武汉科技大学

武科大办发〔2022〕18号

关于印发《武汉科技大学网络安全事件应急预案》的通知

校内各单位:

经研究，特制定《武汉科技大学网络安全事件应急预案》。现予以印发，请遵照执行。

武汉科技大学

2022年10月18日

武汉科技大学网络安全事件应急预案

第一章　总　　则

第一条 编制目的。为建立健全学校网络安全事件应急机制，提高学校有效预防、及时控制和妥善处置各类突发网络安全事件能力，最大程度预防和减少网络安全事件及其造成的损害和影响，保障学校网络安全，保证正常的教学、科研、生产和生活秩序，维护公共安全和校园稳定，根据国家相关法律法规和上级文件精神，结合学校实际，制定本预案。

第二条 编制依据。预案依据《中华人民共和国网络安全法》、《互联网信息服务管理办法》等法律法规，以及《国家网络安全事件应急预案》、《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）、《教育部关于加强教育行业网络与信息安全工作的指导意见》、《教育系统网络安全事件应急预案》等相关规定编制而成。

第三条 适用范围。本预案适用于学校各二级单位。本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对学校、社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件，网络安全事件分类定义详见附件。

第四条 事件分级。根据可能造成的危害，可能发展蔓延的趋势等，学校网络安全事件分为四级：特别重大网络安全事件（I级）、重大网络安全事件（II级）、较大网络安全事件（III级）、一般网络安全事件（IV级）。

（一）符合下列情形之一的，为特别重大网络安全事件（I级）：

1.受攻击造成学校所有用户无法正常上网。

2.核心业务信息系统（网站）遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力。

3.网络病毒在全校或学校数据中心大面积爆发。

4.核心业务信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改。

5.其他对学校安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（二）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（II级）：

1.受攻击造成学校多个区域用户无法正常上网。

2.受攻击导致DNS服务解析效率大幅下降。

3.核心业务信息系统（网站）遭受严重系统损失，业务处理能力受到重大影响。

4.网络病毒在学校多个单位大面积爆发。

5.核心业务信息系统（网站）的信息或数据丢失或被窃取、篡改。

6.其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（三）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（III级）:

1.受攻击造成一个区域用户无法正常上网。

2.核心业务信息系统（网站）遭受较大系统损失，明显影响系统效率，业务处理能力受到影响。

3.网络病毒在学校某一个单位内广泛传播。

4.非核心业务信息系统（网站）的信息或数据发生丢失或被窃取。

5.其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（四）一般网络安全事件（IV级）:

除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

第五条 工作原则。

（一）统一指挥、密切协同。学校统筹协调网络安全应急指挥工作，建立与国家各级网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（二）分级管理、强化责任。按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各职能部门、直属单位和各学院党组织对本单位网络安全工作负主体责任，负责本单位网络安全应急工作，领导班子主要负责人是网络安全工作第一责任人。

（三）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

第二章　组织结构与职责

第六条 领导机构与职责。学校网络安全和信息化领导小组（以下简称网信领导小组）统筹协调全局性网络安全事件应急工作，指导各单位网络安全事件应急处置；发生I级和II级网络安全事件时，成立学校网络安全事件应急工作组（以下简称应急工作组），负责组织指挥和协调事件处置，应急工作组由分管网络安全工作的校领导，学校办公室、保密办、宣传部、保卫处及网络信息中心负责人组成，并根据实际情况吸纳学校相关二级单位人员参加应对工作。

第七条 办事机构与职责。学校网络安全和信息化领导小组办公室（以下简称网信办，网信办设在网络信息中心）负责网络安全应急管理事务性工作，对接上级网络安全应急办公室和网络安全职能

部门，向网信领导小组报告网络安全事件情况，提出应对措施建议，根据网络安全事件研判等级报请成立应急工作组，统筹组织做好网络安全预防、监测、预警和各项应急处置具体工作。

第八条 各单位职责。网络信息中心负责做好网络安全事件的监测、预警、报告、技术处置和为其他二级单位提供技术支撑等工作，并为网络安全事件应对提供决策支持；学校其他各二级单位按照应急部署，承担各自网络安全责任，全面落实各项工作。

第三章　监测与预警

第九条 安全威胁监测。学校加强对网络安全监测工具的配备；网络信息中心对网络安全威胁进行实时监测和定期扫描，通过建立多方协作的信息共享机制，采用多种途径监测和汇聚漏洞、病毒、网络攻击等网络安全威胁信息，依托各级教育系统网络安全工作管理平台和学校网络安全隐患整改网上流程，实现安全威胁信息的收集、校验、发布、跟踪。各二级单位加强对本单位网络和信息系统（网站）的常规网络安全威胁监测，对发生的威胁及时进行处置和报送。

第十条 预警研判。网络信息中心对监测信息进行研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知有关单位；认为可能发生重大以上（含重大）网络安全事件的信息，应立即向网信领导小组报告。

第十一条 预警响应。网信办负责组织预警响应工作，联系有关部门、安全专业机构和安全专家，对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调调度各方资源，做好各项应急准备，重要情况报网信领导小组。相关单位按照网信办要求，进入待命状态，检查设备、软件工具等，确保处于良好状态。

第四章　应急处置

第十二条 初步处置与事件研判。网络安全事件发生后，监测单位或事发单位应立即向网信办报告，不得迟报、谎报、瞒报、漏报，同时立即联系获取学校技术支撑，组织本单位应急队伍和工作人员，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。网信办经分析研判，初判为特别重大、重大网络安全事件的，应立即报告网信领导小组；认定为特别重大网络安全事件的，同时报省教育厅；对于人为破坏活动，应同时报当地网信部门和公安机关。

第十三条 应急响应。

网络安全事件应急响应分为I级、II级、III级、IV级等四级，分别对应学校特别重大、重大、较大和一般网络安全事件。

（一）I级和II级响应

发生特别重大和重大网络安全事件，由网信办向网信领导小组提出启动I级和II级响应的建议，经批准后，成立应急工作组。

1.启动指挥体系

（1）应急工作组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责，实行24小时值守，成员保持24小时联络畅通。

（2）网信办（网络信息中心）及相关二级单位进入应急状态，在应急工作组统一领导、指挥、协调下组织人员开展应急处置或支援保障工作，启动24小时值守，并派员参加应急工作。

2.掌握事件动态

（1）跟踪事态发展。事发单位与网信办保持联系，及时报告事态发展变化情况和处置进展情况。

（2）检查影响范围。网信办立即全面了解学校网络和信息系统是否受到事件波及或影响，并将有关情况及时报应急工作组。

（3）及时通报情况。应急工作组负责整理上述情况，重大事项及时报网信领导小组，并通报有关单位。

3.决策部署

应急工作组组织有关单位、专家、应急技术支撑队伍等方面及时研究对策意见，对处置工作进行决策部署。

4.处置实施

（1）控制事态防止蔓延。网络信息中心负责采取各种技术措施、管控手段，包括但不限于断开网络、关闭服务器、设置黑名单、暂停账号等，最大限度阻止和控制事态蔓延。

（2）消除隐患恢复系统。根据事件发生原因，针对性制定解决

方案，备份数据，保护设备，排查隐患。对业务连续性要求高的受破坏网络与信息系统要在保证安全的前提下及时组织恢复。

（3）调查取证。网络信息中心和事发单位在应急处置时必须做好相关证据的保存工作，在此基础上开展问题定位和溯源追踪工作，积极配合当地网信部门和公安机关开展调查取证工作。

（4）信息发布。学校党委宣传部根据实际，组织网络安全突发事件的应急新闻工作，指导协调各单位开展新闻发布和舆论引导工作。未经批准，其他单位不得擅自发布相关信息。

（5）协调支持。处置中需要校外技术及工作支持的，由网信办根据实际报应急工作组批准后，报请省、市网信办予以支持。

（6）次生事件处置。对于引发或可能引发其他安全事件的，网信办及时按程序报送应急工作组。

（二）III级响应

1.网信办（网络信息中心）和事发单位进入应急状态，按照本预案做好应急处置工作。

2.事发单位与网信办保持联系，及时报告事态发展变化情况和处置进展情况。网信办将重大事项及时报网信领导小组，并通报有关单位。

3.网络信息中心负责采取各种技术措施、管控手段，阻止和控制事态蔓延。网络信息中心和事发单位在应急处置时必须做好相关证据的保存工作，在此基础上开展问题定位和溯源追踪工作。

4.有关单位根据事件情况通报及网信办要求，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。

（三）IV级响应

事发单位自行做好应急处置，尽快消除隐患恢复系统，处置技术支撑由网络信息中心提供。

第十四条 应急结束。

（一）I级和II级响应

网信办提出建议，报应急工作组批准后，及时通报有关单位。

（二）III级和IV级响应结束

网信办根据实际决定III级和IV级响应的结束。

第五章 调查与评估

第十五条 调查与评估组织。特别重大及重大网络安全事件由网信办组织有关单位开展调查处理和总结评估工作，并将结果汇总报送网信领导小组。较大和一般网络安全事件由事发单位自行组织开展调查处理和总结评估工作，并将结果汇总报送网信办。

第十六条 调查与评估内容。网络安全事件总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后 5 天内完成。

第六章 预防工作

第十七条 日常管理。各单位应做好网络安全事件日常预防工

作，按照信息安全等级保护要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强网络和信息系统的安全保障能力。

第十八条 监测预警和通报。加强网络安全监测预警建设，建立安全隐患定期排查机制，健全网络安全监测预警和通报机制，及时发现并修复安全隐患和威胁，提高发现和应对网络安全事件的能力。

第十九条 应急演练。网络信息中心每年组织针对特别重大或重大网络安全事件的应急演练，检验和完善应急技术能力，提高实战能力。

第二十条 工作培训与宣传教育。网络信息中心定期组织网络安全研讨和培训，做到及时传达网络安全各项保障要求和规范规定，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育，提高各单位网信管理员和在校师生的网络安全意识和网络安全工作实效。

第七章 附 则

第二十一条 预案管理。本预案根据实际情况适时修订，修订工作由网信办组织。

第二十二条 预案解释及实施时间。本预案由网信办负责解释，自印发之日起实施。

附件：武汉科技大学网络安全事件分类

附件：

武汉科技大学网络安全事件分类

武汉科技大学网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他网络安全事件等六类。

一、有害程序事件

包括计算机病毒事件、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等 7 个子类，如系统感染勒索病毒、网站被上传 webshell、系统被渗透或控制等。

二、网络攻击事件

包括拒绝服务攻击事件、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等 7 个子类，如系统遭 DDOS 攻击、SQL 注入攻击、尝试爆破密码等。

三、信息破坏事件

包括信息篡改事件、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等 6 个子类，如发现网络上存在与系统数据高度雷同的数据，或发现业务数据被篡改。

四、设备设施故障

包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障等4个子类，如服务器硬件故障，机房供电中断等。

五、灾害性事件

指由不可抗力的灾害导致的网络安全事件，不可抗力的灾害包括水灾、台风、地震、雷击、坍塌、火灾等。

六、其他事件

指不能归为以上分类的网络安全事件。

武汉科技大学学校办公室　　2022 年 10 月 18 日印发