**新疆师范大学网络与信息安全管理办法**

（经2018年1月17日第二次校长办公会议审议通过）

1. **总则**
2. 为加强学校网络与信息安全管理工作，提高校园网络安全防护能力和水平，稳步推进我校信息化建设，保障我校教育事业健康有序发展。根据《中华人民共和国网络安全法》、《教育部关于加强教育行业网络与信息安全工作的指导意见》和《新疆维吾尔自治区网络安全管理条例》等法律法规及工作要求，结合学校实际情况，特制定本管理办法。
3. 本办法所称网络与信息安全工作是指为保障学校信息化的基础设施和信息系统安全和稳定运行，网络数据的完整性、保密性和可用性，有效应对网络安全事件，防范违法犯罪活动而采取的管理和技术防范措施。网络安全工作保护主体包括：校园网络、数据中心、网站、信息系统及系统所产生的数据、终端计算机、存储介质、网络与信息系统运行日志数据等；涉密的网络与信息安全等不在本办法管理范畴内，由学校相关部门根据《新疆师范大学保密规定》进行管理。
4. 学校按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全的网络与信息安全责任体系，学校各单位和全体师生应按照本办法的要求履行网络与信息安全的责任。
5. **组织领导与职责**
6. 网络安全和信息化领导小组是学校全面推进网络安全和信息化建设的最高管理与决策机构，负责确定学校网络安全和信息化建设战略方向，审定学校信息化建设的总体规划及对信息化建设中重大项目进行决策，批复全校网络安全和信息化建设项目经费。
7. 网络安全和信息化专家咨询组是学校网络安全和信息化建设重大技术问题的论证机构和重大管理事项的专家咨询机构，负责学校网络安全和信息化建设的总体规划的审议、负责学校信息化建设项目的审议、立项、论证。
8. 网络安全和信息化管理办公室（以下简称“网信办”）是学校网络安全和信息化建设管理的具体实施、执行机构，负责学校网络安全总体规划设计，统筹管理学校网络与信息安全建设经费，拟定网络与信息技术安全管理规章制度，组织开展信息系统安全等级保护和关键信息基础设施运行安全检测评估工作，组织网络安全宣传和教育培训工作，监督检查各单位网络安全工作。
9. 信息管理中心负责学校网络安全保障体系的建设、运行维护、技术指导和服务支持；监测、跟踪网络运行状态，记录网络安全事件的技术措施，按照规定留存不少于六个月网络日志并实施可回溯机制。
10. 学校主要负责人是学校网络与信息安全的第一责任人，各单位主要负责人是本单位网络安全和信息化工作的第一责任人，负责落实网络与信息安全工作。
11. 学校各单位设信息技术人员，由本单位具有一定计算机能力且沟通协调能力较强的人员担任，负责本单位网络与信息安全工作的具体实施。
12. **校园网络运行安全管理**
13. 校园网络是指校园范围内连接各种信息系统及信息终端的计算机网络，包括校园有线网络、无线网络、虚拟网络和专用网络。
14. 校园网络基础设施由学校统一规划、建设、管理，提供统一互联网出口、统一安全防护，校内各单位及个人不得擅自建设、更改、损毁、挪用校园网设施，不得私接外网出口。运营商网络的引入需要提交网络安全和信息化领导小组讨论决策。
15. 校园网入网实行“实名注册、认证上网”，未经登记不得以任何方式私接校园网，严禁借用或盗用其他用户上网账户使用校园网，严禁使用无线路由器或网络代理上网。
16. 校园网用户应文明上网，规范网络行为，保护个人账号并定期修改密码。校园网用户的上网行为不得危害到学校网络安全和国家网络安全，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等网络攻击活动。
17. 校园网主要服务于学校教学、科研及校务管理等，用户不得将校园网用于其他用途，严禁利用校园网开展各类未经许可的其它网络服务。如在教学、科研上确有特殊需求，需要用户IP地址对外开放服务，信息管理中心审批后可开放，建设单位或个人承担全部网络安全责任。
18. **数据中心安全管理**
19. 数据中心主要包括支撑学校信息系统的物理环境（如机房）、网络设施、服务器、存储、云计算平台、学校中心数据库（其中包含基础数据库）、数据共享交换平台、统一身份认证平台及统一信息门户等关键信息基础设施。信息管理中心负责数据中心的建设、运行、维护和安全管理。
20. 原则上，学校各单位应依托学校数据中心开展信息系统建设，需使用校外数据中心的，须报网信办审批。涉及学校基础数据、师生个人信息（含成人教育、留学生教育、函授培训、预科教育等学生个人信息）或敏感信息的信息系统，不得部署在校外数据中心。
21. 信息管理中心对学校数据中心的使用实施准入管理，负责制定使用数据中心的技术规范和标准，计算资源和存储管理办法、服务器托管的管理办法和服务器购置技术规范。在服务器及系统上线前进行安全检测，符合技术规范标准并检测合格的服务器及系统方可进行托管运行。
22. 数据中心的资源使用（计算资源、存储资源、网络资源）单位应遵循数据中心相关管理制度和技术标准，按需申请，有序使用，不得利用数据中心资源从事任何与申请项目无关或危害网络与信息安全的活动。
23. **信息系统建设与运行安全管理**
24. 校内各类信息系统原则上应依托于学校数据中心建设，使用学校域名并进行登记备案。对于特殊用途的系统需经网信办审核报学校网络安全和信息化领导小组讨论后再行决定，一切责任由建设单位或个人承担。
25. 学校按照同步规划、同步建设、同步运行的原则，规划、设计、建设、运行、管理信息安全设施，建立健全信息技术安全防护体系，全面实施信息系统安全等级保护制度。
26. 信息系统在建设阶段应先由建设单位确定安全保护等级，按照等级保护要求同步落实安全保护措施。信息系统投入试运行后，由建设单位初步验收，出具初步验收报告。对于安全等级第二级以上（含第二级）的信息系统，由信息管理中心组织等级测评，信息系统通过初步验收和信息安全保护等级测评后，由网信办组织竣工验收。
27. 信息系统开发环境、测试环境和生产环境应严格隔离，信息管理中心负责上述环境的建设、运行、维护和管理。
28. 信息系统建设单位可自行或委托信息管理中心维护信息系统；亦可根据实际需要，委托外单位维护信息系统，签订合同后报网信办。
29. 信息系统建设单位应制定信息系统使用与维护的管理制度，规范信息系统使用者和维护者的操作行为。
30. 信息系统运维采用审批授权，运维人员统一通过运维安全审计平台在线管理信息系统。网信办负责管理权限的审批及监督，信息管理中心负责远程运维管理系统的账号分配及授权、运维和管理。
31. 对于安全等级第二级以上（含第二级）的信息系统，信息管理中心将定期组织开展等级测评，查找，发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，四级系统应每年进行两次测评，三级系统每年进行一次测评，二级系统每两年进行一次测评。
32. **信息系统数据安全管理**
33. 信息系统数据是指信息系统收集、存储、传输、处理、检索和运行过程中产生的电子数据，包括：信息化公共基础服务和各单位的管理信息系统的数据、校园一卡通、网站内容、教学资源和网络课程、数字化图书资源、日志记录等。数据安全管理是对信息系统各类数据及运行日志的敏感性、隐私性、安全性和可用性的保护。
34. 信息系统数据的所有者是数据安全管理的责任主体，应当落实管理措施，规范数据的收集、存储、传输和使用，确保数据安全和数据防泄露。
35. 信息系统数据收集应遵循“最少够用”原则，不得收集和信息系统业务服务无关的个人信息，敏感数据必须加密，并具有不可逆推导能力。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。
36. 信息管理中心负责学校核心信息系统的备份、容灾与恢复管理，制订备份、容灾与恢复计划，根据业务实际需求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，并确保备份数据和备用资源的有效性。加强人员对数据安全意识和安全技术培训，杜绝从内部泄露数据的风险。
37. **网站安全管理**
38. 学校各单位开办互联网网站应按照《新疆师范大学网站群管理办法》执行，实行二级网站管理备案制，提交二级网站开通申请表和二级网站备案信息登记表至网信办。网站的备案信息发生变更、网站更改和停用等及时向网信办反馈。
39. 学校各单位网站建设优先纳入网站群，站群不满足业务需求时可协商解决，信息管理中心负责站群平台的技术安全和数据安全。单独建设的网站，在上线前，需通过安全检查方可正式上线，网站安全和数据备份由建设单位负责，服务器资源由学校数据中心提供。
40. 学校网站及各单位网站的信息发布严格实行归口管理，各单位发布至学校门户网站上的新闻由宣传部审核发布，严格遵守“上网的信息不涉密、不违法、不违规”的原则。
41. 实现二级网站年审制，网信办每年对所有二级网站进行清查，有权对无责任人、一年内无更新内容的网站进行关停。
42. 对于使用频度不大、阶段性使用的网站，网站建设单位可采取特殊时段，关闭的方式运行。对于无人管理、无力维护、长期不更新的网站，信息管理中心将执行关闭网站以降低安全风险。
43. **校园终端设备安全管理**
44. 校园终端设备是指由学校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、手机、平板等各类接入校园网的设备。
45. 终端使用人按照“谁使用，谁负责”的原则，应做好终端设备的安全防范，严禁利用校园终端设备传播非法信息、暴恐音视频文件、散播谣言、色情、赌博、暴力等。
46. 信息管理中心建立终端统一管理平台，实现常用正版软件下载分发、系统补丁分发、病毒软件安装升级及漏洞管理等功能。
47. **存储介质安全管理**
48. 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盘等可移动存储介质。
49. 原则上，存储阵列、磁盘库等大容量介质应托管在学校数据中心，并由信息管理中心统一运行、维护和管理。信息管理中心应采取必要技术措施防范数据泄露风险，确保存储数据安全。
50. 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。
51. **人员安全管理**
52. 学校各单位应建立健全本单位的信息安全岗位责任制度，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信息系统管理人员应签订信息安全与保密协议，明确信息安全与保密要求和责任。
53. 学校各单位应加强人员离岗、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，收回校园卡以及学校提供的软硬件设备及信息系统管理权限，并签署安全保密承诺书，做好交接工作。
54. 网信办定期组织相关网络信息安全培训，对安全知识和技能进行考核，并对考核结果进行记录和保存。
55. 应建立外部人员访问数据中心机房等信息化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。
56. **外包服务安全管理**
57. 信息技术外包服务是指信息系统的开发和运维的外包。
58. 外包服务需求单位应与信息技术外包服务提供商签订服务合同和信息安全与保密协议，明确信息安全与保密责任，要求服务提供商不得将服务外包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的信息资产，不得以服务为由强制要求委托方购买、使用指定产品。
59. 信息技术外包服务合同和信息安全与保密协议应按学校合同管理办法的有关要求，报网信办审核。
60. 外包开发的系统、软件上线应用前，外包服务需求单位应组织安全检查，要求开发方在服务期限内及时提供系统、软件的升级、漏洞等信息和相应服务。
61. **网络与信息技术安全教育培训**
62. 网信办负责组织学校网络与信息技术安全宣传和教育培训工作，建立健全相关制度。
63. 网信办定期组织开展针对师生员工的网络与信息技术安全教育，提高师生员工的安全和防范意识。
64. 网信办定期开展针对网络与信息技术安全管理人员和技术人员的专业技能培训，提高信息安全工作能力和水平。
65. **网络与信息技术安全检查监督**
66. 学校各单位定期对本单位网络与信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合网信办的网络与信息安全检查、信息内容检查、终端的安全防护等工作
67. 网信办联合相关部门对学校各单位的网络与信息技术安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。
68. 网信办对年度安全检查情况进行全面总结，按照要求完成检查报告并报学校网络安全和信息化领导小组。
69. **网络与信息安全事件的处理**
70. 网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。
71. 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。
72. 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。
73. 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。
74. 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。
75. 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。
76. 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。
77. 其他事件是指不能归为以上分类的网络安全事件。
78. 校内网络与信息技术安全事件的处理由网信办负责组织实施，安全学校网络与信息技术安全事件处理流程进行分级、分类处理。为避免安全事件不良影响扩大，网信办有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。
79. 网信办负责组建校内网络与信息安全事件安全应急响应组织，制定相应的应急响应流程、规范，并按照学校网络信息技术安全事件处理流程处理相关网络信息安全事件。
80. 网络与信息技术安全事件处理后，由网信办与相关部门共同进行责任认定，并根据本办法第十四章对责任人、责任部门进行处理。
81. **网络与信息安全责任追究**
82. 学校建立网络与信息技术安全责任追究和倒查机制。有关单位在收到网络与信息技术安全限期整改通知书后，整改不力的，学校给予通报批评；玩忽职守、失职渎职造成严重后果的，依纪依法追究第一责任及相关人员的责任。
83. 学校各单位应按照信息技术安全事件报告与处置流程技术、如实地报告和妥善处置信息技术安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报。
84. 学生违反本办法规定的，由网信办会同学生处、研究生处、国际文化交流学院、预科教育学院、保卫处等部门按照《新疆师范大学学生违纪处分办法》相关处理；拒不改正或者导致危害信息技术安全等严重后果的，触犯法律的，移交司法机关处理。
85. **附则**
86. 本办法中下列用语的含义：
87. 网络，是由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络和系统。
88. 网络安全，是指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络存储、传输、处理信息的完整性、保密性、可用性的能力。
89. 信息技术安全事件，是指除信息内容安全事故意外的有害程序事件、网络攻击事件、信息破坏事件、设备实施故障、灾害事件和其它信息安全事件。
90. 本办法自发布起执行，由网信办负责解释。学校原有相关规定与本办法不一致的，按本办法执行。