

# 华南师范大学文件

华师〔2019〕111号

---

## 关于印发《华南师范大学网络与信息安全事件应急处置预案》的通知

各学院、各部处、各单位：

《华南师范大学网络与信息安全事件应急处置预案》已经学校校长办公会议讨论通过，现印发给你们，请遵照执行。

华南师范大学

2019年6月21日

# 华南师范大学网络与信息安全事件 应急处置预案

## 一、适用范围

根据《教育系统网络安全事件应急预案》(教技〔2018〕8号)以及广东省突发事件应急预案等有关规定,结合学校实际制定本预案。适用于我校自建自管的网络与信息系统的,尤其是校园网主干设施、重要信息系统、网站和新媒体平台内容信息安全突发事件的应急处置。

## 二、术语和定义

根据《华南师范大学网络与信息安全管理办法》的定义,本预案所指的学校网络与信息安全,包括校园计算机网络(以下简称校园网)、信息系统(含各类网站、论坛,下同)、新媒体平台公众服务号的运行安全和信息内容的安全。

网络与信息安全事件的分类:网络与信息安全事件主要分为有害程序、网络攻击、信息破坏、信息内容安全和灾害性事件等。

网络与信息安全事件的分级:网络与信息安全事件分为四级:I级(特别重大的网络与信息安全事件)、II级(重大网络与信息安全事件)、III级(较大网络与信息安全事件)、IV级(一般网络与信息安全事件)。

## 三、处置原则

网络与信息安全事件应急处置,依照“统一领导,迅速反应,

密切配合，科学处置”的组织原则和“谁主管谁负责、谁运维谁负责、谁使用谁负责”的协调原则，充分发挥各方面力量，共同做好网络与信息安全事故的应急处置工作。

#### 四、机构与职责

1. 全校网络与信息安全事故应急处置工作由华南师范大学网络安全与信息化建设领导小组统一指导、指挥、协调。各相关单位须坚决执行上级安全部门和学校网络安全与信息化建设领导小组的决定，密切配合，履行职责。

##### 2. 各机构职责

机构名称	工作职责
网络安全与信息化建设领导小组	决定 I 级和 II 级网络与信息安全事故应急预案的启动。 督促检查安全事件处置情况及各有关单位在安全事件处置工作中履行职责情况。 对全校各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。
信息化建设管理办公室	决定 III 级和 IV 级网络与信息安全事故应急预案的启动。 组织协调各有关单位的安全事件处置工作。 牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事故的协调处置。

机构名称	工作职责
网络中心	<p>负责校园网基础设施和大量用户终端的安全事件处置。</p> <p>负责信息化公共云平台、学校公共机房环境和信息化公共基础服务的安全事件处置。</p> <p>负责各类各级网络与信息系统安全事件处置的技术支持。</p>
党委宣传部 校团委 学生工作部 研究生工作部	<p>负责校园网络和新媒体平台公众服务号内容舆情信息的监控和管理，开展网上疏导和正面宣传，做好对外宣传工作。</p> <p>负责内容舆情突发事件的处置。</p> <p>负责应急处置过程中的舆论和宣传处置。</p>
保卫处	<p>负责统筹校园安全稳定工作，联系上级安全管理部门，及时反馈安全相关信息。</p> <p>配合网络中心对网络与信息安全事件进行调查、取证和处置。</p>
校内各二级单位	<p>负责本单位内部的网络与信息安全管理及突发事件应急处置，对照本预案建立单位内部应急处置机制。</p> <p>配合网络与信息安全管理机构落实相关应急处置措施。</p>

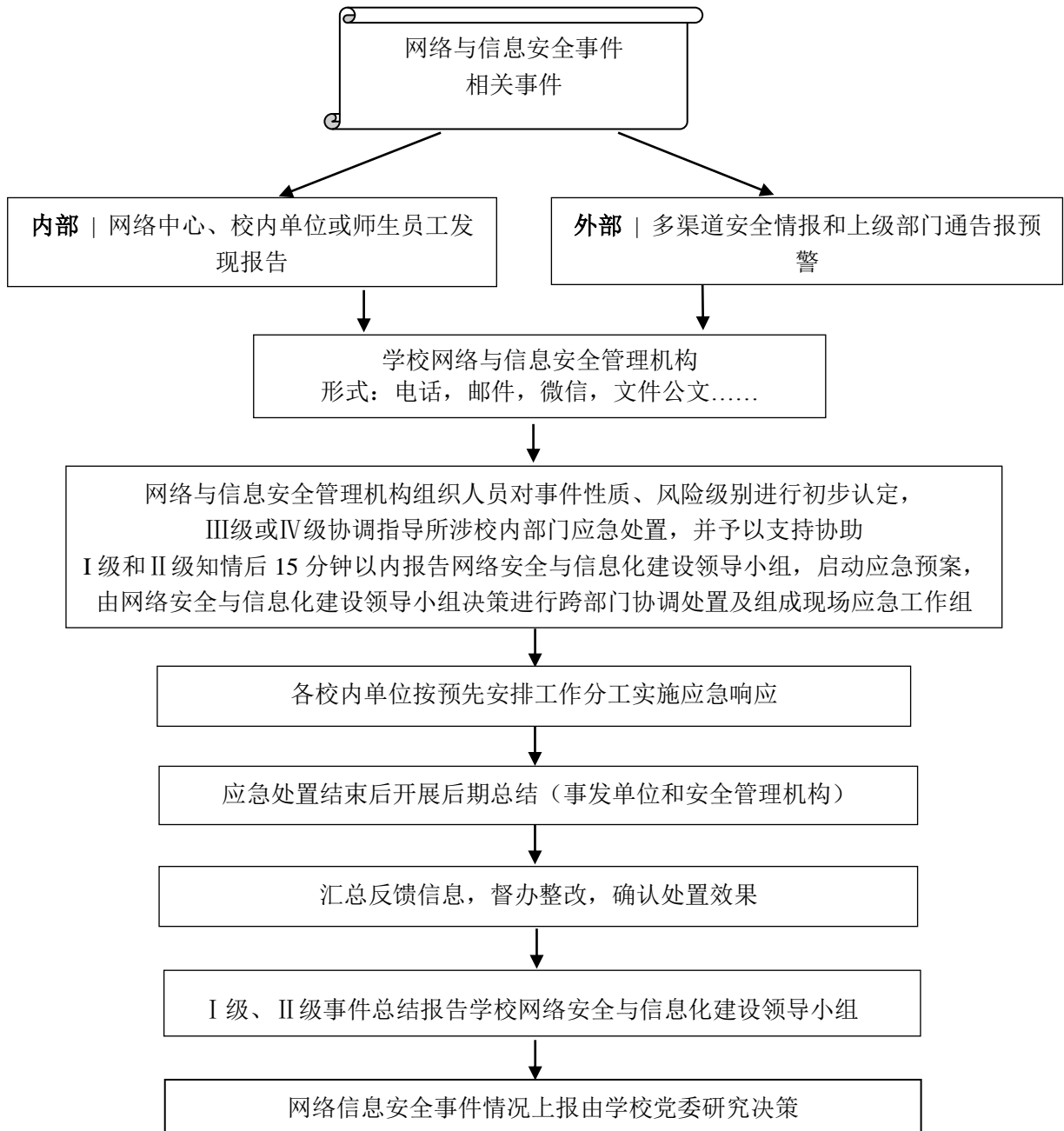
## 五、应急处置程序

1. 响应分级：网络与信息安全突发事件依据可控性、严重程度和影响范围的不同，分为以下四级。

响应分级	事件描述	影响范围	典型情况
I 级 特别重大	会使特别重要的信息系统遭受特别严重的系统损失，产生特别重大的工作和社会影响。	对学校正常工作造成特别严重损害。	灾害性事件、导致特别严重影响的信息内容安全事件。
II 级 重大	会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失，或使学校和师生员工造成重大经济或工作损失，产生的重大的工作和社会影响。	对学校正常工作造成严重损害。	导致严重影响的信息内容安全事件、信息破坏事件和网络攻击事件。

响应分级	事件描述	影响范围	典型情况
III级 较大	<p>会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息系统遭受特别严重的系统损失,或使学校和师生员工造成较大经济或工作损失,产生较大的工作和社会影响。</p>	<p>对学校正常工作造成一定损害。</p>	<p>导致较严重影响或破坏的信息破坏事件、网络攻击事件和有害程序事件。</p>
IV级 一般	<p>会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失,一般信息系统遭受严重或严重以下级别的系统损失,或使学校和师生员工造成较小经济或工作损失,产生一般的工作和社会影响。</p>	<p>对学校某些工作造成影响,但不危及学校整体工作。</p>	<p>影响或破坏程度较轻的网络攻击事件和有害程序事件。</p>

## 2. 响应流程



## 六、保障措施

### 1. 信息保障

学校网络与信息安全管理机构、各二级单位应建立健全并落

实突发公共安全事件信息报送、应急处置等各环节的运行机制，保持通讯方式方法方便快捷，确保信息报送渠道安全畅通，确保按应急处置预案进行信息报送。

## **2. 技术保障**

网络与信息安全管理机构、各二级单位应在网络中心的技术协助下，预先建立出现网络与信息安全事故时的技术处置手段，如“一键断网”“一键关机”等，降低安全事故风险与影响范围。

## **3. 资金保证**

网络与信息安全事故应急处置资金统一列入学校信息化专项和校园网维持发展经费预算。特殊情况由财务处单独列支，确保突发公共事件应急处置所需经费。

## **4. 人员保障**

网络与信息安全管理机构、各二级单位应按照学校的要求组建突发公共事件应急队伍，一旦启动预案，立即投入处置工作。

## **5. 培训与演练**

网络中心定期对校内网络安全技术与管理人员进行安全知识培训，增强预防意识和应急处置能力。有针对性地开展应急演练，模拟处置影响较大的信息安全事件，组织重点单位参加，检验预案的可执行性，确保相关措施有效落实。