中共四川农业大学机电学院委员会文件

院党字〔2024〕5号

机电学院网络安全事件应急预案

第一章　总　则

第一条 为规范和加强学院网络安全应急管理工作，形成科学有效的应急工作机制，切实防范和有效处置对学校学院和社会有严重影响的网络安全事件，最大限度地降低由此所造成的损失和影响，特制定本预案。

第二条 本预案根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《四川农业大学网络安全事件应急预案》的有关要求编制。

第三条 按照《教育系统网络安全事件应急预案》规定，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。网络舆情与信息内容安全事件的应对，按照《四川农业大学信息化和信息安全管理办法》等有关规定执行。

第四条 工作原则

1. 统一领导，明确责任。成立网络安全应急工作小组，按照“谁主管、谁负责，谁主办、谁负责”的原则，明确落实应急处理部门和各单位的安全责任。

机电学院网络安全应急工作小组名单如下:

组　长: 唐　城　许丽佳

副组长: 黄锎靓　张黎骅

成　员: 张丽娜　周书玉　陈文生　杨　梅　唐诗怡　邓又天

2. 快速反应，科学处置。按照快速反应机制，及时获取信息、跟踪研判、科学决策、果断处置，最大限度地降低网络安全事件所造成的危害和影响。

3. 防范为主，加强监控。广泛宣传校园网络安全基本知识，切实落实网络安全防范措施，强化对校园网络系统舆情监控。

第五条 根据网络安全事件的起因、表现、结果等，将事件分为三类，即信息安全类事件、软件系统类事件和设施设备故障类事件。

1. 软件系统类事件

包括计算机病毒、木马、僵尸等有害程序事件，以及混合程序攻击、网络攻击等事件。

2. 信息安全类事件

包括信息篡改、信息假冒、信息泄露、信息窃取、信息丢失事件及其他信息破坏事件。

3. 设施设备故障类事件

包括软硬件自身故障、外围保障设施故障、人为破坏事故和

自然灾害等引发的其他设备设施故障类事件。

第六条 根据网络安全突发事件的可控性、严重程度和影响范围，事件一般分为四级：特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）。

1.特别重大网络安全事件（Ⅰ级）。指扩散性很强，危害性极大，严重影响我校声誉及安全稳定或造成我院网络大面积瘫痪，以及或能衍生其他重大安全隐患的网络安全事件。

2.重大网络安全事件（Ⅱ级）。指扩散性较强，危害性较大，影响我校声誉或造成我院网络部分瘫痪，影响学校安全稳定的网络安全事件。

3.较大网络安全事件（Ⅲ级）。指基本无扩散性，危害性较小，发生在我院个别部门的网络安全事件。

4.一般网络安全事件（Ⅳ级）。指无扩散性，危害性较小，发生在我院个别部门的网络安全事件。

第二章 组织机构与职责

第七条 学院成立机电学院网络安全应急工作小组，统一指挥、协调网络安全事件的应急处置工作。

第八条 学院网络安全应急工作小组主要职责

1. 研究制订我院网络安全应急处置工作计划和政策，推进应急机制和工作体系建设，检查落实预案执行情况。

2. 负责网络安全突发事件的预案演习、政策宣传培训，督促应急保障体系建设。

3. 研判网络安全突发事件信息，下达的应急指令和各项任务，进行应急处置。根据突发事件的影响程度，向上级汇报或请

求协助。

4. 总结评估应急处置工作，建立监督检查和奖惩机制。

第三章 监测预警与先期处置

第九条 信息监测

建立网络安全事件信息接收机制。通过舆情监控、网络员、应急值班等途径收集来自院内、外的紧急事件信息，建立并完善网络安全事件信息的接收机制。

第十条 预警报告

按照“早发现、早报告、早处置”的原则，当可能发生或已发生网络安全突发事件时，工作人员应立即采取措施控制事态发展，并按规定向应急小组报告。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。

第十一条 先期处置

网络安全应急工作小组在接到网络安全突发事件发生或可能发生的信息后，应加强与有关方面的联系，联络信息与教育技术中心或者系统开发商做好应急支援，必要时采用断网、关闭服务器等方式防止事态进一步升级。

第四章 应急处置

第十二条 应急指挥

应急工作小组接到汇报后应立即组织现场处置，查明事件状态及原因，根据问题的性质、危害程度，提出安全警报级别；迅速掌握现场处置工作状态，分析事件发展趋势，研究提出处置方案，提供现场指挥运作的相关保障，统一指挥应急处置工作。

第十三条 应急支援

应急工作小组可根据事态的发展和处置工作需要，及时向上级相关单位申请处置指导和支援。

第五章 后期处置

第十四条 善后处置

在应急处置工作结束后，迅速查找原因，处置涉及的人员或设备，统计各种数据，对事件造成的影响和损失进行分析，尽快恢复正常工作。

第十五条 调查和评估

在应急处置工作结束后，应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失状况和总结经验教训，写出调查评估报告。

第六章 应急保障

第十六条 应急物资保障

建立重要信息系统容灾备份系统，保证重要数据在受到破坏后，可紧急恢复。

第十七条 应急队伍保障

按照一专多能的要求建立网络安全应急保障队伍，同时与上级网络安全管理部门保持联系，作为我院网络安全应急支援单位。加强网络安全教育，增强安全意识。有针对性地开展应急演练，确保紧急事件发生后应急预案能有效执行。

第十八条 经费保障

网络安全事件应急处置资金，应列入年度工作经费预算，切实予以保障。

第七章　附则

第十九条 本预案由机电学院党委办公室负责解释，自发布之日起实施。

中共四川农业大学机电学院委员会

2024年4月1日

四川农业大学机电学院党委办公室　　2024年4月1日印