**杭州市教育系统网络安全事件应急预案**

# 总则

## 编制目的

根据《教育系统网络安全事件应急预案》《浙江省教育系统网络安全事件应急预案》要求，健全完善全市教育系统网络安全事件应急工作机制，规范网络安全事件处置工作流程，提高全市教育系统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，维护全市教育系统安全稳定。

## 适用对象

本预案适用于全市各级教育行政部门及其直属学校（单位）。

## 工作原则

坚持预防为主，提高杭州市教育系统的网络安全防护意识和水平，加强信息系统安全体系建设，按照平台建设运行的特点和规律积极做好日常安全巡检工作，开展安全教育和培训工作，建立完善的安全管理、监督和审查制度，提高应对突发网络安全事件的能力。

提高快速反应能力，建立网络安全预警和事件快速反应机制，建立高效的事件汇报渠道，增强应急处理能力。保证对网络安全事件做到早发现、早报告、早处理、早恢复等环节的紧密衔接，一旦出现影响信息系统的安全事件，快速反应，及时准确处置。

加强安全监管，建立完善的信息系统安全监控和管理机制，对服务器、业务系统运行状况进行持续和重点巡检，及时发现网络安全隐患和事件迹象，进行安全预警并采取针对性的应对措施。

责任到人、制度保障。明确网络安全应急响应工作的角色和职责，保证各项工作责任到人，建立应急响应各项工作的处理流程，实现应急响应工作的规范化、制度化和流程化。

## 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》《关于加强教育行业网络与信息安全工作的指导意见》《教育系统网络安全事件应急预案》《浙江省教育系统网络安全事件应急预案》《浙江省关键信息基础设施网络安全事件应急处臵指南》《信息安全技术信息安全事件分类分级指南》等文件。

## 事件分级

（1）特别重大教育网络安全事件。国家、省关键信息基础设施或统一运行的核心业务系统（网站）遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力，对全市教育系统安全稳定和学校教育教学秩序构成特别严重威胁的；国家、省关键信息基础设施或统一运行的核心业务系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改，对全市教育系统安全稳定和学校教育教学秩序构成特别严重威胁的；网络病毒在全国教育系统大面积爆发；对教育系统安全稳定和学校教育教学秩序构成特别严重威胁，造成特别严重影响的其他网络安全事件。

（2）重大教育网络安全事件。国家、省关键信息基础设施或统一运行的核心业务系统（网站）在我市长时间中断，业务处理能力受到极大影响，市级重要信息系统（网站）瘫痪，丧失业务处理能力，对全市教育系统安全稳定和学校教育教学秩序构成严重威胁的；国家、省关键信息基础设施或统一运行的核心业务系统（网站）以及市级重要信息系统（网站）重要敏感信息或关键数据丢失或被窃取、篡改，对全市教育系统安全稳定和学校教育教学秩序构成严重威胁的；3个以上区、县（市）用户无法正常使用杭州教育城域网的；网络病毒在全省教育系统大面积爆发的；其他对教育系统安全稳定和学校教育教学秩序构成严重威胁，造成严重影响的其他网络安全事件。

（3）较大教育网络安全事件。县级以上重要信息系统（网站）遭受系统损失，造成系统中断，或数据发生丢失、被窃取、篡改，明显影响系统效率，业务处理能力受到较大影响的；网络病毒在全市教育系统多个区、县（市）广泛传播的；对教育系统安全稳定和学校教育教学秩序构成较大威胁，造成较大影响的其他网络安全事件。

（4）一般教育网络安全事件。个别区、县（市）用户无法正常使用杭州教育城域网的；对教育系统安全稳定和学校教育教学秩序构成一定威胁，造成一定影响的其他网络安全事件。

## 事件分类

按照《教育系统网络安全事件应急预案》《浙江省教育系统网络安全事件应急预案》等规定，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。信息内容安全事件应对，参照有关规定和办法。

（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、混合攻击程序事件、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）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。

（5）灾害性事件是指由于自然灾害等其他突发事件导致的网络安全事件。

（6）其他事件是指不能归为以上分类的网络安全事件。

## 工作原则

（1）统一指挥、密切协同。杭州市教育网络安全和信息化工作领导小组（以下简称市教育网信领导小组）统筹协调全市教育系统网络安全应急指挥工作，建立与省教育厅、市网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处理等环节的紧密衔接，做到快速响应、正确应对、果断处理。

（2）分级管理、强化责任。按照属地化管理原则，各级教育行政部门在本地党委和政府领导下，负责本地区教育系统网络安全应急工作。按照“谁主管谁负责、谁运维谁负责”的原则，各级党委（党组）对本地区本单位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。坚持事件处理和预防工作相结合，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理能力，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。

## 工作流程

（1）事前检测阶段：排查安全隐患和漏洞，并及时进行封堵，进一步完善安全策略，提出针对性地安全加固建议或安全解决方案。

（2）事中监测阶段：跟踪事态发展。事发单位与市教育网信领导小组保持联系，及时填写《教育系统网络安全事件情况报告》（ 见附件 1），将事态发展变化情况和处置进展情况上报市教育网信领导小组。

（3）事后处置阶段：接到应急事件处置指令，事发单位迅速行动。第一步：按照应急预案，采取紧急措施，尽可能地降低和避免事件造成的影响，恢复系统正常运行，并将有关情况迅速上报；第二步：分析造成安全事件的根源；第三步：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，并在 10 天内填报《教育系统网络安全事件整改报告》（见附件2）

# 组织机构与职责

## 2.1．领导机构与职责

市教育网信领导小组统筹协调全市教育系统网络安全事件应急工作，指导全市各级教育行政部门、各级各类学校网络安全事件应急处理。发生重大及以上网络安全事件时，成立全市教育网络安全事件应急处理工作组（以下简称市教育网安应急工作组），负责组织指挥和协调事件处理，并根据实际情况吸纳相关教育行政部门、业务主管单位和技术支撑单位等参加应对工作。发生特别重大网络安全事件时，在省教育厅、市委统一指挥下开展应急处理工作，具体参照有关规定执行。

## 2.2．办事机构与职责

在市教育网信领导小组的领导下，市教育网安应急工作组负责网络安全应急管理事务性工作，向市教育网信领导小组报告网络安全事件情况，提出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，指导网络安全支撑单位做好应急处理的技术支撑工作。

## 2.3．教育行政部门和学校职责

各级教育行政部门负责统筹协调组织本地区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。各级教育行政部门和直属学校（单位）按照“谁主管谁负责、谁运维谁负责”的原则，参照本预案制订应急预案，承担各自网络安全责任，全面落实各项工作。

# 应急处置

## 3.1. 应急指挥

（1）本预案启动后，根据事件等级由市教育网信领导小组安排相关人员担任现场指挥角色，参与指挥的有关部门人员迅速赶赴相应现场，进入应急岗位。相关联动部门按照本预案确定的有关职责立即开展工作。

（2）收集相关信息，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，调集和配置应急处置所需要的人、财、物等资源，统一指挥全局网络与信息安全应急处置工作。

## 3.2. 应急支援

本预案启动后，市教育网安应急工作组督促、指导和协调处置工作。根据事态的发展和处置工作需要，及时增派专家小组和应急支援单位，调动必需的物资、设备，支援应急工作。

参加现场处置工作的各有关部门和单位要在现场指挥部统一指挥下，协助开展处置行动。

## 3.3. 信息处理

（1）现场信息收集、分析和上报。市教育网安应急工作组对事件进行动态监测，评估，及时将事件的性质、危害程度和损失情况及处置工作等情况通知市教育网信领导小组，不得隐瞒、缓报、谎报。

（2）信息处理。市教育网安应急工作组要明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告和发布工作。

## 3.4. 扩大应急

经应急处置后，事态难以控制或有扩大发展趋势时，应实施扩大应急行动。

实施应急处置和紧急支援的各级政府和有关单位，要及时增加应急处置力量，加大技术、装备、物资、资金等保障力度，加强工作协调，努力控制事态扩大发展。

## 3.5. 应急结束

网络与信息安全突发公共事件经应急处置后，得到有效控制，由市教育网安应急工作组向市教育网信领导小组提出应急结束的建议，经批准后实施。

# 后期处置

## 4.1.善后处置

在应急处置工作结束后，事发单位要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作，统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施。责任单位要提供必要的人员和技术、物资和装备以及资金等的支持，并将善后处置的有关情况报市教育网安应急工作组。

## 4.2. 调查和评估

在应急处置工作结束后，市教育网安应急工作组应立即组织有关人员和专家组成事件调查组，在当地政府及其有关部门的配合下，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，并根据问责制的有关规定，对有关责任人员作出处理。

# 应急保障

## 5.1. 通信与信息保障

在整合各职能部门专业通信网的基础上，加强应急通信装备准备，建立备份系统和紧急保障措施，形成跨部门、多手段、多路由相结合的反应快速、灵活机动、稳定可靠通信系统。

## 5.2. 应急装备保障

各重要信息系统的业主单位在建设系统时应事先预留出一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。

## 5.3. 数据保障

重要信息系统均应建立异地容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。各容灾备份系统应具有一定兼容性，在特殊情况下各系统间可互为备份。

## 5.4. 应急队伍保障

按照一专多能的要求建立网络与信息安全应急保障队伍。由市教育网安应急工作组选择若干经国家有关部门资质认可的，具有管理规范、服务能力较强的企业作为全市网络与信息安全的社会应急支援单位，提供技术支持与服务；必要时能够有效调动机关团体、企事业单位等的保障力量，进行技术支援。

# 预案演练

建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

附件： 1.教育系统网络安全事件情况报告

2.教育系统网络安全事件整改报告

附件1：

**教育系统网络安全事件情况报告**

单位名称：（需加盖公章）事发时间：年月日 时 分

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 电子邮箱 |  |
| 手机 |  | 传真 |  |
| 事件分类 | □有害程序事件  □信息破坏事件  □灾害事件  □网络攻击事件  □设备设施故障  □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） | 系统名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  系统网址和IP地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  系统主管单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  系统运维单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  系统使用单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  系统主要用途：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否定级：□是□否，所定级别：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否备案：□是□否，备案号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否测评：□是□否  是否整改：□是□否 | | |

|  |  |
| --- | --- |
| 事发单位及事发网络和信息系统功能描述 |  |
| 事件发生时间、事态发展与处理的简要经过。 |  |
| 事件初步估计的危害和影响（影响程度、影响人数、紧急损失等情况） |  |
| 事件原因的初步分析 |  |
| 已采取的应急措施和效果 |  |
| 是否需要应急支援及需支援事项和工作建议 |  |
| 安全负责人意见（签字） |  |
| 主要负责人意见（签字） |  |

附件2：

**教育系统网络安全事件整改报告**

单位名称：（需加盖公章）事发时间：年月日 时 分

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮件 |  |
| 事件分类 | □有害程序事件  □信息破坏事件  □灾害事件  □网络攻击事件  □设备设施故障  □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） |  |