# 江苏省教育厅文件

苏教信〔2018〕4号

## 省教育厅关于印发《江苏省教育系统网络安全事件应急预案》的通知

各设区市教育局、各高等学校、南京工程高等职业学校，省教育厅各处室、直属事业单位：

为完善我省教育信息系统网络安全事件应急工作机制，提高我省教育系统网络安全应急处置能力，根据《中华人民共和国网络安全法》《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》要求，省教育厅制定了《江苏省教育系统网络安全事件应急预案》。现印发给你们，请认真贯彻落实。

省教育厅

2018年12月24日

（此件依申请公开）

# 江苏省教育系统网络安全事件应急预案

## 1 总则

### 1.1 编制目的

根据《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》要求，健全完善全省教育系统网络安全事件应急工作机制，规范网络安全事件工作流程，提高我省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，维护我省教育系统安全稳定。

### 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》《江苏省实施<中华人民共和国突发公共事件应对法>办法》《江苏省突发公共事件总体应急预案》《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》《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

本预案适用于全省各级教育行政部门及其直属单位（以下简称教育行政部门）、各级各类学校以及江苏省教育和科研计算机网（以下简称省教科网）网络安全事件的应对工作。

按照《教育系统网络安全事件应急预案》《江苏省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、信息内容安全事件、设备设施故障、灾害性事件和其他事件（详见附件 1）。其中信息内容安全事件，应参照有关规定和办法。

**1.4 事件分级**

参照《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》等事件分级规定，结合我省教育系统特点,以及网络安全事件可能造成的危害、可能发展蔓延的趋势等，江苏省教育系统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（I级）：

①关键信息基础设施或重要信息系统（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。

②关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对全省教育系统安全稳定和正常秩序构成特别严重威胁。

③网络病毒在全国教育系统大面积爆发并严重影响我省教育系统。

④其他对全省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大量省教科网用户无法正常上网。

②关键信息基础设施或重要信息系统（网站）遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

③关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对全省教育系统安全稳定和正常秩序构成严重威胁。

④网络病毒在全省教育系统范围内大面积爆发。

⑤其他对全省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区县级以上教育城域网、高校校园网大量用户无法正常上网，或无法正常通过专网访问教育管理核心系统（网站）。

②重要信息系统（网站）遭受较大系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

③重要信息系统（网站）的数据发生丢失或被窃取、篡改、假冒，对全省教育系统安全稳定和正常秩序构成较严重威胁。

④网络病毒在我省教育系统多个单位范围内广泛传播。

⑤其他对我省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）除上述情形外，对我省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（IV 级）。

**1.5 工作原则**

**（1）统一指挥、密切协同。**省教育网络安全和信息化工作领导小组(以下简称省教育网信领导小组）统筹协调全省教育系统网络安全应急指挥工作，建立与教育部、省网络安全职能部门、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“属地管理、逐级负责”原则，各级教育行政部门和学校在本地区党委和政府领导下，负责本地区本单位网络安全应急工作。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

省教育网信领导小组统筹协调全省教育系统全局性网络安全事件应急工作，指导我省各级教育行政部门、各级各类学校网络安全事件应急处置；发生重大网络安全事件时，成立省教育网络安全事件应急处置工作组（以下简称工作组），负责组织指挥和协调事件处置，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，在教育部、省委统一指挥下开展应急处置工作，具体参照有关规定执行。

### 2.2 办事机构与职责

在省教育网信领导小组的领导下，省教育网络安全应急办公室（以下简称省教育网络安全应急办）负责网络安全应急管理事务性工作，对接教育部网络安全应急办公室和省级网络安全职能部门，向省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置的技术支撑工作。省教育网络安全应急办的工作由江苏省教育网络安全和信息化工作领导小组办公室承担。

### 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、各类学校按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，参照本预案制定应急预案，承担各自网络安全责任，全面落实各项工作。

**2.4 其他单位职责**

中国教育和科研计算机网华东北地区网络中心和中国电信股份有限公司江苏分公司负责省教科网网络安全事件应急工作。

## 3 监测与预警

### 3.1 预警分级

建立全省教育系统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，我省教育系统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

省教育网络安全应急办通过多种渠道监测、发现已经发生的我省教育系统网络安全事件，将掌握的情况立即通知相关设区市教育行政部门和学校。各单位对本地区、本单位网络和信息系统（网站）的运行状态进行密切监测、一旦发生网络安全事件，应当立即通过电话等方式向上级教育行政部门报告，不得迟报、谎报、瞒报、漏报。

#### 3.2.2 威胁监测

省教育网络安全应急办组织对全省教育系统网络安全威胁进行监测，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，依托江苏省教育网络和信息安全通报平台实现安全威胁信息的收集、校验、发布、跟踪。各单位加强对本地区、本单位网络和信息系统（网站）的网络安全威胁监测，对发现的威胁及时进行处置和上报。

**3.3 预警研判和发布**

各级教育行政部门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；认为可能发生较大及以上网络安全事件的信息，应立即向省教育网络安全应急办报告。

红色预警由教育部网络安全应急办或省网络安全应急办发布。省教育网络安全应急办可根据监测研判情况，提出发布橙色预警和涉及多地区预警的建议，报省教育网信领导小组批准后统一发布。各设区市、县（市、区）教育网络安全应急办可根据监测研判情况发布本地区黄色及以下预警。对达不到预警级别但又要发布警示信息的，各级教育行政部门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、时限要求和发布机关等。

**3.4 预警响应**

**3.4.1 红色预警响应**

根据《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》精神，由教育部网络安全应急办或省网络安全应

急办组织红色预警响应工作。

（1）省教育网络安全应急办根据教育部网络安全应急办或者省网络安全应急办统一部署，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，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。重要情况报教育部网络安全应急办或者省网络安全应急办。

（2）有关单位实行24小时值班，相关人员保持通信联络畅通。

（3）省教育网络安全技术支撑部门进入待命状态，研究制订应对方案，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）省教育网络安全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跟踪研判，做好监测分析和信息搜索工作，研究制订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。密切关注舆情动态，加强教育引导，采取有效措施管控风险。重要情况报教育部网络安全应急办和省网络安全应急办。

（2）有关单位按照省教育网络安全应急办要求，实行24小时值守，相关人员保护通信联络畅通。

（3）省教育网络安全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，研究制订应对方案，检查设备、软件工具等，确保处于良好状态。

**3.4.3 黄色预警响应**

（1）省教育网络安全应急办、设区市教育行政部门或学校启动应急预案，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）有关设区市教育行政部门或学校及时将事态发展情况上报省教育网络安全应急办。省教育网络安全应急办密切关注事态发展，有关重大事项及时通报有关单位。

（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。

#### 3.4.4 蓝色预警响应

各级教育行政部门、各学校根据预案，组织做好预警响应工作。

### 3.5 预警解除

预警发布部门根据实际情况，确定是否解除预警，及时发布预警解除信息。

## 4 应急响应

### 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，组织本单位的应急队伍和工作人员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，初判为较大及以上网络安全事件的，应立即报告省教育网络安全应急办；对于人为破坏活动，应同时报当地网信部门和公安机关。

省教育网络安全应急办组织研判，认定为重大及以上网络安全事件的，报省教育网信领导小组批准后及时报教育部网络安全应急办和省网络安全应急办。

**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，分别对应教育系统特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。

**4.2.1 I 级响应**

对于特别重大网络安全事件，由教育部网络安全应急办、省网络安全应急办统一组织应急处置工作，具体要求以教育部网络安全应急办、省网络安全应急办部署为准。

（1）掌握事件动态

①跟踪事态发展。事发单位与上级网络安全应急办保持联系，将事态发展变化情况和处置进展情况上报。

②检查影响范围。有关单位立即了解本地区、本单位主管的网络和信息系统是否受到事件的涉及或影响，并将有关情况及时报上级网络安全应急办。

③及时通报情况。省教育网络安全应急办负责整理上述情况，重大事项及时报教育部网络安全应急办和省网络安全应急办。

（2）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。事发单位根据事件发生原因，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。省教育厅新闻办根据实际，组织网络安全突发事件的应急新闻工作，指导协调各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。处置中需要技术及工作支持的，由省教育网络安全应急办根据实际，商教育部网络安全应急办或省网络安全应急办予以支持。

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

**4.2.2 II 级响应**

发生重大网络安全事件，由省教育网络安全应急办向省教育网信领导小组提出启动 II 级响应的建议，经批准后，成立工作组。

（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，省教育网络安全应急办实行 24 小时值守。

②有关单位网络安全职能部门进入应急状态，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，并派员参加省教育网络安全应急办工作。

（2）掌握事件动态

①跟踪事态发展。事发单位与省教育网络安全应急办保持联系，及时填写《教育系统网络安全事件情况报告》（附件2），将事态发展变化情况和处置进展情况上报省教育网络安全应急办。

②检查影响范围。有关单位立即了解本地区、本单位主管的网络和信息系统是否受到事件的涉及或影响，并将有关情况及时报省教育网络安全应急办。

③及时通报情况。省教育网络安全应急办负责整理上述情况，重大事项及时报工作组和教育部网络安全应急办、省网络安全应急办。

（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。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。省教育厅新闻办根据实际，组织网络安全突发事件的应急新闻工作，指导协调各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。处置中需要技术及工作支持的，由省教育网络安全应急办根据实际，报请工作组批准后，商教育部网络安全应急办或省网络安全应急办予以支持。

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

**4.2.3 III 级响应**

发生较大网络安全事件，由事发单位所在的设区市教育行政部门或高校确定并启动 III 级响应。

（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《教育系统网络安全事件情况报告》，逐级上报省教育网络安全应急办。

（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，商省教育网络安全应急办或当地网络安全应急办予以协调。

（4）有关单位根据通报，结合各自实际有针对性的加强防范、防止造成更大范围影响和损失。

#### 4.2.4 IV 级响应

事发单位按相关预案进行应急响应。

### 4.3 应急结束

#### 4.3.1 I 级响应结束

以教育部网络安全应急办或省网络安全应急办部署为准。

#### 4.3.2 II 级响应结束

经工作组批准报教育部网络安全应急办或省网络安全应急办同意后，省教育网络安全应急办根据实际决定 II 级响应的结束，并通报有关情况。

#### 4.3.3 III 级、IV 级响应结束

由事发单位完成应急处置后，自行解除 III 级、IV 级响应状态，并报上级网络安全应急办。

## 5 调查与评估

特别重大网络安全事件的调查处理和总结评估工作根据教育部、省委有关规定执行。重大网络安全事件经教育部网络安全应急办、省网络安全应急办同意后，由省教育网络安全应急办组织有关单位开展调查处理和总结评估工作，并将调查评估结果报省教育网信领导小组后按程序报教育部网络安全应急办和省网络安全应急办。较大网络安全事件根据事发单位属性，由事发单位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逐级上报省教育网络安全应急办。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。

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，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，并填报《教育系统网络安全事件总结调查报告》（附件 3）。

## 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，根据本预案制订完善本单位、本地区的应急预案和配套的管理制度，进一步细化应急操作流程，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。各级教育行政部门应全面掌握本地区信息系统（网站）情况，建立本地区的网络安全监测预警和通报机制，并指导、监督本地区教育机构及时修复安全威胁，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

省教育网络安全应急办每年组织针对重大网络安全事件的跨地区、跨层级的应急演练，检验和完善预案，提高实战能力。各级教育行政部门、各高等学校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网络安全应急办。

### 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，充分利用网络安全宣传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

各单位应落实网络安全应急工作责任制，明确网络安全职能部门，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部门、具体岗位和个人，建立健全应急工作机制。

### 7.2 技术支撑

各级教育行政部门、各学校和厅直属单位，应明确或建立网络安全技术支撑单位，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、应急技术支撑工作。

### 7.3 专家队伍

省教育厅建立我省教育系统网络安全专家组，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。各级教育行政部门、各高等学校根据地方或单位实际，建立本地区、本单位的网络安全专家咨询队伍，提高应急保障能力。

### 7.4 基础平台

省教育厅加强江苏省教育网络和信息安全通报平台建设，通过平台通报网络安全事件信息和网络安全威胁信息，增强全省教育系统网络安全预警和态势感知能力。有条件的单位应加强监测预警通报和应急管理信息化平台建设，并与省级平台实现数据的双向共享，建立我省教育系统网络安全态势感知体系，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

加强与网络安全职能部门、网络安全专业机构、行业学会（协会）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处置机制。

### 7.6 经费保障

各单位应为网络安全应急工作提供必要的经费保障，完善政策和资金渠道，支持网络安全应急技术支撑队伍建议、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 奖惩

各级教育行政部门、各学校可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，依照有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。修订工作由省教育网络安全应急办组织。

各单位要根据本预案制订或修订本单位、本地区的网络安全事件应急预案。各预案要做好与本预案的衔接，并逐级报省教育网络安全应急办。

### 8.2 预案解释

本预案由省教育网络安全应急办负责解释。

### 8.4 预案实施时间

本预案自印发之日起实施。

附件：1.网络安全事件分类

2.教育系统网络安全事件情况报告

3.教育系统网络安全事件总结调查报告

附件 1

# 网络安全事件分类

网络安全事件可分为有害程序事件、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、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件。如系统感染勒索病毒、网站被上传 webshell、系统被渗透或控制等。

（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。如系统遭 DDOS 攻击、SQL 注入攻击、尝试爆破密码等。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件。如发现网络上存在与系统数据高度雷同的数据，或发现业务数据被篡改。

（4）信息内容安全事件是指通过网络发布、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、社会稳定和公共利益的事件。如网站被悬挂反动标识，或有人在网站互动区发布非法内容等。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障。如服务器硬件故障，机

房供电中断等

（6）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。如机房遭遇地震、火灾等。

（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

# 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__分

| | | | |
|---|---|---|---|
| 联系人姓名 | | 电子邮箱 | |
| 手机 | | 传真 | |
| 事件分类 | □ 有害程序事件　□ 网络攻击事件<br>□ 信息破坏事件　□ 设备设施故障<br>□ 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: _____<br>2. 系统网址和 IP 地址: _____<br>3. 系统主管单位/部门: _____<br>4. 系统运维单位/部门: _____<br>5. 系统使用单位/部门: _____<br>6. 系统主要用途: _____<br>_____ | | |

| | |
|---|---|
| | 7. 是否定级 □是　□否，所定级别：_____<br>8. 是否备案 □是　□否，备案号：_____<br>9. 是否测评 □是　□否<br>10.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、事态发展与处置的简要经过。 | |
| 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) | |

备注：省教育网络安全应急办联系电话：025-83752162。

附件 3

# 教育系统网络安全事件总结调查报告

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<br>□ 信息破坏事件　□ 设备设施故障<br>□ 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: _____<br>2.系统网址和 IP 地址: _____<br>3.系统主管单位/部门: _____<br>4.系统运维单位/部门: _____<br>5.系统使用单位/部门: _____<br>6.系统主要用途: _____<br>_____<br>7.是否定级 □是　□否，所定级别: _____<br>8.是否备案 □是　□否，备案号: _____ | | |

| | |
|---|---|
| | 9.是否测评 □是　　□否<br>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） | |

备注：省教育网络安全应急办联系电话：025-83752162。

抄送:中国教育和科研计算机网华东北地区网络中心、中国电信股份有限公司江苏分公司。

省教育厅办公室　　2018 年 12 月 26 日印发