山东管理学院文件

鲁管院发〔2024〕50号

关于印发《山东管理学院网络与信息安全应急管理办法(2024年修订)》的通知

各部门、单位:

《山东管理学院网络与信息安全应急管理办法(2024年修订)》已经学校党委会研究通过,现印发给你们,请认真遵照执行。

山东管理学院

2024年12月19日

山东管理学院网络与信息安全应急管理办法
(2024年修订)

第一章　总　则

第一条　为进一步做好山东管理学院网络与信息安全事件的应急工作，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》和《山东管理学院信息化工作管理办法》等相关规定，特制定本办法。

第二条　网络与信息安全事件指危害信息系统安全、影响系统正常使用，或数据遭篡改、破坏、泄露或者非法获取、非法利用的事件。

第三条　本办法适用于山东管理学院发生和可能发生的网络与信息安全突发事件。

第四条　工作原则：谁主管谁负责、谁主办谁负责、谁使用谁负责；应急机制：统一领导，快速反应，密切配合，科学处置。

第二章　事件内容与等级划分

第五条　网络与信息安全事件具体内容

（一）数据因人为原因、软硬件缺陷或故障、自然灾害等遭到破坏、篡改、窃取及泄露，危害数据完整性、机密性、可用性，对国家安全、学校或个人利益造成危害的。

（二）网络与信息系统的硬件受到人为或自然灾害破坏，不能正常发挥其部分功能或全部功能。

（三）网络与信息系统感染病毒或遭受黑客攻击，局部或全部数据和功能受到损坏，使系统不能工作或工作效率急剧下降。

（四）系统面临意外停电而又无后备供电措施。

（五）系统的关键岗位人员不能上岗。

第六条 网络与信息安全事件等级划分

（一）一般等级：局部网络或信息系统受到一定程度损坏，但在短时间内（分钟级）即可恢复的，对学校某些工作造成影响，但不危及学校整体工作。

（二）紧急等级：受人为原因或自然灾害，学校某一区域的网络与信息系统瘫痪，重要数据被破坏、丢失，需要数小时才能恢复业务的，对学校正常工作造成一定损害，造成的损失较大。

（三）严重等级：学校的网络与信息系统发生全校性瘫痪，大量业务数据或重要数据遭到破坏、丢失，需要数天乃至数周才能恢复业务的，对学校正常工作造成严重损害，事态发展超出技术部门控制能力，造成学校巨大经济损失或造成社会影响。

（四）特别重大等级：学校网络与信息系统发生全校性大规模瘫痪，造成网络和信息系统的根本性破坏，数据完全丢失，业务无法恢复，对学校正常工作造成特别严重损害，引发特别重大网络安全事件，事态发展超出学校控制能力。

第三章 应急响应小组、事件报告和处理

第七条 当遇到严重及特别重大网络与信息安全事件时，由网络安全与信息化领导小组牵头，成立应急响应小组。应急响应

小组快速调动相关资源,协调本单位和相关单位的信息安全专家,防止事件处理的任何环节出现延迟，以最快速度确定故障点，及时排除故障，保证系统正常运行。

第八条 相关组织机构职责

（一）网络安全与信息化领导小组

1.决定严重等级和特别重大等级的网络与信息安全事件应急预案的启动。

2.督促检查安全事件处置情况及各有关单位在安全事件处置工作中履行职责情况。

3.对全校各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。

（二）党委(院长)办公室(法律事务中心)

1.组织协调有关部门查处利用计算机网络泄密的违法行为。

2.牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。

（三）宣传部、学生工作部（处）、团委

1.负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题进行分析研判。

2.负责组织协调舆情突发事件及应急处置过程中相关舆论的处置。

（四）安全保卫处

1.密切配合公安部门，做好网络与信息安全事件的处置工

作。

2.负责及时收集、通报和上报网络与信息安全事件应急处置情况。

（五）网络信息中心

1.负责校园基础网络系统安全。

2.负责计算机病毒疫情和大规模网络攻击事件的处置。

3.负责校级网络与信息安全事件处置的技术支持。

（六）其他部门

1.对照本办法建立单位内部应急处置机制。

2.负责本部门内部的网络与信息安全管理和突发事件应急处置。

3.配合各部门落实相关应急处置措施。

第九条 网络与信息安全事件的报告

（一）当遇到一般等级网络与信息安全事件时，发现人应立即报告本部门领导和网络信息中心。网络信息中心通知有关人员立即进行处理，并上报网络安全与信息化领导小组办公室。

（二）当遇到紧急等级网络与信息安全事件时，发现人应立即报告本部门领导、网络信息中心。网络信息中心领导组织有关人员到现场处理，同时要立即上报网络安全和信息化领导小组。

（三）当遇到严重等级网络与信息安全事件，发现人应立即报告本部门领导、网络信息中心、网络安全与信息化领导小组。网络安全与信息化领导小组牵头成立应急事件响应小组，立即组

织有关人员到现场处理，并将情况上报至学校党委。

（四）遇到特别重大等级网络与信息安全事件，发现人应立即报告本部门领导、网络信息中心、网络安全与信息化领导小组。网络安全和信息化领导小组牵头成立应急响应小组，必须第一时间稳定事态，防止危害进一步扩大，并上报学校上级单位。

第四章　应急计划

第十条　针对各类网络与信息安全事件制定行之有效的应急计划。

（一）应急计划须条理清楚、语言简洁、步骤分明、具有强可操作性。

（二）应急计划须有多种备用方案，每种方案均可独立实施，应有各种方案的优先排序。

（三）应急计划须有明确的负责人与各级责任人的职责。

（四）应急计划应便于培训和实施演习。

（五）应急计划简单流程图须公布在显著和方便的位置，以便发生事故时，能迅速、方便地执行。

第十一条　应急计划应包括紧急措施、备用资源、恢复过程、应急计划关键信息。具体如下:

（一）紧急措施

制定对各种网络与信息安全事件的响应规程、抢救计划、救护计划和撤离计划，以保护人员生命，降低财产损失。

（二）备用资源

备用软件资源：对数据信息资源需要有足够备份，并将备份存放于免受攻击或受灾害影响的地方。

重要或大型系统中的关键设备和信息安全产品应采用双机热备份,对特别重要信息应尽可能采取安全保密的异地备份措施。

备用设备：在工作现场设有设备主板、硬盘、光驱等备件，以及其它备用的外部设备。

备用电源：应配置不间断电源，一般不间断电源应可在断电后维持系统工作二小时以上。应配置备用交流稳压电源。重要系统和大型系统应配备多种供电来源，甚至配备发电设备。

经费保障：网络与信息安全事件应急处置专项经费，应列入年度预算，切实予以保障。

（三）系统恢复

首先恢复重要的安全产品，保证系统安全情况下，再恢复应用系统。

（四）应急计划关键信息

应急计划关键信息须张贴在显著位置，应急计划关键信息主要包括：火警电话、报警电话、应急负责人电话和住址等。

第五章　应急演练、培训

第十二条　应每年至少组织一次对系统用户进行安全应急培训和应急演练，并根据演练结果对应急预案进行评审和修订。

第十三条　发生应急事件并处理完成后应当对事件进行分析总结，进行风险评估，改进不足，弥补漏洞。

第十四条 发生应急事件并处理完成后应当进行专题教育和培训。

第六章 附 则

第十五条 本办法由网络安全与信息化领导小组办公室负责解释。

第十六条 本办法自发布之日起施行，原《山东管理学院网络与信息安全事件应急预案》（鲁管院发〔2018〕107号）同时废止。

山东管理学院院长办公室 2024年12月23日印发