安徽新闻出版职业技术学院
网络与信息安全突发事件应急预案

1. 总则

1.1 编制目的

提高我院应对网络与信息安全突发事件能力，有效预防和控制各种突发事件发生，保障网络与信息安全与稳定，最大限度地减轻网络与信息安全突发事件的危害，维护学院正常的教育教学秩序，维护社会稳定。

1.2 编制依据

认真贯彻中央网络安全和信息化领导小组指示，依据《国家信息化领导小组关于加强信息安全保障工作的意见》《关于信息安全等级保护工作的实施意见》《关于开展信息安全风险评估工作的意见》《中华人民共和国计算机信息系统安全保护条例》《国家突发公共事件总体应急预案》《国家网络与信息安全事件应急预案》《中华人民共和国计算机信息网络国际互联网管理暂行规定》《计算机病毒防治管理办法》《安徽省教育系统网络与信息安全突发事件应急预案》《安徽新闻出版职业技术学院突发公共事件总体应急预案》等有关法律法规。

1.3 适用范围

本预案适用于安徽新闻出版职业技术学院对网络与信息安全突发事件的应急处置工作。

1.4 分类分级

本预案所指的网络与信息安全突发公共事件，是指突然发生，造成或可能造成影响我院乃至社会稳定的紧急事件。

按照网络与信息安全突发公共事件的性质、机理和发生过程，网络与信息安全突发公共事件分为以下几类：信息内容安全事件、有害程序事件、网络攻击事件、信息破坏事件、设备设施故障和灾害性事件等。

（1）信息内容安全事件是指通过网络传播法律法规禁止信息、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事件。

（2）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（3）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（4）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

网络与信息安全事件由低到高分为四级。

1.4.1 一般事件（Ⅳ级）

单个楼宇网络、单独信息系统遇到以上事件，受到一定程度的损坏，对相应楼宇或某个部门的教育教学、办公及宣传工作有一定影响，但不危害学院整体安全和秩序的突发公共事件。

1.4.2 较大事件（Ⅲ级）

某一部分网络、信息系统或院级应用系统（如：主页、办公网、校园网、邮件、域名等）遇到以上事件造成系统瘫痪，对学院的办公、科研、教学等造成一定损害，但是可以在一定时间内通过恢复、重建、屏蔽信息言论等技术手段进行处置的突发公共事件。

1.4.3 重大事件（Ⅱ级）

网络与信息系统遇到以上事件，造成全局瘫痪（所有应用系统），对学院安全、教育教学秩序、科研、办公和公共利益造成严重损害，但是可以在一定时间内通过恢复、重建、屏蔽信息言论等技术手段进行处置的突发公共事件。

1.4.4 特别重大事件（Ⅰ级）

网络与信息系统遇到以上事件，发生全局性大规模瘫痪，事态发展超出自己控制能力，学院安全、教育教学秩序、科研、办公和公共利益造成不可挽回的特别严重损害的突发公共事件。

1.5 工作原则

1.5.1 积极防御、综合防范。立足安全防护，加强预警，重点保护基础信息网络和重要信息系统；从预防、监控、应急处理、应急保障和打击犯罪等环节，从法律、管理、技术、人才等层面，采取多种措施，共同构筑网络与信息安全保障体系。

1.5.2 以人为本、快速反应。把保障公共利益以及师生的合法权益作为首要任务，及时采取措施，最大限度地避免损失；网络与信息安全突发事件发生时，应按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，尽快控制局面。

1.5.3 明确责任、加强协作。按照谁主管谁负责、谁运营谁负责的原则，建立和完善信息安全责任制、协调管理机制和联动工作机制；加强部门间的协调与配合，加强经常性的信息沟通和经验交流，各司其职，各尽其力，共同履行应急处置工作的管理职责。

1.5.4 依靠科学、平战结合。加强技术储备，规范应急处置措施与操作流程，实现网络与信息安全突发事件应急处置工作的科学化、程序化与规范化；树立常备不懈的观念，定期进行预案演练，确保应急预案发挥重要作用。

2. 应急处置组织机构及其主要职责

成立网络与信息安全突发事件应急处置工作组（以下简称处置工作组）

组 长：分管信息安全的学院领导

副组长：图书馆（网络信息中心）主任

成 员：各部门负责人

主要职责：按照国家有关要求，制定网络与信息安全突发事件应急预案，突发事件发生后，应在第一时间启动应急预案；负责学院网络与信息安全的监测预警和风险评估控制、隐患排查整

改工作；负责发布和取消预警信息；事件发生后，配合相关部门积极开展应对处置工作；加强教职工和学生的网络与信息安全培训，定期组织演练。

3. 预防预警

3.1 信息监测与报告

3.1.1 进一步完善网络与信息安全突发公共事件监测、预测、预警制度。落实责任制，按照“早发现、早报告、早处置”的原则，加强有关各类网络与信息安全突发公共事件和可能引发突发公共事件信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共事件时，按规定及时向学院突发公共事件应急处置工作领导小组（以下简称领导小组）报告，初次报告最迟不得超过半小时。重大和特别重大的网络与信息安全突发公共事件实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

3.1.2 建立网络与信息安全报告制度。发现下列情况时应及时向领导小组报告：利用网络从事违法犯罪活动的情况；网络或信息系统通信和资源使用异常；网络和信息系统瘫痪；应用服务中断或数据篡改，丢失等情况；网络恐怖活动的嫌疑情况和预警信息；其他影响网络与信息安全的信息。

3.2 预警处理与发布

3.2.1 对于可能发生或已经发生的网络与信息安全突发公共事件，立即采取措施控制事态，并在 1 小时内进行风险评估，判定事件等级。必要时应启动相应的预案，同时向处置工作组报告情

况。

3.2.2 处置工作组接到报警信息后应及时组织有关专家对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全警报级别，并及时向领导小组报告。

3.2.3 领导小组接到报告后，对发生和可能发生Ⅰ级或Ⅱ级的网络与信息安全突发公共事件时，应迅速召开应急处置工作会议，研究确定网络与信息安全突发公共事件的等级，决定启动本预案，同时确定指挥人员，并向相关部门进行通报。

4 . 事件应急响应

4.1 一般事件（Ⅳ级）

领导小组启动Ⅳ级响应，按照相关预案进行应急处置，网络信息中心相关负责同志及时赶赴现场，组织协调、通报学院所属部门，联络技术人员，配合技术人员及时处置并进行恢复。及时向网络信息中心负责人上报事件信息及处置进展情况。

4.2 较大事件（Ⅲ级）

在一般事件（Ⅳ级）响应基础上，网络方面可以通过使用备用设备等方式恢复；信息系统方面可以通过与系统所属单位配合进行处置。及时向网络信息中心负责人上报事件信息及处置进展情况。

4.3 重大事件（Ⅱ级）

在（Ⅲ级）响应的基础上，网络信息中心可以通过使用备用设备等方式恢复；信息系统方面可以暂停使用系统等进行处置。及时向院领导上报事件信息及处置进展情况。

4.4 特别重大事件（Ⅰ级）

在（Ⅱ级）响应的基础上，网络信息中心可以通过联系设备产品厂家、通信服务商等要求在最短时间内维修，并要求其提供替用设备等方式恢复；信息系统方面可以暂停使用系统等进行处置。及时向省委宣传部、省教育厅领导上报事件信息及处置进展情况。

5. 后期处置

恢复重建工作按照“谁主管谁负责，谁运行谁负责，谁开发谁维护”的原则，由网络信息中心负责组织并协调各相关单位制定恢复、整改或重建方案，报相关主管部门审核实施。

6 . 应急保障

6.1 人员保障

学院组建网络与信息安全突发事件应急预备队，一旦启动预案，立即投入使用。

6.2 培训演练保障

积极开展应急处置工作队伍的技能培训，定期进行安全演练，提高协同作战和快速反应能力。

7. 附则

本预案由处置工作组负责解释，自印发之日起实施。