南充文化旅游职业学院文件

南文旅职院发〔2023〕31号

南充文化旅游职业学院
关于印发《南充文化旅游职业学院网络安全管理制度（试行）》的通知

各系（部、院）、部门：

经学院2023年意识形态专题会审议、批准，现将《南充文化旅游职业学院网络安全管理制度（试行）》印发大家，请严格贯彻执行。

特此通知。

南充文化旅游职业学院

2023年7月4日

南充文化旅游职业学院
网络安全管理制度（试行）

第一章　总　则

第一条 为深入贯彻落实网络安全政策文件要求和网络安全等级保护政策要求,加强南充文化旅游职业学院的网络安全管理工作,增强学院全体师生网络安全意识,切实提高学院信息系统安全保障能力，特制定本制度。

第二条 本制度适用于南充文化旅游职业学院网络安全管理工作。

第三条 南充文化旅游职业学院网络安全与信息化工作领导小组负责本制度的审核和修订,由领导小组办公室负责本制度的贯彻和执行。

第四条 本制度主要遵循《信息安全技术——网络安全等级保护基本要求（GBT 22239-2019）》标准的要求，同时在部分环节也符合以下两个国际标准。

ISO/IEC 27001 信息安全管理体系要求。

ISO/IEC 27002 信息安全、网络安全和隐私保护——信息安全控制。

第二章　网络安全方针

第五条 南充文化旅游职业学院总体安全方针为：提高全体师生网络安全风险意识，确保信息系统安全；坚持以人为本，强化网络安全管理。

第三章　安全管理制度

第六条 网络安全策略

网络安全是南充文化旅游职业学院稳定运行的重要保障，学院将遵照“统一规划、分级管理、积极防范、人人有责”的原则，通过风险评估和风险管理，采取一切可能的措施，加强学院网络安全的建设和管理。

南充文化旅游职业学院网络安全与信息化工作领导小组是学院网络安全与信息化工作的最高机构。网络安全与信息化工作领导小组办公室（以下简称“网信办”）是学院网络安全日常工作和执行机构。

南充文化旅游职业学院全体师生均有参与网络安全管理、保护学院网络安全的义务和责任。全体师生应积极参加各种形式的网络安全教育和培训，遵守相关国家的法律法规、行业规范和学院各项相关制度。

承载信息系统的所有软硬件设施及物理环境均应受到适当的保护。

采取必要的措施保护南充文化旅游职业学院信息的机密性，

以防止未经授权的不当存取。同时应确保信息不会在传递的过程中，或因无意间的行为透漏给未经授权的第三者。

采取必要的措施确保南充文化旅游职业学院信息的完整性，以防止未经授权的篡改。

采取必要的措施确保南充文化旅游职业学院信息的可用性，以确保使用者需求可以得到满足。

采取必要的措施确保南充文化旅游职业学院信息的连续性，以确保业务持续可用。

南充文化旅游职业学院相关的网络安全措施或规范应符合现行法律法规的要求。

南充文化旅游职业学院全体师生都有责任通过适当的上报机制，报告所发现的网络安全意外事故或网络安全弱点。

任何危及网络安全的行为,都应诉诸适当的惩罚程序或法律行动。

第七条 网络安全目标

最大限度保证信息系统的完整性、保密性和可用性免遭破坏。确保每年网络安全重大事故的发生频率为可控范围内的最低，目标为**“0”**次。

第八条 网络安全管理框架

南充文化旅游职业学院网络安全管理框架是根据 **ISO/IEC 27001**《信息安全管理体系标准要求》中的控制目标和控制项，

并结合南充文化旅游职业学院的实际情况所建立的。符合“PDCA”的管理模式。

P（PLAN）过程是计划过程，指统一规划和设计南充文化旅游职业学院的网络安全目标和安全控制策略,指导南充文化旅游职业学院整体的网络安全管理工作。

D（DO）过程是执行过程，指南充文化旅游职业学院在开展网络安全工作中需要落实的管理要求，包括网络安全制度管理、人员安全管理、系统建设安全管理、信息系统运维管理、变更管理和信息资产安全管理等，指导日常的网络安全管理工作。

C（CHECK）过程是检查过程，指南充文化旅游职业学院开展网络安全工作的持续改进机制，通过网络安全风险评估、等级保护测评、检查，监督和审核等方式，指导网络安全管理体系控制要求不断完善。

A（ACTION）过程是处置过程，指南充文化旅游职业学院网络安全事件处置和应急预案，通过发现和总结网络安全问题，形成新的管理办法和控制措施,确保网络安全管理体系的适用性和有效性。

南充文化旅游职业学院网络安全管理框架通过 PDCA 各环节的不断完善，实现网络安全管理体系自身的持续改进，从而提高网络安全管理体系的全面性、有效性和适用性。

第九条 网络安全管理原则

主要领导负责原则:网络安全与信息化工作领导小组的主要领导确立南充文化旅游职业学院网络安全保障的宗旨和政策,负责提高全员的安全意识,组织有效的安全保障队伍,调动并优化配置必要的资源,协调安全管理工作与各部门工作的关系,并确保其落实、有效;

全员参与原则:跟核心业务信息系统相关的所有运行维护人员应普遍参与信息系统的安全管理,并与相关方面协同、协调,共同保障信息系统安全;

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命周期,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,维护和持续改进网络安全管理体系的有效性;

依法管理原则:网络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;

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;

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。

第十条 文件评审及发布制度

（一）体系文件生命周期流程

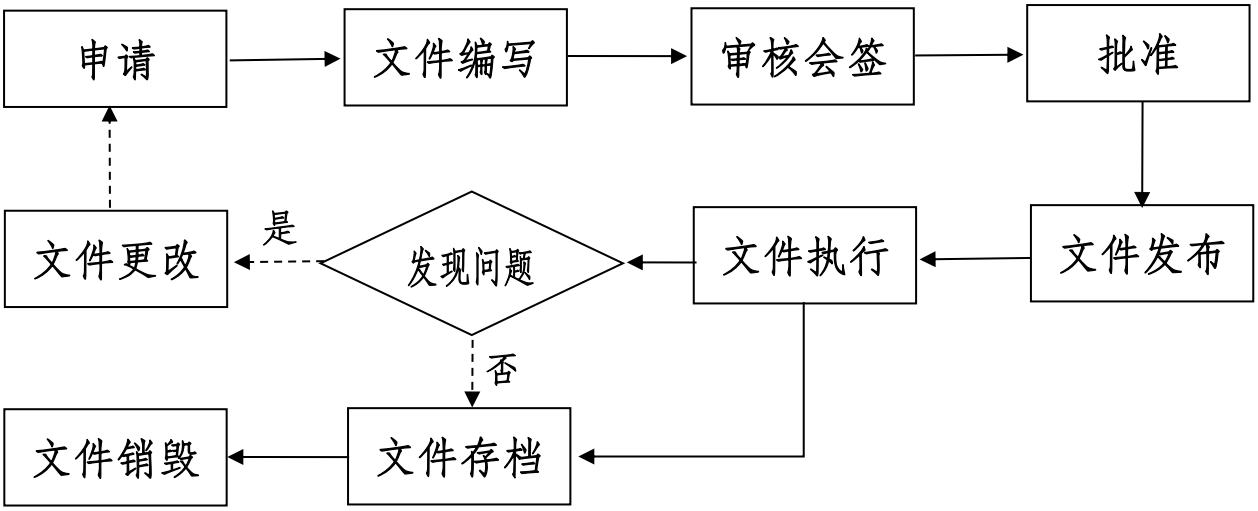

图 1 体系文件流程图

（二）体系文件策划

网信办组织相关人员，根据《信息安全技术——网络安全等级保护基本要求（GBT 22239-2019）》《信息安全技术 信息系统安全管理要求（GBT 20269-2006）》《ISO/IEC 27001 信息安全管理体系》的要求，结合实际的职责和工作流程，策划制定网络安全管理体系文件的架构，并形成《南充文化旅游职业学院网络安全管理体系文件框架》（以下简称“文件框架”）。

网信办将制定的文件框架汇报给网络安全与信息化工作领导小组,网络安全与信息化工作领导小组对文件框架进行审批确认。

（三）体系文件架构与编写

网信办根据审批后的文件框架及清单,负责组织编写各类文件。总策略文件为《网络安全方针与安全策略》《网络安全与信息化领导机构组成与职责》，它定义了安全管理的基本原则、基本方向、安全管理的组织框架和职责划分等。程序规范类文件主要包括《人力资源安全管理程序》《系统建设管理》《物理与环境安全管理》等管理标准文件，主要规定了各个领域的安全管理的基本原则和目标。记录类文件主要是各个领域安全管理的过程文档，是整个安全管理体系有效执行和落地的主要手段，也是安全管理体系的过程记录，可作为对外的网络安全质量保证。其中总体策略类文件由网络安全与信息化工作领导小组署名,其他类文件由职能部门署名。编写完成的文档需先经过各相关部门的初审，然后由网信办进行评审，最后由网络安全与信息化工作领导小组进行批准定稿，并形成评审记录表。

（四）体系文件的评审

网信办应定期发起对体系文件的评审,对体系文件的评审应至少每年进行一次。评审流程如下：

1. 网信办发起对体系文件的评审申请，网络安全与信息化

工作领导小组审核确认后批准评审要求。

2. 网信办制定评审计划。计划中应确定各文档对应的评审责任人以及实施评审的时间计划。

3. 各评审责任人根据时间计划，结合内部审核、管理评审、风险评估及日常记录的结果，评估现有文件的有效性和充分性。如果确定文档有必要进行修改，应填写《制度文件修订记录》。

4. 如果修改的内容只涉及网络与信息化中心，则由网信办主要负责人进行审批，在审批同意后，由文档评审责任人进行修改。

5. 如果修改的内容涉及到网络与信息化中心以外的部门，需要所有涉及部门的会签。会签后，由文档评审责任人进行文档修改。

6. 修改完毕之后，各责任人将《制度文件评审记录》和完善后的体系文件版本一并报送网信办，由网信办进行标识和保存。

7. 网信办最终对评审结果向网络安全与信息化工作领导小组进行汇报。

（五）体系文件的作废

1. 在体系文件的评审过程中，如果评审责任人认为文件应当作废，则填写《体系文件作废申请表》，由网信办审批后，报网络安全与信息化工作领导小组进行审批。

2. 网络安全与信息化工作领导小组审批完成后，网信办负责通知所有相关人员，并对《南充文化旅游职业学院网络安全管理体系文件框架》进行更新。

第四章　安全管理机构

第十一条 网络安全与信息化工作领导小组办公室是学院网络安全与信息化领导小组的日常工作和执行机构，负责贯彻落实领导小组的决策部署和学院网络安全的管理工作。

第十二条 网信办主任职责

主任：直接对网络安全与信息化工作领导小组负责，负责网络安全与信息化工作领导小组宏观策略和项目规划的落地执行；在网络安全与信息化领导小组的领导下，协调网信办工作成员完成方案起草，流程收集，需求汇总等工作；协调网信办工作人员的工作分配，人员管理等。

副主任：协助网信办主任完成宏观策略和项目规划的落地执行，任命网络安全角色和岗位，并明确各网络安全岗位的职责，组织并实施网络安全管理评审，督促各成员统一协作，完成方案起草，流程收集，需求汇总等工作。

第十三条 网信办工作人员职责

负责系统调试、日程维护、人员培训、人员组织、安全管理等具体工作。具体职责如下：

（一）负责网络安全体系建设具体工作实施和推进，与工作

小组组长及时沟通并汇报有关情况。

（二）负责与相关公司沟通协调项目实施情况以及项目在单位内部的推进和后续知识转移。

（三）负责安全管理体系的建立并监督网络安全管理制度的执行。

（四）对网络安全相关项目进行规划和监督，确保网络安全风险评估和管理工作能够落实。

（五）制定年度评审计划，确定评审范围和内审内容。

（六）负责网络安全策略、标准、流程和制度的编写、审核及推广。

（七）制定业务连续性计划。

（八）建立与内部/外部专家、权威机构、利益伙伴之间的沟通渠道，统一控制对外信息发布和通告。

第十四条 网络安全例会管理

（一）网络安全与信息化工作领导小组负责高层网络安全例会的发起，网信办负责中层网络安全例会的发起，负责中高层网络安全例会记录工作、与外部相关单位的沟通与协作管理。

（二）中层网络安全例会由网信办负责发起，至少每半年需要组织一次常规的网络安全例会，例会参会人员至少要包括网信办主要成员和执行层各角色的管理人员。在发生小范围内网络安全事件时如需要，网信办可随时召集发起网络安全工作会议，通

知相关人员参加,就网络安全管理各项制度和执行情况做出及时调整和部署。

（三）常规的中层网络安全例会的主要内容是就各阶段的网络安全检查结果进行上会检查和审批,对网络安全检查中发现的各项问题提出解决办法和规避措施,对外包运维人员的工作内容进行确认和审核,就发现的各类网络安全问题及时提出解决方案并落实到相关责任人。

（四）遇有工程或项目时,可根据工程和项目进度情况或者工程和项目的需要随时召开网络安全例会,且可不拘泥于网信办范围，可召集相关的合作单位、合作方、内部相关部门的相关人员一起参加网络安全例会，并做好例会的记录工作。

（五）高层网络安全例会由网络安全与信息化工作领导小组负责发起，至少每年需要组织一次常规的高层网络安全例会，例会参会人员包括网络安全与信息化工作领导小组主要成员。在发生大范围的网络安全事件、有重大网络安全事件发生、或者有重大信息系统建设项目时，如有必要，由网络安全与信息化工作领导小组发起，或者由网信办提议，由网络安全与信息化工作领导小组发起高层网络安全与信息化工作领导小组会议,通知相关人员参加，及时协调各方资源，共同协作，解决相关问题，或完成各项部署。

（六）常规的高层网络安全例会的主要内容是听取网络安

全与信息化工作领导小组的网络安全工作季度报告,就网络安全各项工作根据报告提出调整和解决方案,并协调各方资源,共同协作,完成各项网络安全工作。高层网络安全例会的另一重要内容是就网络安全管理体系的各项管理制度,根据运行中发现的问题,及时进行调整和部署,不断完善学院网络安全管理体系。

第十五条 外部协作管理

网信办负责建立并保持与兄弟单位、公安机关、通讯公司等对口单位的合作与沟通,就兄弟单位的成熟经验、政策法规、当前的信息热点事件展开交流与合作。如交流与合作内容比较正式,且有正式的会议形式,则需做好会议记录工作,会议记录的模板可用网络安全例会的模板代替,但会议主题需注明为“合作沟通”。

第五章　人员安全管理

第十六条 网络安全人员管理制度

(一)网络安全岗位人员任职期间及离职时的考核管理由网信办负责。

(二)网信办心须与信息系统关键岗位人员签订保密协议。

(三)各信息系统使用部门负责本部门人员的日常管理工作。

第十七条 网络安全培训管理

网信办负责制订各类岗位和人员的网络安全相关培训计划,

并按照计划执行各种形式的网络安全培训。各部门负责人协助网信办开展覆盖本部门范围的相关安全培训，全体师生积极参加网信办组织的各类网络安全培训。

第十八条 网络安全意识培训

（一）网络安全意识培训对象

南充文化旅游职业学院全体师生都应接受网络安全意识的培训。

（二）网络安全意识培训时机

新入职职工在上岗前都应接受网络安全意识培训；

针对现有师生，网信办应确保每年至少提供一次基础的网络安全意识培训，以确保所有师生都保持必要的网络安全意识。

第十九条 网络安全技术培训

（一）网络安全技术培训对象

网络安全技术培训对象主要是网信办的技术人员，各处室信息专员。

（二）网络安全技术培训时机

网络安全技术人员在上岗前都应接受网络安全技术培训；

针对现有的网络安全技术人员，应确保每年至少提供一次基础的网络安全技术培训；

当出现新的网络安全技术时，应确保所有的网络安全技术人员参加相应的培训。

第六章　系统建设管理

第二十条 安全方案设计

（一）应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；

（二）应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

（三）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

（四）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

（五）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第二十一条 自行软件开发

（一）应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；

（二）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

（三）应制定代码编写安全规范，要求开发人员参照规范编写代码；

（四）应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

（五）应确保对程序资源库的修改、更新、发布进行授权和批准。

第二十二条 系统交付

（一）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

（二）应对负责系统运行维护的技术人员进行相应的技能培训；

（三）应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；

（四）应对系统交付的控制方法和人员行为准则进行书面规定；

（五）应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

（六）系统建设完成后，项目承建方要依据项目合同的交付部分向网络与信息化中心进行项目交付，交付的内容至少包括：

1. 制定详细的系统交付清单，对照系统交付清单，对交付的设备、软件和文档进行清点；

2. 制定项目培训计划，对系统运维人员进行技能培训，目标是经过培训的系统运维人员能胜任日常的运维工作；

3. 提供系统建设的各类过程文档，包括但不限于：实施方案、实施记录等；

4. 提供系统运行维护的帮助和操作手册；

5. 系统交付过程文档必须有项目承建方和网络与信息化中心双方项目负责人进行签字确认；

6. 系统交付工作由网络与信息化中心、系统交付商共同参与，双方签字后，交付物交由网络与信息化中心管理。

7. 必须安照系统交付的要求完成交付工作。

第七章　系统运维管理

第二十三条 计算机设备使用规范

（一）计算机主机的放置必须与音箱、打印机等设备保持适当距离，以防止信号相互干扰及过热现象。

（二）计算机及其外部设备必须放置在干燥、通风凉爽、避免阳光直晒的地方，以防止潮湿引起电路短路。

（三）计算机及其外部设备必须定期进行清洁除尘工作，以保持其干净清洁。

（四）开机时应该先给外部设备加电，然后才给主机加电。

（五）在电脑运行过程中，机器的各种设备不得随便移动，严禁带电插拔各种接口卡（**USB** 接口除外），严禁带电装卸外

部设备和主机之间的信号电缆。如有上述动作，则必须关机断开电源进行操作。

（六）不得频繁开关机。关机后如果需要重新启动设备，则应该在关闭计算机主机后等待 10 秒钟以上后重新开机。

（七）计算机病毒防治。计算机病毒一般通过数据交换的途径传播，尤其盗版软件与网络是病毒传播的重要途径。因此，计算机的防病毒应做到以下几点：

1. 使用统一防病毒软件进行查杀。

2. 定期更新病毒库。

3. 不得使用未经网络与信息化中心批准的软件。

4. 避免与可能有病毒的计算机交换数据

5. 不打开未知邮件，计算机出现提示时应看清内容、弄清原因再确认

6. 发现计算机病毒应当及时清除；无法清除的，应当及时通知网络与信息化中心，并采取断网等隔离措施，防止再次对有毒数据进行访问。

（八）其它

1. 定期对计算机重要数据进行备份，防止因计算机故障及其它原因造成的数据丢失。

2. 严禁在计算机上安装游戏软件。

3. 严禁在计算机上安装非法盗版软件，凡在计算机上安装

非法盗版软件造成版权问题的,属于个人侵权问题,与学院无关。

4. 严禁随意对学院计算机软件或其它数据进行更改、删除、卸载。

第八章　解释与施行

第二十四条 本制度由网络安全与信息化领导小组办公室负责解释。

第二十五条 本制度自印发之日起施行。

南充文化旅游职业学院办公室　　2023年7月4日印发