 网站账号密码、权限、技术信息等网站安全关键性信息严禁使用 QQ、邮件等任何学校无主权的公众平台传播，效仿公安网络安全保卫支队做法，应最好采用纯人工方式对接，确实需要通过网络传播的应使用我校 OA 系统或我校即时协同系统发送，有关学校网站的机密性技术讨论内容应在我校即时协同系统中进行，以最大程度避免关键性信息泄露。

3. 网站新闻编辑操作严格规定在工作人员的办公室电脑上进行，不得在网吧、宿舍或他人电脑或其他公共或私人场所电脑上操作，操作前应检查好个人电脑安全，禁止在未安装杀毒软件及防火墙软件的电脑上执行网站编辑操作，如对电脑安全情况不确定的应报网络中心技术协助处理，识记网站账号和密码应采取人工记忆的方式，禁止使用 word、excel 或记事本文件在电脑上以文件的形式存储，以免因电脑中病毒、木马而泄露账号密码。

4. 各网站管理的账号密码实行周期更新及复杂度要求的管理措施。明确学

校各网站使用的管理账号均应符合复杂度要求，具体如下：

- 账号名称为 admin 的均应修改为“字母+数字”组成的 6 位以上组合。
- 密码应设置为“字母+数字”组成的 8 位以上组合。
- 账号或密码不允许使用个人生日、办公或手机电话号码及 123456、nnxy 等极易被猜测的字符。
- 各网站管理账号和密码应至少每学期更换一次，以进一步强化账号密码安全。

5. 网站后台管理程序控制。为强化安全，减少隐患，各网站后台管理页面一律禁止互联网访问，有关网站的新闻编辑等管理性操作只能在校园网内进行。对于网站内容不常需要更新的网站，将关闭其后台管理，在需要更新时经该网站编辑负责人与网络中心联系后临时性开放，新闻更新后即刻关闭。

三、网站监控

1. 有效的网站监控和第一时间对黑客攻击事件及其影响的发现是网站安全工作的的重要内容。我校网站运行监控工作由网络中心具体牵头，各二级学院、处室的网站管理员及新闻信息联络员队伍也应协助对学校门户网站的运行进行监控，各二级学院及处室同时负有对本部门所用网站的运行监控职责。

2. 网站的运行监控工作暂无自动化手段，只能采用人工浏览检查网页是否正常的形式完成，要求各网站信息管理员每日最少对学校门户网站及自身所管理的二级学院或处室部门网站检查浏览 3 次以上，每日浏览和检查的时间可根据实际情况自行安排。

3. 服务器日常监控工作由网络中心负责，对服务器的开放端口及权限严格控制，执行对病毒、木马和可疑文件的每日轮询检查和查杀，每日对服务器的操作系统补丁安装情况进行检查，确保服务器安全技术保障工作仔细、全面。

4. 保卫处协助对网站进行监控。图书馆一层视频监控室内增设电脑 1 台专用于学校网站的浏览监控使用，实现网站运行的 24 小时值班监控，并填写值班监控记录，一旦发现网站异常即与网络中心取得联系。

第八章 网络安全管理制度

一、网络安全规划

网络安全与信息化领导小组办公室负责学院网络安全规划设计、建设、管理、维护等工作，确保网络设计方案符合网络安全需求。

二、网络接入和安全管理

1. 一般控制情况

(1) 对网络设备、网络设备之间的连接线缆和重要网络端口进行标识。

(2) 划分 VLAN 和安全域，VLAN 和安全域间设置访问或隔离等控制措施。

2. 校园网建设及弱电施工管理

(1) 南宁学院校园网的规划、建设和管理维护由网络中心负责。学校各项用网需求均应报网络中心统筹规划和建设落实，校内线路、光缆、服务器、网络设备及带宽等网络资源均由网络中心统筹管理和规划分配。

(2) 未经网络中心许可，任何单位或个人不得从事在私人空间或管理范围以外的弱电布线、埋管、安装等弱电施工内容，未经授权不得使用或改变校园内弱电管道、桥架、线槽、设备等公共弱电基础设施，不得改变校园网拓扑结构。确因业务要求需增设或调整网络的，均应书面提出申请，在学校批准后方可按有关规范、标准在网络中心的指导下实施。

(3) 电信、联通、移动、广电网络等运营商、银行等各类进驻校内的单位，如因业务要求需在校园内进行网络布线、基站安装、无线覆盖等弱电项目施工的，按以下规定和步骤执行。

- 施工单位或施工需求方以正式函件向学校提出施工申请，说明施工的目的、内容和方法并附施工图，涉及建筑物外立面的要提供实景效果图，施工内容较复杂的应提前与学校网络中心进行现场勘查和沟通。
- 施工申请经网络中心初审后报学校审定，批准后，网络中心向施工申请单位开具弱电施工批准单，由施工单位在批准单上备案施工负责人及联系方式后方可进场施工。

- 施工方需严格按照经过学校审核的施工图施工，施工使用到校园内弱电管道、桥架等基础设施的，需在施工中及时恢复原貌，桥架盖打开后要牢固盖回，井盖掀起后要及时牢固复原，绿化带开挖需及时修复。

(4) 校园内弱电施工原则上不允许使用重型工程机械，不允许破坏校园道路、建筑物等重要校园基础设施，有特殊情况的需在施工申请中说明，经学校审批后方可施工。

(5) 施工方要对施工安全负责，管井处施工需放置安全标识或围栏，掀起的井盖和桥架盖应妥善处置做好安全措施并及时牢固复原，因施工过程引发的安全事故由施工方负责，因未遵守施工管理要求而引发的安全事故由施工方负责。

(6) 学校保卫处配合网络中心对校园内弱电施工进行监管，对未获得施工批准单的施工项目及施工人员要坚决制止，对违反施工要求的施工问题要及时整改。

3. 校园网接入控制及管理维护

(1) 校园网的主要构成形式。南宁学院校园内网络由覆盖校园内办公（或值班）场所、教学场所、教师宿舍、图书馆、体育馆、演艺中心、活动中心等公共场所的办公教学网络和覆盖学生宿舍和大学生创业园的学生网络两种形式构成。

(2) 办公教学区、公共活动区及教师宿舍区校园网的接入方式及其管理维护。校园内办公（或值班）场所、教学场所、教师宿舍、图书馆及活动中心等公共场所的网络用户均使用场所室内固定安装的插座面板以有线的方式接入校园网。图书馆等其他由学校提供校园网无线接入的场所，用户可通过带WLAN功能的设备使用无线的方式连接指定的WIFI接入校园网。办公教学区、公共活动区及教师宿舍区的有线和无线网络直属南宁学院网络中心管理和维护，其网络故障的申报由南宁学院网络中心直接受理。

(3) 学生宿舍及大学生创业园的网络接入及其管理维护。学生宿舍及大学生创业园内的学生网络用户使用由运营商（电信、移动或联通公司）提供的网络接入服务，网络的开通和使用由学生自行向运营商申请开通并使用其提供的互联网接入服务，该部分网络的接入使用及管理维护由运营

商负责，其网络故障的申报由相应的互联网接入服务提供商（运营商）受理。

(4) 校园网接入服务的提供范围。南宁学院校园网及其设施原则上仅提供给本校教职员工及学生使用，进驻校园的任何外单位、公司、商铺及外来务工人员在未获批准的情况下均不能接入南宁学院校园网，不能使用包括插座、线路、管道、桥架、设备在内的任何校园网基础设施。外单位及外来人员上网所需的一应设备、线路及互联网接入服务等均由使用人自行解决，其网络行为由使用人自行负责。

(5) 外单位或外来人员接入使用校园网的办理要求。学校幼儿园、办学或科研合作单位以及其他进驻校园内的外单位或外来人员，因教学、科研或服务等合理需求确有必要接入和使用南宁学院校园网的，需向网络中心提交正式的书面申请，经学校批准并在财务处缴纳核定的有关资费后方可接入和使用校园网络。

4. 校园网的使用和安全管理

(1) 南宁学院校园网仅提供给校园网用户在正当的办公、教学及生活娱乐中使用，校园网的所有用户必须遵守国家有关法律、法规，严禁使用校园网从事违法违纪的网络活动，使用人需对自身提供的网络信息负责。

(2) 南宁学院校园网上的任何用户均不得利用校园网资源私设任何形式的网关或代理服务器以供其他用户上网使用，不得利用校园网从事网络资源转租、私设商业性服务器或网站等商业经营活动，不得利用校园网络提供任何带有非法内容的信息服务，如有违反，将终止该用户的校园网使用，涉及违法违规的将移交司法机关按国家有关法律法规处理。

(3) 在南宁学院校园网上不允许进行任何干扰其他用户正常用网的活动，这些活动包括但不局限于散布计算机病毒、蠕虫、木马，通过网络访问未经授权的他人电脑及各类网络设备或数据内容。校园网用户严禁使用聚生网管、网络执法官、网络剪刀手等各类网络管控工具软件以及 ARP 攻击程序和恶意流氓软件等破坏正常网络秩序的工具软件，确属用于教学、实验和研究性质需要使用此类软件的，需报网络中心批准并在实验室场所使用，否则一经定位查实将取缔违反者的校园网使用资格，造成破坏

构成违法违纪的移交司法机关按国家有关法律法规处理。

(4) 图书馆等由学校统一部署并开放无线网络的场所内，为避免信号干扰、保护信道资源，未经网络中心批准，严禁私设无线路由器、无线热点（含手机无线热点功能）及 DHCP 服务器等提供网络基础服务的设施，其校园无线网络的建设、管理、维护和服务提供统一由网络中心负责。

(5) 任何校园网用户均不能使用校园网发布反华言论、邪教言论、网络谣言、网络诈骗、黄色内容等违纪违规的网络信息，不得查阅、复制和传播有碍社会治安和有伤风化的信息，违者将视其具体性质按有关规定处理，造成违法的移交司法机关按国家有关法律法规处理。

(6) 校园网用户不得通过校园网从事任何有损公共利益或他人利益的黑客活动，不得入侵或篡改破坏任何未经授权的设备及信息系统，不能使用注入、跨站、网络窃听、中间人攻击、暴力破解等任何手段获取未经授权的信息数据，校内场所严禁未经批准的网络刺探和扫描行为，违者取缔校园网使用资格，损害公共利益的移交司法机关按国家有关法律法规处理。

(7) 南宁学院校园网的所有用户必须接受并配合国家安全部门依法进行的监督检查。

(8) 校园网用户应加强信息安全意识，加强网络和信息安全知识学习，谨防电信类诈骗信息，对个人使用和管理的计算机、服务器、平板电脑或带网络功能的各类设备要妥善管理，养成良好而安全的使用习惯，妥善保管好重要数据及银行账号、支付账号等重要虚拟资产，避免造成学校或个人的经济损失。

5. 其他事项

(1) 因教学或科研工作需要，经学校批准后由校内各单位、组织或个人自建自管的服务器及信息系统，应由该服务器或信息系统的归属部门或个人做好系统的安全保障工作，并对所提供的信息内容及其信息系统的安全负责。

(2) 因教学或科研工作需要，经学校批准后由校内各单位、组织或个人自建自管的服务器及信息系统，如需通过校园网向互联网进行信息发布以提

供互联网服务的，需向网络中心提出书面申请，在学校批准后可托管硬件至网络中心机房而后开通。信息系统所包含的操作系统、软件、程序和数据等内容的管理和维护仍由原系统所属的部门或个人通过远程桌面的方式负责管理和维护，管理者对发布的信息系统内容及信息系统安全负责，如发布的信息系统及其内容按国家有关规定需要工信部及公安备案的，需按照有关国家规定进行备案后方可通过校园网发布到互联网上。

三、网络安全审计

1. 开启网络设备日志，记录与网络安全相关的操作与活动。
2. 日志保存时间至少保证在六个月以上。
3. 在网络关键位置采取网络审计手段，对网络访问操作行为进行记录，定期对记录进行评审，将评审结果进行记录。

四、网络设备管理

1. 网络管理员负责对设备日志、网络监控情况、报警情况进行日常管理和检查，做好工作记录。
2. 网络设备尽可能采取最小服务，以提高网络设备的吞吐率和运行稳定性。
3. 阻断校外网络对管理后台的访问。
4. 设备管理人员定期对网络配置、网络设备日志进行备份，并做好备份记录。
5. 妥善保存与管理网络配置、网络设备日志及网络设备备件，保证备份的安全性。
6. 定期对配置备份及设备备件进行测试，保证其可用性，并对测试结果进行记录。
7. 定期对网络设备巡检，并形成书面维护记录，运行日志进行较长时间的保存，一般是 3 个月。
8. 及时对网络设备安装的软件进行更新。
9. 定期对设备口令进行更新。

五、网络安全检查

1. 制定详细的网络检查项目，日常检查网络系统运行情况，将检查结果进行记录。

2. 定期对网络设备配置进行检查和评估，确保网络配置与安全策略保持一致，并对检查结果进行记录。

3. 由相应管理员定期对网络系统进行漏洞扫描，及时修补网络系统安全漏洞，保存扫描记录和补丁记录。

第九章 信息系统安全管理制度

一、信息系统建设和管理的工作及责任划分

1. 网络中心是学校信息系统建设及数字化建设的牵头部门，统筹校园数字化和信息化工作。

2. 各分院、处、室可根据自身工作需要提出信息系统建设的需求，对适合本部门工作并实际需要的软件、程序或操作系统提出建设方案，具体运行实施及技术支持由网络中心统一负责。

3. 为提高软硬件资源利用率和运行效率，为现有或新建信息系统提供可靠的技术保障，各信息系统建设、运行所需的服务器、网络带宽等硬性资源由网络中心统一调配，校内资源不足的由网络中心统一提出采购或租用方案，避免各部门因自身技术能力不足而造成系统安全或运行问题，避免各自为战造成资源浪费。

4. 各信息系统的内容由使用部门具体负责，如各分院网站内容由各分院自行更新等，由网络中心提供技术支持和运行保障。

5. 各信息系统的定级、备案、评测、整改、维护工作由网络中心统筹负责。

二、信息系统安装及接入

1. 校属所有网站、信息系统等必须统一安装在标准化中心机房服务器上，以保证恒温、恒湿、不间断供电、防雷、防火、防盗、防静电等运行环境安全可靠。

2. 为提升运行效率、管理效率和服务器利用率，校属各信息系统均需采用虚拟化方式运行，统一在 SCVMM 虚拟化系统中心集中式管理，硬件资源的分配需根据各信息系统的需求及实测的平均访问流量进行优化。

3. 重要的信息系统均应通过虚拟化数据中心技术建立备机，以保障重要信息系统的数据安全和不间断运行，当主机出现故障时，负责该信息的管理员应在 1 小时内切换备机运行，并将处理情况记录上报。

4. 各信息系统所在服务器均应实现双线及双线以上的千兆校内网络接入，

以保障系统所提供的网络服务不间断运行。

5. 各服务器安装应按照用途、性能、安装方式等进行分类，安装至规划的机房区域内，机架式服务器安装应遵照操作方便、通风散热、线路平整的原则妥善部署。

6. 各信息系统均需安装在 windows 2003 server sp2 及更高版本的 windows server 平台或 red hat enterprise server 5.0 及更高版本的 red hat linux 平台上，window server 平台的磁盘分区必须为 NTFS,不可使用 FAT16 或 FAT32 等安全性不足的磁盘分区。

7. 在安装各信息系统软件前必须确保其操作系统环境已安装最新系统补丁，以保障安装环境的安全。

8. 各信息系统的安装环境上必须安装防木马及防病毒软件，并设置其病毒或木马库的自动更新。

9. 各信息系统安装的承载服务器必须采用双电源接入并保证其中至少一路为 UPS 供电接入，以保障信息系统的物理安全性。

10. 各信息系统的安装环境必须有前置防火墙保护。

11. 各信息系统的安装应遵循最小化安装原则，任何不涉及应用信息系统运行必须的程序、软件或插件均不得安装，以保证系统运行效率和安全性的最大化。

三、信息系统变更

1. 变更准备

(1) 对于标准变更，必须提前 1 个工作日提交实施方案，并通知受影响用户以及关联系统负责人。根据变更影响程度，采取相应措施，如遇变更时长超过 1 小时的的标准变更，需要发布维护公告。

(2) 重大变更实施前必须对变更对象相关配置进行临时备份，并判断是否需要发布维护公告。

(3) 变更方案应通过测试，测试结果需填写在变更申请表。

2. 变更审批

(1) 根据相关规定，提交系统变更方案进行审批，经审批后方可实施。

(2) 信息中心主任提出的标准变更不需要经过审批，与信息中心人员商定并

通过测试后实施变更，保存变更记录。

(3) 所有标准变更必须通过流程审批才能实施。变更申请人对于有固定周期、或低影响的标准变更，可将变更计划一次性提交审批。除非变更计划发生改变，否则后续变更无需再提交申请。

(4) 变更申请人必须根据变更级别定义对变更进行分级，对实施方案进行操作可行性审批。对于重要变更、工作日的标准变更必须提交变更审批人审批。

(5) 紧急变更必须由变更审批人批准，实施完毕后需补交审批流程。

3. 变更实施

(1) 除非特批，关于信息安全类的变更时间需控制在固定的时间内。

(2) 在变更实施后必须需由相关人员对影响范围内的应用系统进行验证。

(3) 变更实施人在变更成功实施后需通知变更审核人，在确认实施成功后方可结束变更，保存变更记录。

(4) 如遇变更失败需执行回退操作时，需获得变更审核人批准。失败后需查明原因，并提交相关文案。

4. 变更分类及级别定义

(1) 变更分类

根据变更的紧急程度将变更类型划分为标准变更和紧急变更，具体定义见下表：

序号	变更类型	类型描述
1	标准变更	提前计划且需通过审批的才能实施的变更。例如：硬件设备更换、防火墙策略更改等。
2	紧急变更	在变更计划之外，为应对突发的紧急情况必须立即执行的变更。例如：系统重大故障。

(2) 变更级别定义

根据变更影响程度对变更进行级别划分，具体定义见下表：

序号	级别	级别描述
1	重要	满足下列条件之一即可认为是“重要”： 1）影响学院核心业务；

		2）系统需停机时间超过 1 小时； 3）实施风险较大，易造成数据丢失，例如丢失当天业务数据。
2	一般	1）系统部分组件或集群部分主机不能提供服务，例如 Web 集群 WEB01 服务器停机维护； 2）停机时间不超过 1 小时； 3）回退方式简单，不会影响业务数据。

四、各信息系统及其依赖环境的配置及安全管理

1. 严禁使用 QQ、邮件等任何学校无主权的公众平台传播，效仿公安网络安全保卫支队做法，应最好采用纯人工方式对接，确实需要通过网络传播的应使用我校 OA 系统或我校即时协同系统发送，有关的机密性技术讨论内容应在我校即时协同系统中进行，以最大程度避免关键性信息泄露。

2. 识记系统、设备等的账号和密码应采取人工记忆的方式，禁止使用 word、excel 或记事本文件在电脑上以文件的形式存储，以免因电脑中病毒、木马而泄露账号密码。

3. 重要节点密码管理、各信息系统管理后台及操作系统账号密码必须满足复杂度要求、周期更新要求，具体为：

- 第一，账号不能设置为 admin、administator、root、cisco 等易于猜测的常用名。
- 第二，密码须由英文字母、数字、字符综合组成且密码长度不得小于 8 位。
- 第三，账号或密码不允许使用个人生日、办公或手机电话号码及 123456、nnxy 等极易被猜测的字符。
- 第四，各管理账号和密码应至少每学期更换一次，以进一步强化账号密码安全。

4. 各信息系统及其所属操作系统均应开启日志审计功能，对密码错误的登录次数进行限制，对超过限制次数的登录尝试实行挂起阻断操作。

5. 对网站等信息系统的管理后台实行登录限制，指定只有校园网内部可登录访问并更新网站内容，阻断校外网络对管理后台的访问，以保障系统不被黑客入侵发生网页篡改等事件。

6. 不可将信息系统服务程序（如 IIS 等）安装在系统分区上，需对 IIS 等服务程序的默认安装位置进行修改，安装在非系统的 NTFS 分区上。

7. 通过修改注册表或关闭服务的手段关闭各信息系统所属操作系统的默认共享，以提高操作系统的安全性。

8. 对 IIS 等应用服务程序需删除不必要的程序映射，如“.htw、.ida、.idq、.cer、.cdx、.asa、.htr、.idc、.shtm、.shtml、.stm、.printer”等以提高应用系统安全性。

9. 严格控制各信息系统目录内容的访问权限，具体规则如下。

- 第一，对脚本文件目录仅授予执行权限，关闭读取和写入权限。
- 第二，对图片上传或文件上传等目录仅授予读取和写入权限，关闭执行权限。
- 第三，对应用系统允许访问的可执行程序文件，如“.exe“等程序文件仅授予读取权限。

10. 各信息系统必须关闭其操作系统上不必要的服务、禁用如”guest”等不必要的用户，停用 netbios 等不需要的本地连接协议，仅开放必须的 TCP 或 UDP 端口。

11. 数据库系统必须修改其账号口令，sa 等高权限账号密码不可为空，其密码应满足制度中所定义的密码复杂度要求。

五、信息系统安全审计

1. 建立网络日志服务器，对各网络设备的登录、访问、修改事件进行审计记录并长期存储。

2. 建立 AAA 服务器，对网络设备和服务器的登录进行统一的认证授权和记录。

3. 建立网络流量和设备监控体系并采用液晶显示设备实时显示。

4. 定期审查应用程序日志，对可疑的入侵或非法操作行为进行跟踪，及时

掌握网络及信息系统运行状况，对校内发生的违规操作或入侵行为予以记录并形成统计，对造成恶劣影响的信息安全事件视情况报学校领导处理。

六、数据容灾备份

1. 信息数据根据系统情况和备份内容采用完全备份、增量备份、差分备份、按需备份的方式，由相关管理员根据情况选取合适的方式。
2. 一般采用自动化备份手段对数据进行定期、定时备份，减少人工干预，避免误操作。
3. 重要信息系统数据必须采用 raid5、raid1 等冗余磁盘阵列方式进行存储以保障数据安全性，避免因设备故障、恶意篡改等原因造成数据丢失及不可恢复。
4. 容灾备份采用独立设备+同步软件的方式实现，以保障其可靠性。
5. 备份数据至少保存六个月。
6. 数据恢复。

- 当信息中心服务器确认出现故障时，由系统管理员进行系统恢复。
- 系统管理员由信息中心主任指定专人负责。当人员变动时应有交接手续。
- 当网络线路不通时，网络系统维护人员应立即到场进行维护，当光纤损坏时应立即使用备用光纤进行恢复，交换机出现故障时，应使用备用交换机。
- 对每次的恢复细节应做好详细记录。
- 定期对全系统备份数据要进行模拟恢复，以检查数据的可用性。

第十章 病毒及恶意代码防范管理制度

一、病毒及恶意代码防范的日常管理

1. 安装杀毒软件的计算机，不得自行卸载或安装第二套防杀恶意代码软件，以免造成杀毒功能失效或系统不稳定情况，且任何人员不得擅自停用杀毒软件。

2. 信息系统所使用的软件必须是正式版本，不得使用测试版和盗版软件。安装重要的软件，需向网络信息中心主管提出申请，经同意后安装。

3. 定期进行培训，提高所有用户的防病毒及恶意代码意识和安全技能。

4. 相关管理员定期对网络和主机进行病毒及恶意代码检测，及时更新病毒及防恶意代码软件版本，并保存更新记录。

5. 办公、教学终端及时进行补丁升级，避免因操作系统漏洞而造成的病毒及恶意代码入侵，并做好重要数据的备份。

6. 加强计算机病毒及恶意代码、木马防范基础工作，计算机终端需设置开机密码，严格设置共享资源读、写权限；介质（磁盘、光盘和 U 盘等）复制、使用前先作病毒及恶意代码检测，确认无病毒及恶意代码后才能使用。

7. 局域网与互联网之间实施物理隔离，连接互联网的终端用户不许下载和运行来历不明的程序,对于不明来历的邮件附件也不要随意打开。下载的软件、信息和数据要先查毒后使用。

8. 对移动介质、移动设备接入网络要进行严格控制，避免因上述原因发生病毒及恶意代码感染事件。

9. 因工作需要不得不使用的移动介质（设备）的，必须由使用人递交介质使用申请，获网络中心主管批准，并将介质进行恶意代码检测，确认无毒后，方可接入指定网络内使用。

10. 定期检查网络内服务器的杀毒软件运行状态，并将检查结果进行记录。

二、病毒及恶意代码的查杀与处理

1. 一旦发生病毒及恶意代码入侵事件，必须立即上报相关管理人员，并采取措施进行病毒及恶意代码查杀工作，如下载专杀工具、进行手工杀毒等。

2. 一旦部门局域网内计算机发生感染病毒及恶意代码疫情，为避免计算机疫情扩散，将封堵该部门局域网与业务网之间的物理链路，待采取进一步措施查杀灭病毒及恶意代码，在疫情警报解除后，再恢复网络间物理链路的连接。

第十一章 信息安全事件管理制度

一、信息安全事件的定义和范围

1. 信息安全事件是指对任何信息技术资源合法使用、操作造成威胁的事件，或对信息技术资源具有潜在危险的任何一种情况。

2. 信息中心负责信息安全事件的接报、汇总、通报和处置工作。信息中心负责信息安全事件协调，网络安全与信息化领导小组办公室安全合规岗位配合。

3. 信息安全事件包括，但不限于：

- 系统感染计算机病毒。
- 学院网络遭遇外部入侵或攻击。
- 内部人员、承包方人员和第三方人员利用学院网络进行破坏。
- 信息系统敏感数据泄露或失窃。
- 学院数据处理设备失窃。

4. 符合以下条件之一的信息安全事件必须报告领导：

- 导致计算机重要信息系统中断或运行不正常超过 30 分钟。
- 严重威胁学院信息、信誉安全。
- 因计算机安全事件造成学院不能正常使用，且影响范围影响区域。

二、信息安全事件的监控和处理

1. 安全事件管理分为安全事件监控和安全事件处理。安全事件监控完成对安全事件迹象的检测和分析，发现和报告安全事件的存在。安全事件处理是对被发现的安全事件的响应处理过程，包括四个主要阶段：控制、证据收集、根除与恢复以及事后分析。

2. 安全事件监控包括信息安全事件监测、预测和预警，应按照“早发现、早报告、早处置”的原则，加强对各类信息安全事件和可能引发信息安全事件的有关信息的收集、分析判断和持续监测。

3. 职工发现学院发生信息安全事件后，需向中心应急联络员报告，确认故障情况，确认故障处理时间，准确定性故障级别。

4. 学院信息系统运行环境出现的安全事件按照相关规定执行。

5. 应急联络员接到报告后，需立即采取措施控制事态，如断开受病毒感染的系统的网络连接，及时通知信息中心和用户部门负责人，协调控制事件的影响。保留相关的防火墙、路由器、入侵检测系统、操作和应用系统日志等，以备检查。

6. 应急联络员根据事态发展，协调信息中心相关科室进行事件处理和平息，并及时向信息中心主管报告事件发展情况。

7. 应急联络员在事发 24 小时内，向信息中心提交信息安全事件报告，填写《信息安全事件报告》，信息安全事件报告包括以下内容：

- 信息安全事件发生的时间、地点、单位、单位负责人和联系方式。
- 信息安全事件的类别、涉及软硬件系统的情况和事件发生的过程。
- 信息安全事件造成的后果和影响范围。
- 信息安全事件发生的根本原因。
- 责任人或涉案人员。
- 信息安全事件发生后采取的应急措施。
- 未来的防范措施。

三、信息安全事件监督和总结管理

1. 为预防同样信息安全事件的再次发生，信息中心安全合规岗应按《南宁学院信息安全管理制度》的规定，不定期进行抽查，对各项制度、计划、方案、人员和物资等方面进行验证。对于发现的安全弱点应及时上报信息中心相关负责人。对未有效落实事件处理方案及预防措施和有关规定的内部人员进行通报批评。对于承包方或第三方服务商产生的安全弱点通报其项目负责人，并督促其限时整改，逾期未整改完成的将按照相关外包管理规定对其所在公司进行处罚直至终止合同。

2. 信息中心人员、承包方人员、第三方服务商人员、驻学院服务人员等信息中心范围内人员，有义务对发现的安全弱点及时上报相应信息中心负责人。相关小组对发现的安全弱点应及时进行整改处理，避免信息安全事件的发生。

3. 信息中心应将信息安全事件的应急管理和工作流程等作为信息安全风险培训的内容，增强信息安全事件处置工作中的组织能力。

第十二章 信息安全应急管理制度

一、突发事件分类

1. 自然灾害：指地震、火灾等因自然因素引起的网络与信息系统的损坏。

2. 事故灾难：指电力中断、网络损坏、软件、硬件设备故障等引起的网络与信息系统的损坏。

3. 人为破坏：指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

4. 根据《信息安全事件分类分级指南》（GBZ 20986-2007），将信息安全事件分为以下几类：

(1) 有害程序事件（MI）

(2) 网络攻击事件（NAI）

(3) 信息破坏事件（IDI）

(4) 信息内容安全事件（ICSI）

(5) 设备设施故障（FF）

(6) 灾害性事件（DI）

(7) 其他事件（OI）

二、职责

网络安全与信息化领导小组办公室、应急小组负责研究制订信息安全应急处置工作的规划、计划和应急预案，制定应急预案演练计划和应急预案具体实施工作。

三、事件分级

1. 根据信息安全突发事件的可控性、严重程度和影响范围，将网络信息安全突发事件分为四级：I 级（特别重大）、II 级（重大）、III 级（较大）、IV 级（一般）。具体级别定义如果国家有关法律法规有明确规定的，按国家有关规

定执行。

2. Ⅰ级（特别重大）：造成学院信息系统发生大规模瘫痪，事态的发展超出区一级相关主管部门的控制能力，对国家安全、社会秩序、公共利益或学院形象造成特别严重损害的突发事件。

3. II 级（重大）：造成学院重要信息系统瘫痪，对国家安全、社会秩序、公共利益或学院形象造成严重损害，需要上级部门或公安部门协助，乃至需跨地区协同处置的突发事件。

4. III 级（较大）：造成学院信息系统瘫痪，对国家安全、社会秩序、公共利益或学院形象造成一定损害，但只需在技术支持单位和信息中心协同处置的突发事件。

5. IV 级（一般）：造成学院信息系统受到一定程度的损坏，对本单位的权益有一定影响，但不危害国家安全、社会秩序和公共利益，可由网络信息中心自行处置的突发事件。

四、信息与网络安全突发事件处理原则

1. 预防为主。立足安全防护，加强预警，重点保护基础信息网络和关系信息安全、稳定的重要信息系统，从预防、监控、应急处理、应急保障等环节，在管理、技术、人员等方面采取多种措施充分发挥各方面的作用，共同构筑信息与网络安全保障体系。

2. 快速反应。突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。 第十六条 分级负责。按照“谁主管，谁负责”的原则，建立和完善安全责任制及联动工作机制。根据各负责人的职能，各司其职，加强各负责人的协调与配合，共同履行应急处置工作的管理职责。

3. 以人为本。把保障人员以及公共利益的安全作为首要任务。

4. 常备不懈。加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

五、监督管理

1. 加强对信息安全等方面专业技能的培训，指定专人负责安全技术工作。并将信息安全突发事件的应急管理、工作流程等列为重要培训内容，增强应急处置工作中的组织能力。

2. 应急预案定期演练。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

第十三章 附　　则

1. 本标准由网络信息中心负责解释。
2. 本标准自颁布之日起实行。