江苏省徐州医药高等职业学校
网络与信息安全应急预案

第一章 总　　则

第一条　为提高处置网络与信息安全突发事件能力，加强网络与信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保网络与信息系统的实体安全、运行安全和数据安全，最大限度地避免、减轻网络与信息安全突发公共事件的危害，维护正常的办公、教学秩序,根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》等相关法律、法规和相关文件精神，特制定本预案。

第二条　本预案所指的网络与信息安全突发事件，是指重要网络与信息系统突然遭受不可预知外力的破坏、毁损、故障以及人为攻击，利用网络从事违法违规活动，发生对教育、教学、科研、管理和服务造成或者可能造成重大危害的紧急事件。

第二章 分类分级

第三条　根据网络与信息安全突发事件的发生过程、性质和特征，网络与信息安全突发事件可划分为网络安全突发事件和信息安全突发事件。网络安全突发事件是指自然灾害、事故灾难和人为破坏引起的网络与信息系统的损坏；信息安全突发事件是指信息内容遭到人为攻击造成泄密、篡改、删除，或利用信息网络发布违法违规的不良信息。

自然灾害是指地震、台风、雷电、火灾、水灾等。

事故灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

人为破坏是指人为破坏网络线路、通信设施、黑客攻击、病毒攻击、恐怖袭击等事件。

第四条 根据网络与信息安全突发事件的可控性、严重程度和影响范围，将网络与信息安全突发事件分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）。

Ⅰ级（特别重大）：网络与信息系统发生全局性大规模瘫痪，或违法违规信息大规模传播，对教育、教学、科研、管理、服务和公共利益造成特别严重损害，且事态发展超出学校可控能力的突发事件。

Ⅱ级（重大）：网络与信息系统造成全局性瘫痪，或违法违规信息大规模传播，对教育、教学、科研、管理、服务和公共利益造成严重损害，需要校内外、跨部门协同处置的突发事件。

Ⅲ级（较大）：局部网络与信息系统瘫痪，或违法违规信息在学校范围内传播，对教育、教学、科研、管理、服务和公共利益造成一定损害，只需要校内部门协同处置的突发事件。

Ⅳ级（一般）：网络与信息系统受到一定的损坏，对广大师生和其他组织的权益有一定影响，但对学校教育、教学、科研、管理、服务和公共利益的危害不大的突发事件。

第三章 适用范围与工作原则

第五条 网络与信息系统的重要性级别与其造成突发事件的等级相关。网络与信息系统的重要性级别是根据其在学校教育、教学、科研、管理和服务中的重要程度，遭到破坏后对学校教育、教学、科研、管理和服务以及其他合法权益的危害程度来确定的。

本预案适用于Ⅰ-Ⅳ级网络与信息安全突发事件和可能导致Ⅰ--Ⅳ级网络与信息安全突发事件的应对处置工作。

第六条 工作原则

1.居安思危，预防为主。立足安全防护，加强预警，重点保护基础信息网络和关系校园安全、教学秩序、师生稳定的重要信息系统，从预防、监控、应急处理、应急保障等环节，在管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

2.加强管理，分级负责。按照 “谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强部门间协调与配合，形成合力，共同履行应急处置工作的管理职责。

3.定期演练，常备不懈。加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发事件应急处置的科学化、程序化与规范化。

4.快速反应，减少损害。在网络与信息安全突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，及时采取措施，最大限度地避免公共财产、信息资产遭受损失，最大程度地减少危害和影响。

第四章 组织体系与工作职责

第七条 学校成立网络与信息安全应急协调领导小组，组长由学校信息化分管校领导担任，成员由各部处负责人组成，领导小组办公室设在电教图书信息中心，办公室主任由电教图书信息中心主任担任，其成员由各部门信息管理员和网络技术人员组成。

第八条 网络与信息安全应急协调领导小组主要职责与任务是统一领导网络与信息安全突发事件应急处置工作，指导和督促

网络与信息安全应急机制建设，组织网络与信息安全突发事件的处理、援救，协调解决灾害处置工作中的重大问题等。

第五章 预防措施

第九条 各部门要严格执行校园网络与信息系统安全各项管理制度，对本部门所负责管理的校园网络平台、应用平台和信息系统采取相应安全保障措施。

第十条 加强对校园网内计算机设备的管理，强化网络与信息安全教育，加强对重要网络设备的软件和硬件防护。

第十一条 实行信息网上发布审批制度。及时防范处理可能引发校园网络与信息安全事件的信息。

第十二条 电教图书信息中心加强对校园网络的监控和安全管理，做好相关数据日志记录，同时做好数据备份及登记工作，建立灾难性数据恢复机制。

第六章 处置流程

第十三条 预案启动。发生校园网络与信息安全事件后，领导小组办公室和相关的信息系统的用户部门应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，确认突发事件的类别和等级，并参照下述响应机制对突发事件进行处置。

第十四条 发生Ⅲ级或Ⅳ级突发事件时，领导小组办公室和相关用户部门，应立即向领导小组和分管校领导报告事件的性质、来源、范围及损害等情况，并自行负责应急处置工作。

根据网络与信息安全事件分类采取不同应急处置方式：

1. 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，采取设备的断电与拆卸、搬迁，硬盘的拔出与保存等方法。

2.设备故障事件：判断故障发生点和故障原因，迅速联系 IT 运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

3.网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定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，保护健康的计算机系统，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，寻找并公布病毒攻击信息，以及杀毒、防御方法。

（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。

4.信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或断开网络连接，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；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。

第十五条 发生Ⅰ级或Ⅱ级突发事件处理方式。

发生Ⅱ级突发事件响应：领导小组办公室立即上报学校网络与信息安全工作领导小组，由领导小组统一组织、协调指挥进行应急处置；

发生Ⅰ级突发事件响应：领导小组办公室立即上报学校网络与信息安全工作领导小组，领导小组再上报至上级相关部门。

第十六条 安全事件发生后，应及时采取行动，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。

第十七条 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。

第十八条 在确保安全事件解决后，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 系统恢复运行后，领导小组办公室组织人员对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于重大事件或存在非法犯罪行为的，第一时间向公安机关网络监察部门报案。

第七章 保障措施

第二十条 加强队伍建设，不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置科学得当。

第二十一条 不断完善网络安全整体方案，加强技术管理，完善软硬件设施建设，确保信息系统的稳定与安全。根据工作需要聘请信息安全专家、顾问为应急处置过程和重建工作提供咨询

和技术支持。

第二十二条 领导小组办公室定期对相关工作人员进行网络与信息系统安全知识培训，增强预防意识和应急处置能力。有针对性地开展应急抢险救灾演练，确保相关措施的有效落实。

第八章 附　　则

第二十三条 本预案自颁布之日起试行。

第二十四条 本预案由电教图书信息中心负责解释。