郑州澍青医学高等专科学校文件

校字〔2022〕32号

郑州澍青医学高等专科学校
网络安全事件应急预案（试行）

第一章　总则

第一条　依据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《中华人民共和国计算机信息系统安全保护条例》《信息安全技术信息安全事件分类分级指南》《教育系统网络与信息安全类突发公共事件应急预案》等国家、教育行业有关法律法规和标准规范。为建立健全我校网络安全事件应急工作机制，有效预防并科学应对网络安全突发事件，提高网络安全事件处置能力，最大限度地预防和减少网络安全事件造成的损失和危害，确保校园网络和信息系统的正常运行和安全稳定，维护校园

正常秩序，保护公众利益，维护国家安全、公共安全和社会秩序，特制定本预案。

第二条 本预案适用于学校范围内网络安全事件的应急处置。

第二章 网络安全事件分级

第三条 本预案中所指网络安全事件是指由于人为原因、软硬件本身缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。网络安全事件可划分为有害程序事件、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、灾害性事件和其他事件七个基本分类。

第四条 根据《信息安全技术信息安全事件分类分级指南》，将安全事件划分为四个等级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）：

Ⅰ级（特别重大），重要网络与信息系统发生全校性大规模瘫痪，事态发展超出学校网络安全和信息化领导小组的控制能力，对学校安全、秩序和学校公共利益造成特别严重损害的突发事件。

Ⅱ级（重大），重要网络与信息系统全校性瘫痪，对学校安全、秩序和学校公共利益造成严重损害，需要跨部门协同处置的突发事件。

Ⅲ级（较大），某一区域的重要网络与信息系统瘫痪，对学校安全、秩序和学校公共利益造成一定损害，但不需要跨部门协同处置的突发事件。

Ⅳ级（一般），重要网络与信息系统受到一定程度的损坏，对学校师生员工和一些部门的权益有一定影响，但不危害学校安全、秩序、学校公共利益的突发事件。

第三章　组织机构与职责

第五条　学校网络安全和信息化领导小组是网络安全事件应急处置领导机构，学校网络安全和信息化领导小组办公室统筹协调组织校内网络安全事件应对工作，建立健全跨部门联动处置机制，校长办公室、党委办公室、党委宣传部、信息管理中心等相关单位按照职责分工负责相关网络安全事件应对工作。

第六条　学校各单位按照职责和权限，负责本单位网络和信息系统安全事件的预防、监测、报告和应急处置工作。对照本预案，建立本单位应急处置机制。

第四章　应急处置

第七条　网络安全事件发生后，校内各单位应立即启动应处置急预案，组织指导实施处置并及时报送信息。校党委宣传部、信息管理中心、责任单位领导及相关人员应第一时间到达现场，采取断网等先期应急处置措施，控制事态，消除隐患，将损害和影响降到最低，同时组织研判，保存证据，做好信息通报工作。对于初判为较大及以上等级的网络安全事件，应立即报告网络安全和信息化领导小组办公室，并由学校网络安全和信息化领导小组将相关情况向省教育厅网信办、省公安厅、市公安局等部门报告。

第八条 学校网络安全和信息化领导小组办公室组织有关单位尽最大可能收集网络安全事件相关信息，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，并根据事件等级采取相应的应急响应。

1. Ⅰ级、Ⅱ级、Ⅲ级响应：网络安全和信息化领导小组办公室应跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况及时上报省教育厅网信办、省公安厅、市公安局等部门。处置中需要上级部门网络安全应急技术支撑队伍配合和支持的，网络安全和信息化领导小组办公室予以协调。各单位根据网络安全和信息化领导小组办公室的通报信息，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

2. Ⅳ级响应：各单位及时、自主按相关预案进行应急处置，做好处置记录，并报网络安全和信息化领导小组办公室。

第九条 根据网络安全事件分类采取不同的应急处置方式：

1. 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，甚至相应楼层的网络，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，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价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 地址的访问。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：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止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。

2. 信息内容安全事件：检测或接到校内网站出现不良信息报告后，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，查找信息发布人并做好善后处理。对上级部门或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。

3. 设备故障事件：判断故障发生点和故障原因，迅速联系信息管理中心尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

4. 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。

第五章　预防工作

第十条　加强校园网络与信息系统安全管理，坚持“谁主管谁

负责、谁运维谁负责、谁使用谁负责”的原则，建立预警监测体系，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高网络安全事件的应对能力。

第十一条 不断健全和完善学校网络和信息系统的技术防护体系，在校园网边界、数据中心边界、重要信息系统等边界，加强安全防御设备和策略，发现异常及时处置并逐级报告。

第十二条 学校各单位按职责做好网络安全事件日常预防工作，加强各单位的网络和信息系统安全管理，制定完善的相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份。

第十三条 建立安全巡查制度。党委宣传部、信息管理中心及各单位网络安全负责人应密切监视信息系统内容，执行值班制度，做好校园网络与信息系统安全的日常巡查及日志保存等工作，以便及时应对突发性事件。

第十四条 建立应急预案定期演练。通过定期组织演练，提高防范意识及技能，发现应急工作体系和工作机制存在的问题，不断完善应急水平，提高应急处置实战能力。

第六章 保障措施

第十五条 加强学校各单位和相关人员的网络安全知识培训，特别是加强网络安全应急技术支撑队伍建设，不断提高信息安全防范意识和技术水平，提高应急处置能力，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。

第十六条 网络安全和信息化领导小组统筹协调网络安全保障工作,加强校园网络安全监测,在重大活动和关键时间节点,重点部门、重点岗位保持24值班，加强网络安全的防范，确保校园网络安全。

第十七条 加大资金投入，完善网络安全监测预警平台，建设支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、预案演练、物资保障等工作开展。

第十八条 责任与奖惩。网络安全事件应急处置工作实行责任追究制。各单位要认真贯彻落实预案的各项要求与任务，对未有效落实预案各项规定（如迟报、谎报、瞒报、漏报网络安全事件重要情况或者应急管理工作中有失职、渎职行为等）的单位进行通报批评，相关责任人给予处分，责令限期改正。对落实到位的给予相应的奖励。

第七章 附则

第十九条 本预案由学校网络安全和信息化领导小组负责解释。

第二十条 本预案自印发之日起实施。

2022年6月10日

郑州澍青医学高等专科学校校长办公室　2022年6月10日印发