中共华东师范大学委员会文件

华师网信〔2021〕2号

关于印发《华东师范大学网络安全事件应急预案（2021年修订）》的通知

各单位:

为健全完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护学校及师生利益，维护学校网络安全稳定，根据国家相关法律法规，结合学校实际，对原《华东师范大学校网络安全事件应急预案（2019年修订）》（华师网信〔2019〕1号）进行了修订调整。现予印发，请各单位遵照执行。

特此通知。

中共华东师范大学委员会

2021年5月8日

华东师范大学网络安全事件应急预案
（2021年修订）

1 总 则

1.1 编制目的

健全完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护学校及师生利益，维护学校网络安全稳定。

1.2 编制依据

《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》等法律法规，《上海市网络安全事件应急预案》《教育系统网络安全事件应急预案》《关于加强教育行业网络与信息安全工作的指导意见》《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)等文件。

1.3 适用范围

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，对学校网络和信息系统（含网站，下同）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。关于信息内容安全事件的应对，参照有关规定和办法。

经评估分析我校的核心业务、支撑核心业务运行的网络及信息系统、影响核心业务运行的网络及信息系统安全风险、信息安全管理现状等关联关系，现将网络和重要信息系统应急预案（附件2）作为本预案的子预案。本预案适用范围包含但不限于以上信息系统。

1.4 事件分级

根据信息系统所承载的业务对国家安全、社会生活、学校工作的重要性以及业务对信息系统的依赖程度，将学校信息系统划分为重要信息系统和一般信息系统。重要信息系统包括学校网络安全等级保护二级及以上的信息系统。

本预案所指网络安全事件分为四级：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：

①关键信息基础设施遭受特别严重损失，造成系统大面积瘫痪，完全丧失业务处理能力。

②关键信息基础设施的重要敏感信息或关键数据丢失或被窃取、篡改。

③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）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

① ecnu.edu.cn域名的权威系统解析效率大幅下降。

②关键信息基础设施遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响。

③重要信息系统的重要敏感信息或关键数据发生丢失或被窃取、篡改。

④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:

①全校范围大量用户无法正常上网。

②重要信息系统遭受较大系统损失，明显影响系统效率，业务处理能力受到较大影响。

③网络病毒在全校范围内广泛传播。

④重要信息系统的信息或数据发生丢失或被窃取、篡改、假冒。

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。

（4）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。

1.5 工作原则

（1）统一指挥、密切协同。网络安全事件发生后，由学校网络安全与信息化领导小组（以下简称“学校网信领导小组”）统一领导、统一指挥，相关单位人员各司其职、密切协同、快速响

应、正确应对、果断处置。

（2）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，建立健全网络安全责任制、协调管理机制和联动工作机制。

（3）预防为主、平战结合。坚持事件处置和预防工作相结合，做好预防、预判、预警工作。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。

2 组织机构与职责

2.1 领导机构与职责

学校网信领导小组统筹协调学校层面网络安全事件应急工作，指导各二级单位网络安全事件应急处置；发生重大以上（含重大）网络安全事件时，成立学校网络安全事件应急工作组，负责组织指挥和协调事件处置。

2.2 办事机构与职责

在学校网信领导小组的领导下，网络安全与信息化管理办公室（以下简称“学校网信办”）负责协调组织学校网络安全事件应对工作，对接上级网信安全职能部门，统筹组织网络安全监测工作，指导网络安全支撑单位做好应急处置的技术支撑工作。

2.3 二级单位与职责

学校各二级单位对照本预案建立单位内部应急处置机制与预案，承担各自网络安全责任，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

3.2.1 事件监测

学校网信办会同相关部门通过多种渠道监测、发现已经发生的学校网络安全事件，将掌握的情况及时通知相关二级单位。各二级单位对本单位网络和信息系统的运行状况进行监测，一旦发生网络安全事件，应立即通过电话等方式报告学校网信办，不得迟报、谎报、瞒报、漏报。

3.2.2 威胁监测

学校网信办会同相关部门组织对学校网络安全威胁进行监测，建立多方协作的信息共享机制，依托校内外多种途径监测、汇聚关于漏洞、病毒、网络攻击等网络安全威胁信息，对发现的威胁及时处置、发布和上报。

3.3 预警研判和发布

学校各级单位对监测信息进行研判，认为需要立即采取防范措施的，及时通知有关单位；对可能发生重大以上（含重大）网络安全事件的信息及时向学校网信办报告。

学校网信办可根据监测研判情况，提出发布本校橙色以下（含橙色）预警的建议，报学校网信领导小组批准后发布。对达不到预警级别但有需要发布警示信息的，学校网信办可发布风险提示信息。

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、时限要求和发布单位等。

3.4 预警响应

3.4.1 红色、橙色预警响应

（1）学校网信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，协调组织资源调度和部门联动的各项准备工作，重要情况报学校网信领导小组、上级和当地网信部门。

（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；有关重大事项及时通报相关单位。

（3）有关单位实行24小时应急值守，相关人员保持通信联络畅通。

（4）信息化治理办公室（以下简称“信息办”）等安全技术支撑部门做好与专业机构沟通协调的准备工作；应急技术支撑队伍进入待命状态，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、蓝色预警响应

有关单位启动相应网络安全事件应急预案，组织开展预警响应。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。

3.5 预警解除

预警发布单位根据实际情况，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，根据不同的事件类型和事件原因，采取科学有效的处置措施，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。经分析研判，初判为特别重大、重大、较大网络安全事件的，立即报告学校网信办。学校网信办组织研判，认定为特别重大、重大网络安全事件的，报上级和当地网信部门；对于人为破坏活动，同时报公安机关。

4.2 应急响应

网络安全事件应急响应分为四级，级别由高到低依次用Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级表示，分别对应学校特别重大、重大、较大和一般网络安全事件。

4.2.1 Ⅰ级响应

发生特别重大网络安全事件，由学校网信办向学校网信领导小组报告，成立应急工作组。

（1）启动指挥体系

①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。工作组成员保持24小时联络畅通。

②事发单位进入应急状态，在工作组的统一领导、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。学校网信办与上级和当地网信部门保持联系，将事态发展变化情况和处置进展情况及时上报。

②检查影响范围。有关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学校网信办。

③及时通报情况。学校网信办负责整理上述情况，重大事项及时报工作组、学校网信领导小组、上级和当地网信部门。

（3）决策部署

工作组组织有关单位、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。如有必要积极配合网信部门和公安机关开展调查取证工作。

④信息发布。学校网信办根据实际，组织网络安全突发事件的应急新闻工作，指导协调相关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协调外部支持。处置中需要外部技术及工作支持的，由学校网信办根据实际，报当地网信部门、协调专业机构和专家予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，学校网信办应及时按程序上报。在相关部门应急处置中，学校网信办做好协调配合工作。

4.2.2 Ⅱ级、Ⅲ级响应

（1）事发单位进入应急状态，按照相关应急预案做好应急处置工作。

（2）事发单位及时报本单位网络安全第一责任人，由事发单位网络安全第一责任人报学校网信办。学校网信办将有关重大事项及时通报学校网信领导小组。

（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，由学校网信办予以协调。

4.2.3 Ⅳ级响应

事发单位按相关预案进行应急响应，并及时将事态发展变化情况报学校网信办。

4.2.4 特例

对于由于系统维护升级等原因导致的、预期时间和范围内的服务中断或者受到干扰的情况，其事件严重级别可参照上述级别描述调整降级。

4.3 应急结束

4.3.1 Ⅰ级响应结束

学校网信办提出建议，报学校网信领导小组批准后，及时通报有关单位。

4.3.2 Ⅱ级、Ⅲ级、Ⅳ级响应结束

事发单位提出建议，报学校网信办。学校网信办通报相关单位。

5 调查与评估

特别重大、重大网络安全事件由学校网信办组织有关单位进行调查处理和总结评估，并按程序上报。较大网络安全事件由学校网信办组织有关单位进行调查处理和总结评估。一般网络安全事件由事件发生单位自行组织调查处理和总结评估，相关总结调查报告报学校网信办。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原则上在应急响应结束后5天内完成。

6 预防工作

6.1 日常管理

各单位按职责做好网络安全事件日常预防工作，制定完善相

关应急预案和配套的管理制度，建立完善的应急管理体制。按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、隐患排查、风险评估和容灾备份，加强信息系统的安全保障能力。

6.2 监测预警和通报

各单位应加强网络安全监测预警和通报，及时发现并处置安全威胁。学校网信办和信息办应全面掌握学校信息系统情况，建立重点系统的网络安全监测预警和通报机制，并指导、监督校内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。

6.3 应急演练

学校网信办每年协调组织校内相关部门对特别重大事件进行演练，检验和完善预案，提高实战能力。各单位每年至少组织一次预案演练，并将演练情况报学校网信办。

6.4 宣传教育

各单位应将网络安全教育作为国家安全教育的重要内容，加强对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。同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提升在校师生的网络安全意识。

6.5 工作培训

各单位应定期组织网络安全培训，将网络安全事件的应急知

识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

7 保障措施

7.1 机构和人员

各单位应落实网络安全应急工作责任制，将网络安全应急工作作为重点工作予以部署。按照“谁主管谁负责”的原则，把网络安全应急工作责任落实到具体部门、具体岗位和个人，建立健全应急工作机制。各单位网络安全工作第一责任人、直接责任人、网络安全联络员信息及联络方式及时向学校网信办报备。

7.2 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。

7.3 专家队伍

建立学校网络安全应急专家组，完善专家研判分析与支撑保障机制，为网络安全事件的预防和处置提供技术咨询和决策建议。

7.4 信息共享与应急合作

加强与上级主管部门、网络安全职能部门、网络安全专业机构、行业学会等单位的对接与合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

7.5 经费与物资保障

学校和各单位为网络安全事件应急处置提供必要的经费保障，利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。各单位要根据实际需要，做好网络与信息系统设备储备工作。

7.6 通信保障

建立无线、有线以及基础电信网络相结合的应急通信系统，确保应急处置时通信畅通。

7.7 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，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附 则

8.1 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。修订工作由学校网信办组织。

各单位要根据本预案制定或修订本单位网络安全事件应急预案。各预案要做好与本预案的衔接，并报学校网信办。

8.2 预案解释

本预案由学校网信办、信息办负责解释。

8.3 预案实施时间

本预案自发布之日起实施。

附件：1. 网络安全事件分类

2. 网络和重要信息系统应急预案

3. 名词术语

4. 应急处置工作流程图

5. 应急工作组职责分工及联系方式

6. 网络安全事件报告表

附件 1:

网络安全事件分类

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、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

（1）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。

（2）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。

（3）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。

（4）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。

（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安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

附件 2:

网络和重要信息系统应急预案

（1）校网络突发事件应急预案

（2）门户系统突发事件应急预案

（3）科研管理系统突发事件应急预案

（4）招生系统突发事件应急预案

（5）研究生招生系统突发事件应急预案

（6）校园卡系统突发事件应急预案

（7）公共数据库系统突发事件应急预案

（8）财务系统突发事件应急预案

（9）邮件系统突发事件应急预案

（10）网站群系统突发事件应急预案

（11）开放教育学院网络教育门户网站突发事件应急预案

（12）开放教育学院网络教育教务管理系统突发事件应急预案

（13）开放教育学院必修课系统突发事件应急预案

（14）开放教育学院选修课系统突发事件应急预案

（15）开放教育学院论文系统突发事件应急预案

附件 3:

名词术语

【重要敏感信息】

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果:

（1）损害国防、国际关系;

（2）损害国家财产、公共利益以及个人财产或人身安全;

（3）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等;

（4）影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为;

（5）干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责;

（6）危害国家关键基础设施、政府信息系统安全;

（7）影响市场秩序，造成不公平竞争，破坏市场规律;

（8）可推论出国家秘密事项;

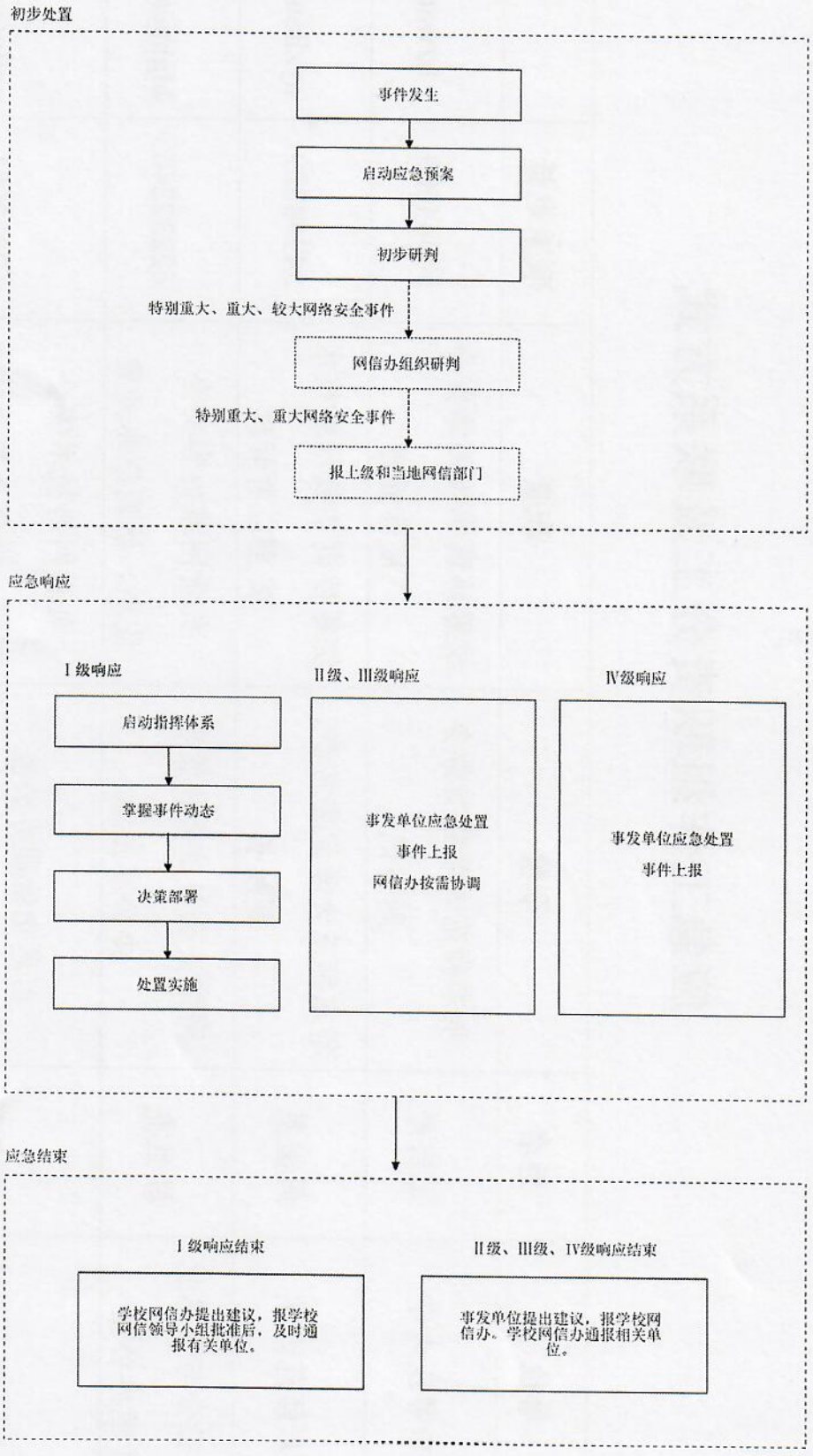
（9）侵犯个人隐私、企业商业秘密和知识产权;

（10）损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术云计算服务安全指南》（GB/T31167-2014））

附件 4:

应急处置工作流程图



附件 5:

应急工作组职责分工及联系方式

单位	姓名	职位	职责	联系电话	电子邮件
华东师范大学	王宏舟	华东师范大学党委常务副书记	统筹协调学校网络安全应急管理	54344609	hzwang@ecnu.edu.cn
华东师范大学	周傲英	华东师范大学党委常委、副校长	统筹协调学校网络技术安全应急管理	54344829	ayzhou@sei.ecnu.edu.cn
网络安全与信息化管理办公室	顾红亮	网络安全与信息化管理办公室主任	负责网络内容安全监测，协调应急处置	62232246	hlgu@admin.ecnu.edu.cn
信息化治理办公室	刘志鹏	信息化治理办公室副主任（主持工作）	负责网络技术安全监测、应急处置及技术支撑	62233081	zpliu@admin.ecnu.edu.cn

附件 6:

网络安全事件报告表

事件发生单位		发生时间	
安全事件现象描述 （包括事件发生现象、 发生位置、影响范围等）			
已经造成的损失和 预计损失			
已经采取的措施			
报告人		报告时间	