阜阳职业技术学院网络信息安全事件应急处置办法

阜职院〔2021〕124号

第一章　总 则

第一条 为科学有效预防和应对网络与信息安全突发事件，确保校园网络与信息系统正常运行，根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《信息安全事件分类分级指南》（GB/T20986-2007）等相关文件，结合学校工作实际，制定本办法。

第二条 校园网络信息安全事件是指校园信息化基础设施、应用系统、网站、系统数据等因各种因素遭到破坏，对学校工作、师生学习、生活秩序造成负面影响的事件。

第三条 处置流程遵循“统一领导、预防为本、快速反应、科学处置”的原则，最大可能的降低危害和影响。

第二章　安全事件等级划分

第四条　网络信息安全事件依据发生过程、性质和特征不同，可分为以下四类：

（一）网络攻击事件：由于遭受恶意程序感染、非法入侵或其他技术手段攻击，造成校园网络和信息系统运行异常或存在潜在危险，或造成信息被篡改、伪造、泄漏、窃取等而导致的网络安全事件。

（二）设备故障事件：由于信息系统或外围软硬件设施故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的网络安全事件。

（三）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。

（四）信息内容安全事件：利用校园网络在校内外传播法律法规禁止的信息，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安全事件。

第五条　网络信息安全事件按照可控性、严重程度和影响范围不同，可划分为四级：

（一）Ⅰ级（特别重大）：事件导致发生全校性大规模网络及系统瘫痪，或发生严重信息内容安全事件和信息破坏事件，对学校正常工作造成特别严重损害，造成严重社会影响，事态发展超出学校控制能力。

（二）Ⅱ级（重大）：事件导致校园网发生全校性瘫痪，或发生信息内容安全事件和信息破坏事件，对学校正常工作造成严重损害，并造成一定社会影响。

（三）Ⅲ级（较大）：事件导致校园网某一区域的重要网络与信息应用系统瘫痪，或由于网站敏感信息、谣言等，对学校正常工作造成一定损害，但未造成社会影响。

（四）Ⅳ级（一般）：事件导致某一局部网络或信息应用系统受到一定程度损坏，学校工作受到一定影响，但不危害学校整体工作。

第三章　组织机构及职责

第六条　学校网络安全和信息化领导小组（以下简称学校网信领导小组）为网络信息安全事件应急处理领导机构，其职责包括：

（一）负责网络与信息安全工作的组织、协调和监督，制定相关制度和应急预案。

（二）根据网络信息安全事件程度提出相应级别预案的启动，组织协调成员单位落实应急预案，共同做好处置工作。

（三）负责及时收集、通报和上报网络信息安全事件处置的有关情况。

（四）对全校各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

第七条　各单位及部门职责包括：

（一）党政办公室：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；负责涉密事件的处理。

（二）图文信息中心：负责校园基础网络及公共服务信息系统安全，保证校园网络信息服务不中断；负责网络攻击、设备故障类事件的处置；负责全校网络信息安全事件处置的技术支持工作。

（三）组织人事部（宣传统战部）：负责学校舆情监测和信息内容安全类事件的处置，加强涉及师生政治思想方面的预警性、倾向性、苗头性问题的分析研判，妥善有效应对。

（四）保卫处：密切联系公安部门，负责涉及人为破坏类事件的处置，配合重大安全事件的处置。

（五）其他单位：各教学单位、各部门负责本单位网站和业务系统的信息安全事件的处置工作，对照本办法，建立本单位应急处置机制。

第四章　安全事件预防与发现

第八条　按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各教学单位、各部门要做好网络信息安全事件的隐患排查工作，制定和完善管理制度，做好日常管理和监控，避免和减少网络信息安全事件的发生和危害。

第九条　健全技术防护体系。图文信息中心在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御和入侵检测工具，进行实时监测和

定期扫描，发现异常情况及时防范处理并逐级报告。同时做好操作系统升级杀毒，数据备份、安全审计等日常管理工作。

第十条　建立安全事件巡查制度。各教学单位、各部门负责所主办网站内容的日常监控，图文信息中心定期开展巡检工作，做好校园网络与信息安全的日常巡查及日志保存工作，以保证最先发现安全事件并及时处置突发性安全事件。

第五章　安全事件研判与处置

第十一条　在突发安全事件后，当值人员应根据实际情况立即采取本办法中的应急处置措施进行处置，将损害和影响降到最小范围，保护现场并报告本单位安全责任人和主要负责人。在事件处置结束前要进行动态监测、评估，及时将事件现状及处置工作等情况向上级汇报，不得瞒报、缓报、谎报。节假日或夜间突发安全事件，当值人员报党政办公室值班人员，由其负责与学校网信领导小组等相关部门进行联系，并协调相关部门进行处置。

第十二条　启动预案：发生网络信息安全事件后，涉事部门应第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场，并报告本单位分管领导和学校网信领导小组。

第十三条　事件定级：学校网信领导小组紧急组织有关单位，尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认事件的类别和等级。

第十四条　应急响应：根据事件等级采取相应的响应方式

（一）I 级：事发单位立即向学校网信领导小组汇报并给出处置建议，由学校网信领导小组统一就事件事态做出研判并组织应急处置。必要时由学校报告市网信办和当地公安部门，由公安部门指挥协调有关单位和我校协同进行应急处置。

（二）II 至 III 级：事发单位及时上报学校网信领导小组，由领导小组指挥、协调成员单位进行应急处置。涉及人为主观破坏事件时由学校保卫处报告当地公安部门。

（三）IV 级：事发单位及时、自主进行应急处置，做好处置记录。必要时请求相关部门协同处置。

第十五条　应急处置方式：根据网络信息安全事件分类采取不同应急处置方式。

（一）网络攻击事件：判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

1．病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口和相应楼层的网络，及时请有关技术人员协助进行杀毒处理。

2．外部入侵：判断入侵的来源，区分外网与内网，评估入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评估威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

3．内部入侵：排查入侵来源，如 IP 地址、所在物理位置等信息，同时断开对应的交换机端口，针对入侵方法调整或升级入侵检测设备。对于无法及时控制的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二）设备故障事件：判断故障发生点和故障原因，迅速联系设备厂家或运营商尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（三）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

（四）信息内容安全事件：接到校内网站出现不良信息的反馈时，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，追溯信息发布源，并做好善后处理。对公安机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（五）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理，不能处理的及时咨询国家信息安全机构。

第十六条　应急支援

应急措施实施后，事态仍难以控制或有扩大发展趋势时，学校网信领导小组要根据事态情况召开应急处置会议，研究采取有利于控制事态的非常措施，并向市网信办、市网安支队、运营商等相关单位请求援助。

第十七条　信息发布

当网络信息安全事件突发时，图文信息中心及时做好信息发布的技术支持工作，保障组织人事部（宣传统战部）等引导舆论和公众行为，避免影响社会或学校秩序。党政办公室等相关部门密切关注安全事件引起的反应，当安全事件引发网上舆情时，要及时组织引导，充分发挥校园媒体和学生组织的作用，在网上进行正面宣传，抵制负面影响，及时采取措施。同时对出现的关于网络安全事件以及处置工作的不正确信息要进行澄清、纠正，接受群众咨询，释疑解惑，稳定人心。

第十八条　后续处理：

（一）网络信息安全事件应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

（二）网络信息安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（三）网络信息安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

第十九条　总结上报

（一）网络信息安全事件情况报告和事后整改报告应于处置完毕后 3 个工作日内以书面报告的形式报送学校网信领导小组。事件情况报告由发生安全事件的单位组织编写，由本单位主要负责人审核后，签字加盖公章报送学校网信领导小组。涉及人为因素的，应将事件情况报告抄送校保卫处。

（二）图文信息中心对网络信息安全事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告，报送学校网信领导小组。

（三）发生Ⅱ至Ⅰ级网络信息安全事件，在报告学校的同时，还应报告上级行政主管部门和网络安全主管部门，属于重大安全事件或存在违法犯罪行为的，须第一时间向公安机关报案。

第六章　附则

第二十条 本办法由图文信息中心负责解释，自发布之日起施行。