

黄冈师范学院网络安全事件应急预案

为了更好落实教育部制定的《教育系统网络安全事件应急预案》和湖北省教育厅办公室关于印发《湖北省教育系统网络安全事件应急预案》的通知要求，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，提高学校及校内各单位网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，保护学校公共利益，维护学校安全稳定，特制定黄冈师范学院网络安全事件应急预案。

1 总则

1.1 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，《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）《教育系统网络安全事件应急预案》《湖北省教育厅 公安厅关于加强全省教育行业网络与信息安全的指导意见》《湖北省教育系统网络安全事件应急预案》等相关文件。

1.2 适用范围

本预案适用学校及校内各单位。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、信息内容安全事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。其中，信息内容安全事件的应对，参照有关规定和办法。

1.3 事件分级

参照《教育系统网络安全事件应急预案》《湖北省教育系统网络安全事件应急预案》事件分级规定，结合学校实际，以及可能造成的危害、发展蔓延的趋势等，学校网络安全事件划分为四个等级：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关键信息基础设施或统一运行的核心业务信息系统（网站）遭受特别严重损失，造成应用系统（网站）大面积瘫痪，丧失业务处理能力。
- ②网络病毒在学校主页及多个应用系统（网站）大面积爆发。
- ③关键信息基础设施或统一运行的核心业务信息系统（网站）的重要敏感信息或关

键数据发生丢失或被窃取、篡改、假冒。

④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、事态发展超出学校控制能力的网络安全事件。

(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(Ⅱ级)

①关键信息基础设施或统一运行的核心业务信息系统（网站）遭受严重系统损失，造成应用系统（网站）瘫痪，业务处理能力受到重大影响。

②网络病毒在学校个别应用系统（网站）内部大面积爆发。

③核心业务应用系统(网站)的重要敏感信息或关键数据发生丢失或被窃取、篡改、假冒。

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、事态发展超出技术部门控制能力，需要学校各部门协同处置的网络安全事件。

(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重要业务应用系统（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。

②网络病毒在校内多个部门内广泛传播。

③重要业务应用系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒。

④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、对学校正常工作造成一定损害，网信办可处理的网络安全事件。

(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、不危及学校整体工作，网信办或各单位可处理的网络安全事件，为一般网络安全事件。

1.4 工作原则

学校网络安全和信息化委员会（以下简称网信委）统筹协调学校网络安全应急指挥工作，网络安全和信息化委员会办公室（以下简称网信办）负责落实具体网络安全事件应急预案。按照“谁主管谁负责、谁运维谁负责”的原则，校内各单位党委、党总支对本部门网络安全工作负主体责任，各单位主要负责人是网络安全工作第一责任人；坚持统一领导、分级负责；坚持统一指挥、密切协同，提高网络安全事件快速响应和科学处置能力；坚持预防为主，预防与应急相结合，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；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

在学校网信委的领导下，网信办统筹协调组织学校及各单位网络安全事件应对工作，发生特别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，并根据实际情况报请市网委办、网监部门和上级主管部门共同参加应对工作。

2.2 办事机构与职责

在学校网信委的领导下，网信办负责网络安全应急管理的统筹协调工作，对接省教育厅网络安全应急办公室和市网络安全和信息化委员会办公室，向学校网信委报告网络安全事件情况，提出特别重大网络安全事件应对措施建议，统筹组织网络安全监测工作，指导校内各单位做好应急处置的技术支撑工作。网信办设在信息化建设办公室，负责监测、报告网络安全事件和预警信息，为学校及各单位网络安全事件应对提出决策支持和技术支撑。党委宣传部负责学校舆情监测和信息内容安全类事件的处置，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，要加强分析研判，妥善有效应对。保卫部（处）负责涉及人为破坏类安全事件的处置，配合重大安全事件的处置，联系公安部门。

2.3 校内各单位职责

校内各单位负责统筹协调本单位、本部门网络安全事件应急工作，做好网络安全事件的预防、监测、报告和应急工作，制定相应的应急预案，承担本单位、本部门信息系统（网站）的网络安全责任。

3 监测与预警

3.1 预警分级

建立学校网络安全事件预警制度。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学校特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

学校网信办通过多种渠道监测、发现已经发生的网络安全事件，将掌握的情况立即

通知相关单位。各单位对本单位、本部门信息系统（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信办报告，不得迟报、谎报、瞒报、漏报；网信办对校内各单位信息系统（网站）的网络安全威胁进行监测，建立多方协作的信息共享机制，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，依托省教育厅网络安全工作管理平台实现安全威胁的收集、发布、上报处置结果。校内各单位收到网信办对本单位、本部门的信息系统（网站）的网络安全威胁后，应及时进行处置，并将处置结果上报到网信办。

3.3 预警研判和发布

校内各单位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，应当及时通知网信办，各单位的重要业务信息系统应当申请安全等级保护，其他信息系统建议进行等级保护测评。

校内各单位可根据监测研判情况，发布本单位、本部门的黄色及以下预警。网络安全事件发生后，第一，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，第一时间采取断网等有效措施，将损害和影响降低到最小范围，并保留现场和保存网络攻击、网络入侵或网络病毒等证据，同时报告本单位分管领导和网信办；第二，经分析研判，对于人为破坏活动，应同时报保卫部（处）；第三，网信办组织研判，认定为特别重大网络安全事件的，报网信委、市网信委和省教育厅网络安全信息中心。网信办研判，提出发布橙色、红色预警和涉及多个单位预警的建议，报网信委批准后统一发布，对达不到预警级别但又需要发布警示信息的，网信办和各单位可发布风险提示信息。网信办组织相关单位尽最大可能收集网络安全事件相关信息，鉴别性质，确定来源，弄清范围，评估网络安全事件带来的影响和损害，确认网络安全事件类别和等级。预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布单位等。

3.4 预警响应

3.4.1 红色预警响应

(1)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，协调高度各方资源，做好各项准备，重要情况报学校网信委。

(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)相关单位按照网信办要求，实行 24 小时值守，相关人员保持通信联络畅通。

(4)网信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 橙色预警响应

(1)学校、网信办、校内各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。

(2)各单位及时将事态发展情况报网信办，网信办密切关注事态发展，有关重大事项及时通报相关单位。

(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 黄色、蓝色预警响应

各单位根据预案，组织做本单位、本部门预警响应工作。

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 事件报告

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，第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场和保存网络攻击、网络入侵或网络病毒等证据，并报告本单位分管领导和网信办。经分析研判，对于人为破坏活动，应同时报保卫部（处）。网信办组织研判，认定为特别重大网络安全事件的，报网信委和省教育厅网络安全信息中心。

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，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 级响应

发生特别重大网络安全事件的，由网信办向网信委提出启动 I 级响应的建议，经批准后，成立工作组。

(1)成立指挥体系

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，网信办 24 小时值守。

②有关单位进入应急状态，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，并派相关人员参加网信办工作。

(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，及时填写《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到网信办。

②检查影响范围，相关单位立即全面了解本单位、本部门的信息系统（网站）是否受到事件的波及或影响，并将有关情况及时报网信办。

③及时通报情况。网信办负责整理上述情况，重大事项及时报工作组和教育厅网络安全信息中心，并通报相关单位。

(3)决策部署

工作组组织相关单位、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信息系统（网站）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。积极配合网信办和保卫部开展调查取证工作。

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，指导协调新闻发布和舆论引导工作。未经批准，校内任何单位不得擅自发布相关信息。

⑤协调支持。处置中需要技术及工作支持的，由网信办根据实际，报请工作组批准后，报网信委和省教育厅网络安全信息中心予以支持。

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

4.2.2 II级响应

网络安全事件的Ⅱ级响应，由学校确定发布。

(1)响应发布单位进入应急状态，按照相关应急预案做好应急处置工作。

(2)事发单位及时填写《网络安全事件情况报告》，上报网信办，网信办将有关重大事项及时通报学校网信委。

(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，商由相关部门予以协调。

(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 Ⅲ级、Ⅳ级响应

事件发生单位按相关预案进行应急响应。

4.3 应急结束

4.3.1 I级和Ⅱ级响应结束

网信办提出建议，报网信委和工作组批准后，及时通报有关单位，并将结束应急响应上报省教育厅网络安全信息中心。

4.3.2 Ⅲ级和Ⅳ级响应结束

由网信办及相关单位完成应急处置后，自行解除Ⅲ级、Ⅳ级响应状态。

5 调查与评估

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，并将调查评估结果汇总上报到网信委和省教育厅；较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；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，报网信办备案。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。

6 预防工作

6.1 日常管理

各单位应做好网络安全事件日常预防工作，根据本预案制定完善相关的专项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、风险评估和容灾备份，加强信息系统（网站）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，全面掌握本单位、本部门信息系统（网站）情况，网信办指导、监督相关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

网信办协调相关单位定期组织演练，检验和完善预案，提高实战能力，每年至少组织一次应急演练，每年年底前将本年度演练情况报省教育厅网络安全信息中心。

6.4 宣传教育

网信办、各单位应将网络安全教育作为国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规 and 政策的宣传教育，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，提高全校师生的网络安全意识。

6.5 工作培训

网信办应定期组织网络安全培训，提高网络维护人员网络安全意识及防御水平，将网络安全事件的应急知识列为领导干部和相关人员的培训内容，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

7 工作保障

7.1 机构和人员

网信办、各单位应落实网络安全应急工作责任制，提高网络安全意识和管理能力，并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岗位和个人，建立健全应急工作机制。

7.2 技术支撑

网信办、各单位应明确或建立网络安全技术支撑人员，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

学校应建立网络安全专家组，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。网信办、各单位应加强本单位、本部门的专业技术人员队伍建设，提高应急保障能力。

7.4 基础平台

网信办应加强网络安全工作管理平台建设，增强学校网络安全预警和态势感知能力，做到早发现、早预警、早响应，提高应急处置能力。

7.5 信息共享与应急合作

网信办应加强与省教育厅网络安全信息中心、市网信委办公室、网络安全专业机构和行业学会等单位的合作，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机制。

7.6 经费保障

学校、各单位应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、基础平台建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

7.7 责任与奖惩

网络安全事件应急处置工作实行责任追究制。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单位和个人给予适当表彰和奖励；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相关处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 信息安全等级保护制度

信息安全等级保护制度是保障和促进信息化建设健康发展的一项基本制度。根据《中华人民共和国网络安全法》、《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》（教技[2015]2号）等文件要求和规定。《中华人民共和国网络安全法》第二十一条“国家实行网络安全等级保护制度”和第五十九条“网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。”

8.2 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，预案要做好与本预

案的衔接，并报网信办。

8.3 预案解释

本预案由学校网信办负责解释。

8.4 预案实施时间

本预案自印发之日起实施。