

中共北京教育学院委员会文件

京教院党发〔2024〕5号



中共北京教育学院委员会 关于印发《北京教育学院落实网络安全和信息化 工作责任制实施细则（修订）》的通知

各二级党组织、各部门：

经学院四届党委常委会第19次会议研究决定，现将《北京教育学院落实网络安全和信息化工作责任制实施细则（修订）》印发给你们，请认真抓好落实。

中共北京教育学院委员会
2024年5月13日



北京教育学院落实网络安全和信息化 工作责任制实施细则（修订）

第一条 为进一步加强和规范学院网络安全和信息化工作，明确和落实各方责任，确保网络安全和信息化建设项目科学、规范、合理、有序实施，全面提高网络安全和信息化建设质量，保证网络安全和信息化建设可持续发展，根据《中华人民共和国网络安全法》《党委（党组）网络安全工作责任制实施办法》（厅字〔2017〕32号）《中共北京市委网络安全和信息化委员会工作规则》（京网委发〔2019〕1号）等文件精神，结合我院实际，制定本细则。

第二条 网络安全是指通过硬件保护和行为管理等方式保障学院网络设备设施、有线和无线基础网络,以及部署在服务器上的各个信息系统平台或网站数据等的安全，阻断不良信息传播、外部非法访问和各类病毒或木马危害，保障网络系统正常、稳定地运行。

信息化工作是指在学院统一规划和组织下，以现代通信、网络、数据库技术为基础，在教学、科研、管理和服务等各方面应用，以提升教学、科研、管理和服务水平，提高工作效率。包括开发利用信息资源，建设学院信息网络，推进信息化应用，培养信息化人才队伍，制定和完善信息化制度，落实软件正版化工作等。

第三条 网络安全和信息化工作按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，院领导班子主要负责人是学院网络安全和信息化工作的第一责任人，分管网络安全和信息化工作的领导班子成员是直接责任人，其他领导班子成员对分管部门的网络安全和信息化工作负有领导责任。

第四条 成立北京教育学院网络安全和信息化工作领导小组（以下简称“领导小组”）。组长由党委书记、院长担任，副组长由分管院领导担任，成员由院领导班子成员、职能部门负责人、教辅机构负责人、二级学院党政负责人组成。领导小组的职责是：

（一）认真贯彻落实党中央、教育部党组、市委和市教委关于网络安全和信息化工作的重要指示精神、决策部署和任务要求，统一组织领导、统筹协调解决学院网络安全和信息化工作重大问题，推动学院数字化转型；

（二）建立和落实学院网络安全和信息化工作责任制，定期听取网络安全和信息化工作整体情况汇报，把网络安全和信息化工作纳入重要议事日程，明确工作机构及职责分工，加大人力、财力、物力的支持和保障力度；

（三）研究制定学院网络、数据安全和信息化工作发展规划、工作计划、政策规定和工作标准等；

（四）领导重大活动时期网络安全服务保障工作，指挥协调重大网络、数据安全事件应对处置；

（五）研究网络安全人员配置及技能培训，组织开展经常性

网络、数据安全与信息化宣传教育，推进国产网络安全与信息化产品的推广应用；

（六）研究部署软件正版化工作，推进学院软件正版化工作规范化、常态化、制度化、信息化；

（七）按照“谁管业务，谁管业务数据，谁管数据安全”的原则，明确数据安全职责划分，推进数据分类分级管理。指导横向、纵向以及院内跨部门的信息化平台与数据的互联互通与共享。

第五条 领导小组下设网络安全和信息化工作办公室（以下简称“办公室”），办公室设在信息化部门，办公室主任由信息化部门负责人兼任。办公室作为领导小组常设办事机构，其职责是：

（一）落实领导小组的各项工作部署，处理日常事务，全面协调学院网络安全和信息化建设工作；

（二）牵头编制并组织落实学院网络安全和信息化建设发展规划和年度计划；

（三）负责建立健全学院网络安全和信息化工作管理制度；

（四）负责统筹、协调、推动或督促经学院批准立项的信息化建设项目，负责对接经信局、市教委等上级相关单位，积极推动信息化专项申报。统筹管理学院云资源，配合职能部门推进业务管理与服务信息系统的建设、集成、运维和网络、数据安全等工作；

（五）负责落实网络安全等级保护工作，建立信息系统定级

备案台账，开展学院信息系统的定级、评审和备案工作，定期开展等保测评；

（六）牵头建立健全分析研判、应急处置等工作机制，指导、督促各部门落实网络安全工作职责；

（七）制定学院网络安全重大事件应急处置预案，按照实际情况和上级的要求，开展网络安全保障和应急实战演练；

（八）组织开展网络和数据安全宣传教育，加强对信息系统管理员、网络安全联络员的培训，压实责任；

（九）统筹、协调、督查学院软件正版化各项工作，健全学院软件正版化工作机制，逐人签订使用正版软件承诺书，加强培训和宣传。

第六条 成员机构的职责如下：

（一）职能部门、教辅机构

1.认真学习国家和学院相关规章制度，贯彻落实学院关于网络安全和信息化工作的决策部署，把网络安全和信息化工作纳入重要议事日程；

2.落实网络安全和信息化工作责任制，各部门负责人是本部门网络安全和信息化工作的第一责任人，对本部门网络安全和信息化工作负责。部门要确定分管领导、网络安全联络员和信息系统管理员，并明确其职责；

3.根据业务工作需要，提出与本部门职责相关的教学、科研、管理和服务等业务信息系统的建设规划、使用需求和实施方案，

所建设的信息系统，除了满足自身的业务需求外，还需满足学院数据交换、数据共享及安全的要求，并遵循学院统一的相关信息化标准建设。新建信息系统（等保二级及以上）实施方案中必须包括等保测评、安全措施等内容和费用，通过等保测评和验收后，方可上线运行；

4.负责业务相关信息系统的日常管理和运维工作，做好信息系统的推广、使用和用户培训。掌握信息系统的使用情况和安全情况，制定信息系统的使用管理制度和应急预案，加强与相关部门的沟通，按照上级和学院的要求落实信息系统的网络安全措施；

5.指定专人负责本部门的网络安全工作，重点做好网络打印机、传真机、电子显示屏、办公电脑等网络设备的安全管控和防护，对办公电脑进行经常性病毒查杀和漏洞修复。如遇疑难问题，及时与办公室沟通。如遇异常或突发事件应做到及时处理并第一时间报告部门负责人和办公室；

6.组织本部门教职工参加学院的网络安全宣传教育活动，加强网络安全培训，提高教职工的网络安全意识，落实意识形态的各项要求，规范上网行为；

7.负责做好本部门软件正版化自查工作，配合学院软件正版化检查，及时发现问题并积极整改；

8.加强本部门微信公众号、微信、微信群、企业微信、微博等新媒体，以及移动 APP、网络教学等平台的管理；

9.有政务外网、政务内网等专网或涉密网络接入的部门，必须按照专网或涉密网络的管理要求操作使用，并落实责任，做好日常管理。

（二）党政办公室除履行（一）所述的职责外，还应履行如下职责：

1.负责学院信息公开的日常工作；

2.做好学院办公信息保密工作；

3.配合办公室统筹协调各部门落实网络安全和信息化工作责任；

4.负责政务内网接入专线的安全管理。

（三）宣传部门除履行（一）所述的职责外，还应履行如下职责：

1.加强网络意识形态阵地管理，全面了解掌握涉学院网络舆情动向，负责学院舆情的应对处置；

2.负责学院门户网站外网新闻类栏目内容的审核发布；

3.负责学院官方微信公众号的日常运营，加强学院相关微信公众号的整合管理；

4.协助开展网络和数据安全宣传教育。

（四）财务部门除履行（一）所述的职责外，还应履行如下职责：

1.负责学院网络安全和信息化建设的资金保障，为基础硬件设施建设以及网络、数据安全运维、管理和培训提供经费支持；

2.负责政务外网接入专线的安全管理。

(五)安全保卫部门除履行(一)所述的职责外,还应履行如下职责:

1.做好与网络安全和信息化工作相关的保卫与消防安全工作;

2.负责协调市政法、公安等专业部门,配合做好网络安全事件的应对处置。

(六)二级学院

1.认真学习国家网络安全法和学院相关规章制度,贯彻落实学院关于网络安全和信息化工作的决策部署,把网络安全和信息化工作纳入重要议事日程;

2.落实网络安全和信息化工作责任制,二级学院党政负责人是本二级学院网络安全和信息化工作的第一责任人,对本二级学院网络安全和信息化工作负总责。二级学院要指定分管领导、网络安全联络员和信息系统管理员,明确职责;

3.加强对教师和职工的安全教育,提高安全意识,在教学(含网络教学)、科研和管理工作中落实网络安全和意识形态领域的各项要求;

4.根据教学、科研工作需要,提出信息系统方面的使用需求;

5.指定二级学院的网络安全联络员,按照学院要求,负责本二级学院的网络安全工作,重点做好网络打印机、传真机、电子显示屏、办公电脑等网络设备的安全管控和防护,对办公电脑进

行经常性病毒查杀和漏洞修复。如遇疑难问题，可随时与办公室沟通。如遇异常或突发事件应做到及时处理并第一时间报告二级学院党政负责人和办公室；

6.组织教师和职工参加学院的网络安全宣传教育活动和数字素养提升培训，提高教职工的网络安全意识和数字技术资源应用于教育教学的能力；

7.负责做好本部门软件正版化自查工作，及时发现问题并积极整改；

8.加强与部门相关的微信公众号、微信、企业微信、微博等新媒体，以及移动 APP、网络教学等平台的管控。

第七条 建立健全工作机制，领导小组每年至少召开一次专题会议，研究议定重大事项，加强网络安全和信息化工作的措施和人力、物力、财力保障。分管网络安全和信息化工作的院领导每学期至少召集一次工作例会，办公室和相关部门汇报网络安全和信息化工作相关内容，研究工作中遇到的困难和问题，提出解决对策和措施。各部门根据需要，及时召开班子会或党政联席会，研究网络安全和信息化相关工作。

第八条 建立网络安全和信息化工作责任制检查考核制度，健全考核机制，明确考核内容和程序，将考核内容纳入部门考核和中层干部、教职工考核。

第九条 各部门、二级学院违反或未能正确履行本细则所列职责，导致在学院内发生下列网络安全事件，学院将根据有关法律、法规追究其相关责任：

(一)部门管理的信息系统、网站、网络平台等被攻击篡改,导致反动言论或谣言等违法有害信息大面积扩散,且没有及时报告和组织处置的;

(二)发生学院机密信息、大面积个人信息或大量基础数据泄露的;

(三)封锁、瞒报网络安全事件情况,拒不配合有关部门依法开展调查、处置工作,或对有关部门通报的问题和风险隐患不及时整改并造成严重后果的;

(四)发生其他严重危害网络安全的行为的。

第十条 以上各部门和岗位如遇人事调整,由其继任者自动补进。

第十一条 北京市教师发展中心参照本细则执行。

第十二条 本细则未尽事宜按照上级相关规定执行。本细则由领导小组办公室负责解释。

第十三条 本细则自发布之日起施行,《北京教育学院落实网络安全和信息化工作责任制实施细则》(京教院党发〔2020〕12号)文件同时废止。

附件:北京教育学院落实网络安全和信息化工作
责任制工作指标

附件

北京教育学院 落实网络安全和信息化工作责任制工作指标

| 序号 | 工作要求 | 指标描述 | 责任部门 |
|----|------------------------------|---|-----------------------|
| 1 | 院领导班子主要负责人是第一责任人，分管院领导是直接责任人 | 1.通过正式文件或会议纪要明确第一责任人和直接责任人； 2.人员发生变动后及时进行变更。 | 党政办公室 |
| 2 | 明确学院网络安全的主要目标、基本要求、工作任务和保护措施 | 1.制定学院网络安全规划、实施计划或工作方案等文件； 2.提出网络安全的主要目标、基本要求、工作任务和保护措施。 | 信息化部门 |
| 3 | 建立和落实网络安全和信息化工作责任制 | 1.印发学院落实网络安全和信息化工作责任制实施细则。 | 党政办公室 信息化部门 |
| 4 | 把网络安全工作纳入重要议事日程 | 1.领导小组每年至少召集一次专题会议，组织听取网络安全和信息化工作整体情况汇报，研究议定重大事项，加强网络安全工作的措施和人力物力财力保障； 2.直接责任人至少每学期召集一次例会，听取网络安全和信息化相关工作汇报，研究工作中遇到的困难和问题，提出解决对策和措施； 3.各部门（二级学院）根据需要，及时在班子会或党政联席会上研究网络安全和信息化相关工作； 4.按照有关文件、会议精神落实网络安全相关工作要求和部署。 | 党政办公室 信息化部门 各部门 |
| 5 | 明确网络安全工作机构和责任人 | 1.通过制度文件明确学院负责网络安全工作的机构和职责； 2.各部门指定网络安全联络员和信息系 | 组织部门 人事部门 |

| | | | |
|----|------------------------------------|---|--------------------------------------|
| | | <p>统管理员；</p> <p>3.按照实际需要配备网络安全工作人员；</p> <p>4.各项网络安全管理制度健全完善。</p> | <p>信息化部门 各部门</p> |
| 6 | 加大人力、财力、物力的支持和保障 | <p>1.通过日常公用经费等现有预算渠道，切实保障网络系统的安全防护加固、安全运维、安全检测评估、系统安全升级改造、网络安全教育培训、网络安全事件应急处置等支出；</p> <p>2.新建信息化项目的网络安全预算不低于项目总预算的5%。</p> | <p>财务部门</p> |
| 7 | 统一组织领导学院网络安全保护和重大事件处置工作 | <p>1.完善网络安全应急预案，明确重大事件处置由党委统一组织领导，重大情况及时向相关上级单位报告；</p> <p>2.每年至少开展一次网络安全应急实战演练。</p> | <p>信息化部门 安全保卫部门</p> |
| 8 | 加强网络安全防护，抵御和防范网络攻击，强化网络安全事件发现和处置能力 | <p>1.落实网络安全管理制度建设，切实做好网络系统的安全防护加固、安全运维管理、安全检测评估、系统安全升级改造、信息研判和监测预警、网络安全教育培训、网络安全事件应急处置等工作，确保网络安全；</p> <p>2.根据实际，每年开展网络安全检查、处置网络安全事件，并将有关情况纳入年度网络安全工作报告；</p> <p>3.加强对网络打印机、传真机、电子显示屏、办公电脑等网络设备的安全管控；</p> <p>4.对办公电脑进行经常性病毒查杀和漏洞修复。</p> | <p>信息化部门 信息系统管理部门 各部门</p> |
| 9 | 切实做好重大活动时期网络安全服务保障工作 | <p>1.按照上级统一部署，认真落实重大活动时期网络安全服务保障工作各项任务要求。</p> | <p>信息化部门 安全保卫部门 信息系统管理部门</p> |
| 10 | 落实网络安全等级保护工作 | <p>1.建立信息系统定级备案台账，开展学院信息系统的定级、评审和备案工作；</p> | <p>信息化部门 信息系统管理部门</p> |

| | | | |
|----|-------------------------|--|-----------------|
| | | 2.定期开展等保测评。 | |
| 11 | 组织开展经常性网络安全宣传教育 | 1.按照上级统一安排,开展网络安全宣传周活动。 | 信息化部门 |
| 12 | 强化网络安全人员配置及技能培训 | 1.在职人员年度人均接受网络安全培训时间不少于4个学时,并纳入部门考核和中层干部、教职工考核; 2.网络安全专业技术岗位人员年度人均接受专业技能培训不少于8个学时,且获得网络安全专业资质人员占比达到60%以上或虽未达到60%但逐年提高。 | 信息化部门 人事部门 |
| 13 | 落实软件正版化,加快推进国产技术产品的推广应用 | 1.落实办公电脑操作系统、通用办公软件、杀毒软件正版化及服务器软件正版化; 2.采购国产软硬件产品的支出比例符合中央和北京市提出的要求。 | 信息化部门 资产管理部门 |
| 14 | 信息系统建设 | 1.根据工作需要,提出相关业务信息系统建设规划、使用需求和实施方案,所建设的信息系统必须满足学院数据交换、数据共享和安全要求; 2.新建信息系统(等保二级及以上)必须通过等保测评和验收后方可上线运行; 3.信息系统建设时要考虑上线后的运维方式和费用等。 | 相关部门 信息化部门 |
| 15 | 信息系统运维和管理 | 1.保证信息系统正常运行,落实上级的相关安全要求,落实重大活动时期的系统安全; 2.做好信息系统的推广、使用和用户培训; 3.掌握信息系统的使用和安全情况; 4.制定信息系统的管理制度和应急预案。 | 信息系统管理部门 |
| 16 | 新媒体及平台管控 | 1.加强与部门相关的微信公众号、微信、微信群、企业微信、微博等新媒体的管控; 2.加强移动APP、网络教学等平台的管 | 宣传部门 相关部门 |

| | | | |
|----|-----------|--|-------------|
| | | 控; 3.学院门户网站外网新闻类栏目内容必须经宣传部审核; 4.学院官方公众号由宣传部负责日常运营;其他公众号发布内容由相关部门负责人审核。 | |
| 17 | 专网或涉密网络管理 | 1.必须按照专网或涉密网络的管理要求操作使用,并落实责任,做好日常管理。 | 专网或涉密网络接入部门 |