中国矿业大学网络安全事件应急预案

1 总则

1.1 编制目的

为提高学校应对网络安全事件的应急处置能力，建立健全科学、有效、反应迅速的网络安全应急工作机制，预防和减少校园网突发类网络安全事件及其造成的影响、损害，保障校园网络与信息系统正常运行，维护学校安全和稳定，特制定本预案。

1.2 适用范围

本预案适用于全校范围内网络与信息系统，尤其是校园网关键网络设施和重要信息系统安全突发事件的应急处置。按照《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》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。信息内容安全事件的应对，参照学校有关规定和办法。

1.3 事件分级

网络安全事件依据影响范围、严重程度，可分为以下四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1） 符合下列情形之一的，为特别重大网络安全事件（I 级）：

①关键网络基础设施出现故障，故障时间超过 36 小时，全校师生用户无法正常上网。

②网络病毒在全校范围内大面积爆发。

③学校主页、一卡通等核心业务信息系统（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。

④学校主页、一卡通等核心业务信息系统（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。

（2） 符合下列情形之一的，为重大网络安全事件（II 级）：

①关键网络基础设施出现故障，故障时间超过 24 小时，全校师生用户无法正常上网。

②网络病毒在学校多个单位范围内大面积爆发。

③招生系统、教务系统、邮件系统等核心业务信息系统（网站）遭受严重系统损失，造成系统长时间中断瘫痪，业务处理能力受到重大影响。

④招生系统、教务系统、邮件系统等核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改。

⑤其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（3） 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关键网络基础设施出现故障，故障时间超过 12 小时，全校师生用户无法正常上网或访问校内网站。

②网络病毒在学校某一个单位范围内广泛传播。

③科研、财务、办公自动化等重要业务信息系统（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。

④科研、财务、办公自动化等重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒。

⑤其他对教育系统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。

（4） 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。

1.4 工作原则

依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，充

分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

2 组织机构与职责

2.1.领导机构与职责

校突发公共事件应急工作领导小组（以下简称应急领导小组）统筹协调学校网络安全事件应急工作,指导各单位进行网络安全事件应急处置；发生特别重大、重大网络安全事件时，负责组织指挥和协调事件处置。

应急领导小组下设网络安全应急工作组,由学校网络安全工作委员会承担工作职能，统筹组织网络安全预防、监测工作，指导网络安全支撑单位做好应急处置的技术支撑工作。

2.2. 办事机构与职责

在应急领导小组的领导下，网络安全应急处置工作组办公室（即网络安全工作委员会办公室，以下简称网安应急办）负责网络安全应急管理事务性工作，及时收集网络安全事件情况，并向应急领导小组报告，提出网络安全事件应对措施建议，对接教育部网络安全应急办公室（以下简称部网络安全应急办）和省级行政部门。

2.3. 信息中心职责：负责学校网络安全工作统筹规划、建设、管理，做好网络安全事件的预防、监测预警、报告和应急工作，为学校网络安全事件应急处置提供决策支持和技术支撑。

2.4. 党委宣传部：负责学校舆情监测工作，对于涉及师生政治思想方面的预警性、倾向性、苗头性的问题加强分析研判，并妥善有效应对。

2.5. 保卫处：密切联系公安部门，配合信息办做好网络信息安全事件的处置工作。

2.6. 其他单位职责：按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，参照本预案制定单位内部应急预案，承担本单位网络安全主体责任， 全面落实各项工作。

3 监测与预警

3.1. 预警分级

按照紧急程度、发展态势和可能造成的危害程度，学校网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2. 安全监测

信息中心建立多方协作的信息共享机制，通过多种渠道监测、汇集漏洞、病毒、网络攻击、弱口令、暗链等网络安全威胁信息，并及时通报相关单位。各单位对本单位网络和信息系统（网站）的运行状况进行密切监测，一旦发生网络安全事件，应当立即通过电话等方式向网安应急办报告，不得迟报、谎报、瞒报、漏报。

3.3. 预警研判和发布

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，应立即向校应急办报告。

网安应急办可根据监测研判情况，发布黄色、蓝色预警。网安应急办组织研判，提出发布红色、橙色预警的建议，报应急领导小组批准后统一发布。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布机关等。

3.4. 预警响应

3.4.1 红色、橙色预警响应

（1） 校应急办组织预警响应工作，联系有关部门、专业机构和专家，组织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，做好各项准备，重要情况报应急领导小组。

（2） 组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估；密切关注舆情 动态，加强教育引导，采取有效措施管控风险。

（3） 有关单位实行 24 小时值守，相关人员保持通信联络畅通。

（4） 校应急办做好与专业机构沟通协调的准备工作；安全技术支撑部门进入待命状态，研究制定应对方案，检查设备、 软件工具等，确保处于良好状态。

3.4.2 黄色预警响应

（1） 应急工作组启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2） 应急工作组及时将事态发展情况报学校主要领导。

（3） 相关应急技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

3.4.3 蓝色预警响应

事发单位启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

3.5. 预警解除

预警发布机构根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1. 初步处置

网络安全事件发生后，事发单位应立即启动应急预案，立即组织本单位的相关人员根据不同的事件类型和事件原因，采取断网等有效措施进行处置，尽最大努力将损害和影响降到最低，保留网络攻击、网络入侵或网络病毒等证据，并电话报告本单位安全责任人和网安应急办。对于人为破坏活动，应同时报当地网信部门和公安机关。经网安应急办分析研判，初判为特别重大、重大网络安全事件，应立即报告校应急办。对于认定为特别重大、重大网络安全事件的，根据校领导意见，报告部网络安全应急办、省级教育行政部门。

4.2. 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

别对应特别重大、重大、较大和一般网络安全事件。

4.2.1 Ⅰ级、Ⅱ级响应

(1) 启动指挥体系

① 应急领导小组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责。应急领导小组成员保持 24 小时联络畅通，校应急办 24 小时值守。

② 相关单位进入应急状态，在应急领导小组的统一领导、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。

(2) 掌握事件动态

①跟踪事态发展。事发单位与校应急办保持联系，及时填写《教育系统网络安全事件情况报告》，将事态发展变化情况和处置进展情况上报校应急办。

②检查影响范围。各单位立即全面了解本单位主管的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报校应急办。

③及时通报情况。校应急办负责整理上述情况，重大事项及时报应急领导小组。

(3) 决策部署

应急领导小组组织有关单位、专家组、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。采取各种技术措施、管控手段，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及时组织恢复。

③调查取证。事发单位应在保留相关证据的基础上，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。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协调上级支持。处置中需要技术及工作支持的，由校应急办根据实际，报请应急领导小组批准后，商部网络安全应急办、省级教育行政部门予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，校应急办应及时按程序上报。在相关单位应急处置中，校应急办做好协调配合工作。

4.2.2 Ⅲ级响应

(1) 网络安全应急工作组进入应急状态，进行应急处置工作，处置情况及时向学校主要领导报告。

(2) 事发单位及时填写《教育系统网络安全事件情况报告》，报网安应急办。

(3) 处置中需要其他单位和网络安全应急技术支撑队伍配合和支持的，由网络安全应急工作组统一指挥、协调。

(4) 有关单位根据通报，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。

4.2.3 Ⅳ级响应

(1) 事发单位进入应急状态，进行应急处置工作，处置情况及时向分管校领导报告。

(2) 事发单位及时填写《教育系统网络安全事件情况报告》，报网安应急办。

5 具体处置措施

5.1. 有害程序事件

及时查清并断开传播源，判断病毒的性质、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，关闭相应的传播端口，必要时甚至关闭网络设备的连接端口,及时对受感染计算机进行杀毒处理，并在校园网公布病毒攻击信息以及杀毒、防御方法。

5.2. 网络攻击事件

判断入侵来源的 IP 地址，区分外网与内网，对于外网入侵，限

制对方 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。对于内网入侵，查清入侵来源，确定计算机 IP 地址和上网帐号，同时断开对应的交换机端口。最后针对入侵方法调整或更新入侵检测/防御设备规则。

5.3. 信息破坏事件

重要的信息系统的数据应提前做好异地备份,一旦数据遭到破坏性攻击，应立即断开网络连接，进行数据恢复。

5.4. 信息安全事件

当校内网站出现不良信息后，应当保留证据，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。

5.5. 设备故障事件

判断故障发生点和故障原因,如有备用设备,立即替换受损设备，否则联系供货厂商尽快抢修故障设备,优先保证校园网主干网络和主要应用系统的运转。如遇停电紧急事件，根据停电时间、UPS 电池的供电能力保障最重要的设备和信息系统继续运行,关闭次要的设备和信息系统，供电恢复后，及时恢复关闭的网络设备。

5.6. 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。

5.7. 其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。

6 应急结束

一般和较大网络安全事件应急结束由网络安全应急工作组决定，重大和特别重大网络安全事件应急结束由应急领导小组决定。

7 调查与评估

特别重大、重大网络安全事件由校应急办组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总上报应急领导小组。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，并将调查评估结果汇总上报网安应急办。

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。

8 总结上报

发生III级至 I 级事件时，应按照教育部办公厅《信息技术安全事件报告与处置流程（试行）》（教技厅函[2014]75 号）报告教育部，报告流程如下：

（1）事发紧急报告：事件发生后立即以口头通讯方式报教育部教育管理信息中心，涉及人为主观破坏事件应同时报当地公安机关。报告内容包括：时间地点，简要经过，事件类型与分级，影响范围，危害程度，初步原因分析，已采取的紧急措施。

（2）事中处置报告：应在事件发生后 8 小时内以书面报告形式报送教育部科技司（格式见附件 1）。

（3）事后整改报告：应在事件处置完毕后 5 个工作日内以书面报告形式报送教育部科技司（格式见附件 2）。

9 预防工作

10.1. 日常管理

各单位的网络安全负责人应组织开展网络安全事件日常预防工作，建立完善的应急管理体制。做好网络安全检查、风险评估和数据备份，加强信息系统的安全保障能力。

10.2. 监测预警和通报

信息中心建立网络安全监测预警和通报机制，并指导、监督各单位及时修复安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。

10.3. 应急演练

10.4. 信息中心每年组织应急演练，检验和完善预案，提高实战能力，各单位应积极配合。**培训宣传**

信息中心不定期组织各单位网络安全责任人、网络安全管理员开展网络安全培训,利用网络安全周向在校师生进行网络安全基本知识和技能的宣传教育，提高在校师生的网络安全意识。

10.5. 重要保障

在重大活动、会议期间，各单位要加强网络安全事件的防范和应急响应，确保网络安全。重点单位安排人员 24 小时值班，及时发现和处置网络安全事件隐患。

10 工作保障

11.1. 技术支撑

加强网络安全应急技术支撑队伍建设和网络安全物资保障,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。

11.2. 专家队伍

学校建立网络安全专家组,为网络安全事件的预防和处置提供技术咨询和决策建议。

11.3. 资金保障

信息中心应根据校园网络安全防护和应急处置工作的实际需要，申报网络安全设备、工具及安全服务等专项资金，纳入年度预算，由学校给予资金保障。

11.4. 责任与奖惩

学校对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，学校对相关单位责任人给予处分；构成犯罪的，依法追究刑事责任。

11 附则

12.1. 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由信息中心组织。

12.2. 预案解释

本预案由信息中心负责解释。

12.3. 预案实施时间

本预案自下发之日起实施。

校应急办电话：0516-83590013、0516-83590060

网安应急办电话：0516-83590047

附件 1：信息技术安全事件情况报告

附件 2：信息技术安全事件整改报告

附件 1

信息技术安全事件情况报告

单位名称：（需加盖公章）事发时间：年月日分

联系人姓名		手机	
		电子邮箱	
事件分类	□有害程序事件□网络攻击事件 □信息破坏事件□设备设施故障 □灾害事件□其他_____		
事件分级	□Ⅰ级□Ⅱ级□Ⅲ级□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1. 系统名称：_____ 2. 系统网址和 IP 地址：_____ 3. 系统主管单位/部门：_____ 4. 系统运维单位/部门：_____ 5. 系统使用单位/部门：_____ 6. 系统主要用途：_____ 7. 是否定级□是□否，所定级别：_____ 8. 是否备案□是□否，备案号：_____ 9. 是否测评□是□否 10.是否整改□是□否		
事件发现与处置的简要经过			

事件初步估计的危害和影响	
事件原因的初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
单位安全负责人意见（签字）	
单位主要负责人意见（签字）	

附件 2

信息技术安全事件整改报告

单位名称：（需加盖公章）报告时间：年月日

联系人姓名		手机	
		电子邮件	
事件分类	□有害程序事件□网络攻击事件 □信息破坏事件□设备设施故障 □灾害事件□其他_____		
事件分级	□Ⅰ级□Ⅱ级□Ⅲ级□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级□是□否，所定级别：_____ 8.是否备案□是□否，备案号：_____ 9.是否测评□是□否 10.是否整改□是□否		
事件发生的最终			

判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见（签字）	
主要负责人意见（签字）	