**XXX单位**

**网络安全事件应急预案**

（XXXX年XX月XX日修订）

1总则

**1.1　编制目的**

为健全完善XXX单位网络安全事件应急工作机制，规范网络安全事件工作流程，提高网络安全事件应急处置能力，预防和减少网络安全事件造成的损失和危害，维护XXX单位主管系统安全稳定运行，依据国家和教育部有关规定，特制定本预案。

**1.2　编制依据**

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《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》《关于加强教育行业网络与信息安全工作的指导意见》《GB-T 20986-2023 信息安全技术 网络安全事件分类分级指南》等文件。

**1.3　适用范围**

本预案适用于XXX单位主管基础设施、公共平台及信息系统网络安全事件的管理。

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，参照有关规定和办法。

**1.4　事件分级**

XXX单位遵照教育部印发的《教育系统网络安全事件应急预案》中事件分级规定进行事件分级，具体分为四级: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)和一般网络安全事件(IV级)。

（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全国统一运行的核心业务信息系统(网站)遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力。

②关键信息基础设施或全国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丢失或被窃取、篡改。

③其他对教育系统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(II级):

①关键信息基础设施或核心业务信息系统(网站)遭受严重损失，造成系统瘫痪，业务处理能力受到重大影响。

②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。

③其他对教育系统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。

②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。

③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，对教育系统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。**XXX单位网络与信息安全工作领导小组(以下简称领导小组)统筹协调XXX单位网络安全应急指挥工作，建立与主管部门、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。

**（２）分级管理、强化责任。**按照“谁主管谁负责、谁运维谁负责”的原则，XXX单位各部门对本部门网络安全工作负主体责任。领导班子主要负责人是网络安全工作第一责任人。

**（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。

2 组织机构与职责

**2.1　领导机构与职责**

在主管部门的统筹协调下，领导小组统筹协调单位内全局性网络安全事件应急工作。

**2.2　办事机构与职责**

在领导小组的统一领导下，领导小组办公室负责XXX单位网络安全应急管理事务性工作，向领导小组报告网络安全事件情况，提出事件应对处置建议；组织XXX单位应急预案制定、培训及应急演练；组织网络安全事件监测预警、应急处置和技术支撑工作；对接主管部门，研判上报事件和预警信息；组织落实领导小组、主管部门对重特大网络安全事件的响应处置要求；统一指挥协调较大网络安全事件应对工作；根据需要监督指导一般网络安全事件的应对工作。

**2.3　部门职责**

**XXX部门：**负责组织落实领导小组办公室应急职责。

**XXX部门：**负责具体开展网络安全运行监测预警工作，收集汇总并报告预警和事件信息，从技术层面支持基础设施有关事件研判和具体应对处置工作，为网络安全事件的应对提供决策支持和技术支撑；负责组织制定针对机房、系统、网络等层面重要事件的专项应急预案，并定期组织开展专项应急预案演练和培训工作。

**信息系统主管部门：**负责具体开展本部门所主管公共平台、信息系统安全运行监测预警和应急处置工作，收集汇总并报告预警和事件信息；对接业务部门，从业务和技术层面支持事件研判和具体应对处置工作，为网络安全事件的应对提供决策支持和技术支撑；负责组织制定本部门所主管公共平台、信息系统的专项应急预案，并定期组织开展专项应急预案演练和培训工作；牵头组织本部门发生的一般网络安全事件的应急响应和处置。

**2.4　网络安全管理岗位职责**

**网络安全主管：**负责具体组织落实主管部门、领导小组对网络安全事件的应急管理要求；组织开展网络安全预警和事件信息研判、级别判定及信息通报工作，指挥协调应对处置工作。

**网络安全管理员：**负责网络安全应急处置协调工作，落实网络安全主管应急指示。负责收集、汇报事件信息及事件处理情况，执行本岗位相关事件处理和系统恢复工作。

**2.5　运维岗位职责**

负责网络安全事件报告、处置和恢复等具体工作。

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，XXX单位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的特别重大、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**

各部门按照职责分工做好网络和信息系统的运行情况监测，相关人员一旦发现异常情况，立即通知业务主管部门并保护现场、留存日志；业务主管部门网络安全责任人收到异常报告后，应立即组织对异常情况进行确认和初步处理，确认为网络安全事件的，立即上报网络安全主管，填写《网络安全事件情况初报》（见附件1）简要说明事件情况；网络安全主管核实情况后，应立即将网络安全事件信息上报领导小组办公室。事件发生后任何部门和个人不得迟报、谎报、瞒报和漏报。

**3.2.2　威胁监测**

各部门加强威胁信息的监测、收集，通过现有威胁监测技术手段及技术支撑单位提供的威胁情报等，多种途径监测、汇聚漏洞、病毒、网络攻击等威胁信息，对发生的威胁及时进行确认并上报网络安全主管。网络安全主管及时将威胁信息上报有关主管部门。

**3.3　预警研判和发布**

主管部门负责预警信息的研判、发布。网络安全主管根据已发布的预警信息，及时通报相关部门。

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　红色预警响应**

（１）部网络安全应急办组织开展红色预警响应工作。响应期间XXX单位实行24小时值守，相关人员必须保持联络畅通。

（２）网络安全主管按照部网络安全应急办研究制定的防范措施和应急工作方案，组织XXX单位相关部门开展应对预防工作，过程中密切关注事态发展，及时向部网络安全应急办、XXX单位领导小组上报事态发展情况和有关重大事项。

（３）XXX部门、信息系统主管部门等相关人员进入待命状态，协调专业机构研究制定应对方案，确保应急设备、软件工具等处于良好状态，并加强威胁监测和信息搜集工作，及时向网络安全主管上报事态发展情况。

**3.4.2　橙色以下（含橙色）预警响应**

（１）主管部门组织开展橙色以下（含橙色）预警响应工作。响应期间XXX单位相关人员必须保持联络畅通。

（２）网络安全主管根据主管部门对预警响应工作要求，组织XXX单位相关部门开展应对预防工作，过程中密切关注事态发展，及时上报事态发展情况和有关重大事项。

（３）XXX部门、信息系统主管部门做好与专业机构的沟通协调，做好应急准备工作，确保应急设备、软件工具等处于良好状态，并加强威胁监测和信息搜集工作，及时向网络安全主管上报事态发展情况。

**3.5　预警解除**

根据主管部门发布的预警解除信息解除预警，网络安全主管及时将预警解除信息通报XXX单位相关部门。

4应急处置

**4.1　初步处置**

网络安全事件发生后，事件发生部门向网络安全主管（填写《网络安全事件应急处置运转单》（见附件2））、业务主管部门上报事件信息，同时按照有关专项应急预案，第一时间对事件进行初步处置，防止事件蔓延。

网络安全主管收到事件报告后，在按照主管部门要求上报事件信息的同时，应立即启动应急预案，组织事件发生部门、技术人员、应急队伍、专业机构等根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力降低或减缓事件影响。同时根据事件已造成或可能造成的影响和危害进行事件级别研判，对初判为特别重大、重大和较大网络安全事件的，应立即报告领导小组办公室，其中初判特别重大、重大网络安全事件的，领导小组办公室应上报部网络安全应急办和XXX单位领导小组；初判较大网络安全事件，领导小组办公室批示后，由网络安全主管启动相应等级应急响应并指挥、协调事件应对处置工作；初判为一般网络安全事件的，交由事件发生部门网络安全责任人启动应急响应，开展事件应对处置工作。

事件处置过程中相关人员应注意保存网络攻击、网络入侵或网络病毒等证据。

**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**

根据《教育系统网络安全事件应急预案》有关规定，当XXX单位发生特别重大、重大网络安全事件时，由部网络安全应急办发布启动I级、II级应急响应。其中I级响应由教育系统网络安全事件应急工作组统一领导、指挥和协调应急相关工作。II级响应由部应急办统一领导、指挥和协调应急相关工作。在响应期间，XXX单位主要落实以下工作：

（１）XXX单位进入应急状态，启动24小时值守，相关人员必须保持联络畅通。启动I级响应时XXX单位派员参加部应急办工作。

（２）事件发生部门实时跟踪事态发展，并将事态发展变化情况和处置进展情况上报网络安全主管。同时，其他部门应立即全面了解本部门主管的网络和信息系统是否受到事件的波及或影响，并将有关情况及时上报网络安全主管。

（３）网络安全处整理、汇总上述事态发展和影响范围情况，将相关处置记录和有关重大事项及时上报网络安全主管、领导小组和部网络安全应急办。

（４）网络安全主管根据教育系统网络安全事件应急工作组、部网络安全应急办对特别重大、重大网络安全事件的应对处置决策部署，指挥协调相关部门开展应对处置工作。

（５）事件发生部门及事件相关部门网络安全责任人具体组织落实事件应对处置要求，最大限度阻止和控制事态蔓延，根据有关专项应急预案和事件发生原因，协同技术人员、应急队伍或专业机构有针对性的制定解决方案，采取数据备份、保护设备、排查隐患等方式尽快消除隐患，恢复系统正常运行。对业务连续性要求高的受破坏网络和信息系统，要及时组织恢复。

（６）网络安全主管组织相关部门、技术人员、专业机构等，在保留有关证据的基础上，依法合规开展问题定位和溯源追踪工作，并协调配合网信部门和公安机关开展的调查取证工作。

（７）未经批准，XXX单位任何人员不得擅自发布相关信息。

**4.2.2　III级响应**

发生较大网络安全事件时，由网络安全主管发布启动III级响应，按照相关预案组织开展应急响应工作。

（１）启动指挥体系

①中网络安全主管统一指挥、协调、组织事件应对处置工作。

②事件发生部门及事件相关部门进入应急状态，在网络安全主管的统一指挥、协调、组织下，开展应急处置、联络协调或支援保障工作。

（２）掌握事件动态

①跟踪事态发展。事件发生部门实时跟踪事态发展，并将事态发展变化情况和处置进展情况上报网络安全主管。

②检查影响范围。其他部门应立即全面了解本部门主管的网络和信息系统是否受到事件的波及或影响，并将有关情况及时上报网络安全主管。

③及时通报情况。网络安全处整理、汇总上述情况，并向网络安全主管、领导小组及主管部门汇报。

（３）决策部署

网络安全主管组织相关部门网络安全责任人、技术人员、应急队伍、专业机构等研究对策意见，对处置工作进行决策部署。相关部门网络安全责任人具体组织落实决策部署要求。

（４）处置实施

①控制事态防止蔓延，消除隐患恢复系统。

事件发生部门及事件相关部门应采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延，根据事件发生原因，协同技术人员、应急队伍或专业机构有针对性的制定解决方案，尽快消除隐患，恢复系统正常运行。对业务连续性要求高的受破坏网络和信息系统，要及时组织恢复。处置过程中需要有关资源保障支持的，网络安全主管予以协调。

②调查取证。

事件处置人员在处置过程中应注意保留相关证据。网络安全主管组织相关部门、技术人员、专业机构等在保留有关证据的基础上，依法合规开展问题定位和溯源追踪工作。

③信息发布。

对可能涉及的信息发布，由网络安全主管、领导小组或主管部门批准后组织开展。未经批准，任何人员不得擅自发布相关信息。

④次生事件处置。

对于引发或可能引发的其他网络安全事件，各部门应及时按照程序上报事件信息，并在事件处置过程中，做好协调配合工作。

**4.2.3　IV级响应**

发生一般网络安全事件时，由事件发生部门网络安全责任人发布启动IV级响应，按照相关预案开展应对处置工作，组织技术人员、应急队伍、专业机构等对事件进行处置，控制事态防止蔓延，并做好技术处理，尽快消除隐患恢复系统正常运行。过程中有关重大事项及时记录处置情况，并上报网络安全主管。

**4.3　应急结束**

**4.3.1　I级、II级响应结束**

部网络安全应急办发布I级、II级响应结束通报后，XXX单位终止应急响应工作，网络安全主管及时通报有关部门和单位。

**4.3.2　III级响应结束**

网络安全主管根据实际情况决定III级响应的结束，及时通报有关部门和单位。

**4.3.3　IV级响应结束**

事件发生部门完成应急处置后，自行解除IV级响应状态，响应结束信息上报网络安全主管，并及时通报有关部门和单位。

5调查与评估

重大以上（含重大）网络安全事件由网络安全主管协调配合主管部门组织开展的调查处理和总结评估工作，并将调查评估结果汇总上报领导小组和主管部门。

较大网络安全事件由网络安全主管组织开展调查处理和总结评估工作。一般网络安全事件由事件发生部门自行组织开展调查处理和总结评估工作，调查评估结果汇总上报网络安全主管。

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**

各部门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专项应急预案和配套管理制度，建立完善应急管理体制。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，加强信息系统的安全保障能力。

**6.2　监测预警和通报**

领导小组组织健全网络安全监测预警和通报机制，指导、监督各部门安全威胁修复情况。各部门应加强网络安全监测预警和通报，全面排查安全隐患，及时发现并处置安全威胁，提高发现和应对网络安全事件的能力。

**6.3　应急演练**

为检验应急预案有效性，并使相关人员了解应急响应流程和有关要求，在不影响信息系统正常业务运行的情况下，单位每年至少组织一次应急演练，并根据演练情况检验和完善应急预案，提高实战能力。演练前应预先制定演练计划，在计划中说明演练的场景。演练的整个过程应有详细的记录，并形成报告提交网络安全主管。

演练情况每年年底前报部网络安全应急办。

**6.4　宣传教育**

应加强突发网络安全事件预防和处置有关法律、法规、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XXX单位工作人员网络安全意识。

**6.5　工作培训**

单位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事件应急预案的学习，提高网络安全管理人员、技术人员的防范意识和安全技能。

7工作保障

**7.1　责任落实**

XXX单位实行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。网络安全职能部门及其他各部门按照“谁主管谁负责、谁运维谁负责”的原则，把网络安全应急工作责任落实到具体部门、岗位和个人，建立健全应急工作机制。

**7.2　技术支撑**

领导小组组织加强网络安全应急技术支撑队伍建设工作。各部门应明确网络安全技术支撑单位，包括为XXX单位提供基础设施运维、系统开发、网络安全等产品集成、供应，以及从事网络安全专业技术服务的机构等。技术支撑单位配合开展网络安全事件的应急处置工作，提供监测预警、预防防护、应急处置和应急技术支援等。

**7.3　物资保障**

各部门应建立必要的网络安全物资保障机制，做好网络和系统相关文档管理工作，包括使用手册、配置信息、网络拓扑图、工作流程及相关应急预案等，制定物资储备清单和相关单位、部门及领导联系方式清单；应配备必要的应急装备、工具，针对关键或易损设备，配备必要的备机、备品、备件以及其他必须的物资，确保网络安全事件发生时有关物资的保障。

**7.4　专家队伍**

领导小组组织完善专家分析研判与支撑保障机制，建立XXX单位网络安全专家组，为网络安全事件的预防和处置提供技术咨询和决策建议，提高应急保障能力。

**7.5　基础平台**

在加强XXX单位应急基础平台和管理平台建设健全工作的同时，各部门应依托部教育系统网络安全管理平台，增强网络安全预警和态势感知能力，做到网络安全事件的早发现、早预警、早响应和早处理，提高应急处置能力。

**7.6　信息共享与应急合作**

各部门加强与主管部门、监管部门、专业机构、行业学会和教育网网络中心等单位的合作，依托合作单位共享的预警和事件信息，及时进行内部信息共享和处置，提高XXX单位网络安全威胁和事件发现处置能力。

**7.7　经费保障**

XXX单位为网络安全应急工作提供必要的经费保障，利用现有政策和资金渠道，支持网络安全应急处置、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。相关部门应将应急经费列入部门年度预算，当上述费用产生时，在报请网络安全主管审批通过后，可使用此费用，待有关工作或事件处置结束后应提供相关文档作为经费使用审批附件。

**7.8　责任与奖惩**

网络安全事件应急处置工作实行责任追究制。XXX单位领导小组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。修订工作由领导小组统一组织。

相关部门应制定所主管基础设施、公共平台和信息系统的专项应急预案，做好与本预案的衔接，并报领导小组。

**8.2　预案解释**

本预案由领导小组负责解释。

**8.3　预案实施时间**

本预案自印发之日起施行。

附件1

XXX单位

**网络安全事件情况初报**

报告时间： 年 月 日 时 分

|  |  |  |  |
| --- | --- | --- | --- |
| 部 门 |  | 报 告 人 |  |
| 联系电话 |  | 电子邮件 |  |
| 发生网络安全事件的对象名称 |  | | |
| 网络安全事件的简要描述 |  | | |
| 事发部门网络安全责任人意见 | 签名： 日期： | | |
| 网络安全主管意见 | 签名： 日期： | | |

附件2

XXX单位

**网络安全事件应急处置运转单**

|  |  |  |  |
| --- | --- | --- | --- |
| 部 门 |  | 报告人 |  |
| 联系电话 |  | 电子邮件 |  |
| 发生网络安全事件的对象名称 |  | | |
| 网络安全事件简要描述 |  | | |
| 本次网络安全事件的初步影响状况 |  | | |
| 初步判断事件等级 | □特别重大(I级) □重大(II级) □较大(III级) □一般(IV级) | | |
| 初步判定的事故原因 |  | | |
| 当前采取的应对措施 |  | | |
| 事发部门网络安全责任人意见 | 签名： 日期： | | |
| 网络安全主管意见 | 签名： 日期： | | |
| 领导小组办公室意见 | 签名： 日期： | | |
| 事发部门处理情况汇总 |  | | |
| 事发部门网络安全责任人意见 | 签名： 日期： | | |
| 网络安全主管意见 | 签名： 日期： | | |
| 领导小组办公室意见 | 签名： 日期： | | |