山东科技大学

网络安全事件应急响应综合预案

（2020 年 3 月修订）

目录

1 总　则

1.1 编制目的

为了切实做好学校信息安全事件的防范和应急响应工作，进一步提高本学校预防和控制信息安全事件的能力和水平，减轻或消除信息安全事件的危害和影响，保障校园网平稳、安全、有序运行，结合学校工作实际，制定本预案。

1.2 编制依据

根据《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》《信息安全事件分类分级指南（GB/Z20986-2007）》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《教育信息化“十三五”规划》等相关规定以及学校制定的《山东科技大学突发事件总体应急预案》及各专项应急预案等文件，制定本预案。

1.3 适用范围

本预案适用于校园网运行及网络信息方面发生的有可能影响学校、社会和国家安全稳定的网络与信息安全突发事件，包括攻击事件、故障事件、灾害事件和其他类事件。

1.4 工作原则

校园网运行与网络信息安全事件的处理原则：

（1）依法管理：《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》《信息安全事件分类分级指南

（GB/Z20986-2007）》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《教育信息化“十三五”规划》等相关规定以及学校制定的《山东科技大学突发事件总体应急预案》及各专项应急预案等文件精神。

（2）分级负责、责任到人：学校一级由网络安全和信息化领导小组（以下简称“领导小组”）负责，各部门、各单位（以下简称“各单位”）二级由各单位主要领导负责，切实做到“责任落实，层层负责”。

（3）谁主管、谁负责，谁使用、谁负责：网络安全与信息化办公室（以下简称“网信办”）负责网络安全和系统安全，保障校园网的畅通运行和各服务器的正常运转；各单位负责其主管网站上的内容安全、业务系统的权限管理安全和系统内的数据安全，营造健康文明的网络环境，将有害信息造成的不良影响减小到最低限度。

2 组织机构与职责

学校应急响应工作机构按照角色划分为3个功能小组：领导小组，应急响应实施小组，应急响应专家小组。信息安全事件发生后，在领导小组的统一部署下，工作人员各司其职，并严格按照应急响应预案组织实施应急响应工作。

2.1 领导小组

对学校的信息安全工作进行全面的分析研究，制定工作方案，提供人员和物质保障，指导和协调各单位实施信息安全工作预案，处置各类危害校园信息安全的突发事件。具体职责包括：

（1）制定工作方案，提供人员和物质保障。

（2）审核批准应急响应策略、应急响应预案，批准和监督应急响应预案的执行。

（3）指导学校各单位的应急处置工作。

（4）启动定期评审、修订应急响应预案。

（5）组织协调有关部门查处利用计算机网络泄密的违法行为。

（6）负责组织的外部协作，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件的协调处置。

2.2 应急响应实施小组

当由于系统崩溃、病毒攻击、非法入侵等原因造成校园网运行异常或瘫痪时，根据信息安全事件的发展态势和实际控制需要，具体负责现场应急处置工作，尽快恢复学校网络的正常运行，具体职责包括：

（1）负责校园基础网络系统安全。

（2）负责计算机病毒疫情和大规模网络攻击事件的处置。

（3）负责校级网络与信息系统安全事件处置的技术支持。

2.3 应急响应专家小组

聘任校内外专家组成，主要职责是对网络安全中可能遇到的重大问题提供技术咨询，具体职责包括：

（1）对重大信息安全事件进行评估，提出启动应急响应的建议。

（2）研究分析信息安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议。

（3）分析信息安全事件原因及造成的危害，为应急响应提供技术支持。

3 事件分级分类

3.1 事件分类

校园网络与信息安全事件可分为三类：

（1）攻击事件：指校园网络与信息系统因病毒感染、非法入侵等造成学校网站或各单位网站主页被恶意篡改、交互式栏目和邮件系统发布有害信息；应用服务器与相关应用系统被非法入侵，应用服务器上的数据被非法拷贝、篡改、删除；在网站上发布的内容违反国家的法律法规、侵犯知识版权并造成严重后果等，由此导致的业务中断、系统宕机、网络瘫痪等。

（2）故障事件：指校园网络与信息系统因网络设备和计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等。

（3）灾害事件：指因洪水、火灾、雷击、地震、台风等外力因素导致网络与信息系统损坏，造成业务中断、系统宕机、网络瘫痪等。

（4）其他类事件：指不能归为以上分类的网络安全事件。

3.2 事件分级

依照《信息安全事件分类分级指南（GB/Z20986-2007）》，根据安全突发事件的可控性、严重程度、影响范围和校园网络与信息系统的实际情况，安全事件分为四级：特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）。

3.3 事件定级

依据事件分级和事件分类，综合信息系统损失和社会影响程度两个方面，对学校网络与信息安全事件分为四级，特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）。

事件等级	标志性颜色	判断标准	解决时限
特别重大（Ⅰ级）	红色	1.造成校园网络与信息系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于学校是不可承受的。 2.极大威胁国家安全，引起社会动荡，对学校有极其恶劣的负面影响，或者严重损害公众利益。	240 分钟
重大（Ⅱ级）	橙色	1.造成校园网络与信息系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于学校是可承受的。 2.引起社会恐慌，对学校有重大的负面影响，或者损害到公众利益。	120 分钟
较大（Ⅲ级）	黄色	1.造成校园网络与信息系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但学校是完全可以承受的。 2.可能影响到国家安全，扰乱社会秩序，对学校有一定的负面影响，或者影响到公众利益。	60 分钟
一般（Ⅳ级）	蓝色	1.造成校园网络与信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。 2.对国家安全、社会秩序、学校和公众利益基本没有影响，但对个别学生、教职工、法人或其他组织的利益会造成损害。	30 分钟

4 监测与预警

学校的网络通信平台、应用平台和信息系统，参照国家有关信息安全等级保护的要求，按照最终确定的保护等级采取相应的安全保障措施。不断完善网络安全防御系统，包括防火墙、堡垒机、上网行为管理、日志审计系统等，并对网络设备的安全性进行合理配置，根据实际需要做好升级更新工作。

建立健全安全事件预警预报体系，严格执行网络安全管理制度，加强对学校网络、网站、重要信息系统的监测、监控和安全管理，做好相关数据日志记录，设立内容过滤系统，确定合理规则，对校园网络进出信息实行过滤及预警。

做好服务器及数据中心的数据备份及登记工作，建立灾难性数据恢复机制。一旦发生校园网络与信息安全事件，根据事件影响范围和损失程度综合确定预警等级，并采取相应措施。

特殊时期，可根据领导小组的统一要求和部署，由应急响应实施小组进行统一安排，组织专业技术人员对校园网络和信息数据采取加强性保护措施，进行不间断的监控。

5 应急处置

5.1 基本流程

5.1.1 应急启动

特别重大（Ⅰ级）以及重大（Ⅱ级）事件发生时，直接启动的应急处置程序。

较大（III级）发生时，首先由应急响应实施小组进行处理，必要时联系维护支撑单位协助处理。

一般（Ⅳ级）事件发生时，由应急响应实施小组人员进行处理。

5.1.2 启动响应（Ⅰ级、Ⅱ级响应）

5.1.2.1 启动应急指挥体系

进入应急状态，领导小组履行应急处置工作的统一领导、指挥、协调职责，开展应急处置工作。

5.1.2.2 掌握事件动态

应急响应实施小组了解校园网受到事件波及或影响情况，及时将事态发展变化情况和处置进展情况上报领导小组。

5.1.2.3 决策部署

领导小组、应急响应专家小组和应急响应实施小组研究对策，对处置工作做出决策部署。

5.1.2.4 处置实施

领导小组组织应急响应专家小组和应急响应实施小组采取各种技术措施、管控手段，最大限度地阻止和控制事态发展，根据信息安全事件的分类，初步确定应急处置方式，区别对待。

对于能力范围内不能解决的，应立即邀请具备条件的单位进行技术协助。

应急处置人员在应急处置过程中应保留、收集相关证据。

相关信息通告由领导小组决定，并组织网络安全事件的应急新闻发布和舆论引导工作。未经批准，部门或人员不得擅自发布相关消息。

5.1.3 事件级别调整

在应急处置过程中，各专项工作组监控事件动态变化，当认为需要调整事件级别时，按有关流程上报并调整事件响应级别。

5.1.4 结束响应

通过应急处置成功解决信息安全事件后，尽快组织相关人员进行网络信息系统恢复，同时对信息安全事件应急响应进行总结。对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告。报告内容包括：

（1）问题或故障。

（2）原因分析。

（3）采取的应急措施或应急方案。

（4）结果评价。

（5）建议应采取的后续措施或需进一步考虑的解决方案。

（6）总结经验教训。

事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。

5.2 专项应急处理

5.2.1 非法言论

（1）信息确认：确认网站上出现不良信息（或者网页被篡改），将被篡改的页面进行拍照、截图或导出。

（2）通知人员：通知领导小组和应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX年X月X日X点X分，XXX网站XXX页面顶部出现不良信息，信息内容是XXX，已拍照）。

（3）关闭网站：立刻关闭网站。

（4）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等。

（5）确定攻击源：请有关厂商、网警协助确定网络攻击或信息破坏行为信息，确定攻击源。

（6）消除恶意程序：查找攻击源计算机，更新特征库，使用防病毒客户端或使用针对网络攻击或信息破坏程序的专杀工具查杀程序，如果网络攻击或信息破坏程序依旧不能清除恶意程序，则重新安装操作系统并安装防病毒客户端。

（7）加固系统：清除网络攻击、信息破坏程序或安装完操作系统后，应立即修改系统密码，更新系统补丁，升级防病毒客户端程序。

（8）网站恢复：恢复网站页面重新投入使用。

（9）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.2 黑客攻击

（1）信息确认：确认网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或黑客正在进行攻击，将被攻击的计算机、服务器进行拍照、截图或导出。

（2）断开网络：断开网络，并将受影响计算机、服务器的从网络中隔离出来。

（3）通知人员：确定事件类型，通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 服务器遭到黑客攻击，已隔离、拍照）。

（4）报警：领导小组会商后，认为情况严重，则立即向公安部门或上级机关报告。

（5）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等。如果部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）确定攻击源：请有关厂商、网警协助确定黑客攻击信息，确定攻击源。

（7）阻断攻击途径：封锁或删除被攻破的登录账号，阻断可疑用户进入网络的通道。

（8）消除有害程序：更新特征库，使用防病毒客户端或使用针对有害程序的专杀工具查杀有害程序，如有害程序依旧不能清除，则重新安装操作系统并安装防病毒客户端。

（9）加固系统：清除病毒或安装完操作系统后，应立即更新系统补丁，升级防病毒客户端程序，恢复或加固核心交换机、防火墙设置。

（10）客户端、服务器恢复到日常状态。

（11）恢复核心交换机、防火墙设置。

（12）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.3 网络病毒

（1）信息确认：确认计算机、服务器感染有害程序，将被攻击的计算机、服务器进行拍照、截图或导出。

（2）隔离系统：将受影响计算机、服务器的网络断开，拔出网线，使计算机、服务器保持单机状态。

（3）数据备份：对该设备的硬盘进行数据备份。

（4）通知相关人员：确定事件类型，通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 服务器感染有害程序，已隔离、拍照）。

（5）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等，如果部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）确定问题：请有关厂商协助确定有害程序信息，包括有害程序类型、来源、感染途径、感染范围、已遭受的损失等。

（7）消除有害程序：更新病毒库，使用防病毒客户端或使用针对有害程序的专杀工具查杀有害程序，如有害程序依旧不能清除，则重新安装操作系统并安装防病毒客户端。

（8）清查其他系统：利用病毒检测软件对其他机器进行病毒扫描和清除工作。

（9）加固系统：清除病毒或安装完操作系统后，应立即更新系统补丁，升级防病毒客户端程序。

（10）客户端、服务器恢复到日常状态。

（11）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.4 服务器软件系统故障

（1）信息确认：确认软件遭到破坏性攻击，将软件故障情况进行拍照、截图或导出。

（2）启动备份服务器系统：由备份服务器接管业务应用，将故障服务器脱离网络。

（3）转移数据：取出系统镜像备份磁盘，保持原始数据。

（4）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 服务器软件遭到破坏性攻击，已启用备份服务器、拍照）。

（5）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等，如果

部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）重新启动故障服务器系统：重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商，请求技术支援，作好技术处理。

（7）服务器软件系统恢复到日常状态。

（8）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.5 业务数据损坏

（1）信息确认：确认业务数据遭到损坏。

（2）备份数据：备份业务系统当前数据。

（3）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 数据遭到严重性损坏，已备份当前数据）。

（4）备份数据恢复：调用备份服务器备份数据进行修复，若备份数据损坏，调用异地备份数据。若短期内（<2 小时）无法恢复数据，立即向有关厂商请求紧急技术支援，并及时通知业务部门以手工方式开展业务或者暂缓上传上报数据。

（5）检查数据：检查历史数据和当前数据的差别，由相关系统运行负责人员补录数据。

（6）重新备份数据：备份业务系统当前数据。

（7）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.6 核心设备硬件故障

（1）信息确认：确认核心设备硬件发生故障。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 设备硬件发生故障）。

（3）确定问题：查找、确定故障设备及故障原因，若故障设备在短时间内无法修复，系统管理员应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（4）设备修复：能够自行处理，应立即用备件替换受损部件，如果不能自行处理的，立即与设备提供商联系，请求派维修人员前来维修。

（5）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成

网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.7 通信网络故障

（1）信息确认：确认通信线路故障（例如：中断、路由故障、流量异常、域名系统故障等）。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 通信线路中断）。

（3）确定问题：查清通信网络故障位置，隔离故障区域，并通知相关通信网络运营商查清原因；同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接。

（4）通知业务部门：若短期内（<2 小时）无法恢复，及时通知相关部门。

（5）恢复通信网络：恢复通信网络，通知相关部门网络恢复，保证正常运转。

（6）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.8 中心机房断电

（1）启用备用电源：启用 UPS 设备当前的蓄电能力。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理、供电时间等（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房断电，能够继续供电 X 小时）。

（3）通知业务部门：通知所有使用部门，抓紧完成信息处理工作、停止应用。

（4）温度控制：实时检测中心机房的室内温度，空调停止运行的情况下，立即采取其它措施降温，如开门通风等。根据相关情况关闭非重要设备，如机房内温度过高，应立即通知应用部门停止应用并关闭所有设备。

（5）咨询及供电规划：立即向供电部门询问何时恢复供电，并实时检测 UPS 的储存电能，并有计划地使用，如 UPS 电能不足以维持所有设备的运转，酌情关闭相关设备，保证关键设备的运作。

（6）电力恢复：开启设备，系统恢复到日常状态，通知相关部门系统恢复。

（7）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.9 中心机房火灾

无论火情大小，首先保证人身安全。

火情较大时：

迅速撤离现场，拨打 119 报警，并通知领导小组和应急响应实施小组，报告火情（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房火灾，人员全部撤离现场，已拨打 119 报警）。

火情较小时：

（1）火情控制：手持灭火器根据火情报警控制器显示的位置，到达火情发生位置，切断相应设备或机柜电源，若发现明火，立即使用手持式灭火器进行灭火。

（2）火情发展不能自动启动消防系统，需人工启动时，机房人员应在 30 秒内有序撤离机房，并拨打 119。

（3）通知相关人员：通知领导小组和应急响应实施小组，报告火情（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房火灾，人员全部撤离现场，已拨打 119 报警）。

（4）总结汇报：分析火情原因、评估损害程度、总结经验教训、提出改进办法、完善整改措施，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.10 中心机房水情

水情较小时：

若为空调漏水，则关闭空调，联系空调维保厂商进行维修，维修完成后开启空调除湿功能进行除湿。

若为墙壁渗水，联系相关人员维修渗水墙壁，维修完成后开启空调除湿功能进行除湿。

水情较大时：

（1）水情控制：根据水情现场的实际情况，做出相应的反应和处置，切断相关电源、水源，关闭相关设备，确保损失降到最小。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、水情状况、处理等（例如：20XX年X月X日X点X分，中心机房空调排水管破裂，造成机房积水，已切断空调电源和XXX设备电源）。

（3）水情处理：根据水情情况排除积水，维护设备，排除水情隐患。

（4）系统恢复：确认水情隐患排除后，技术保障小组进行系统的恢复。

（5）总结汇报：分析火情原因、评估损害程度、总结经验教训、提出改进办法、完善整改措施，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

6 预防工作

6.1 日常管理

各部门按职责做好网络安全事件日常预防工作，制定、完善相关专项应急处理方案，做好网络安全检查、隐患排查、风险评估和灾难备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

（1）建立健全应急保障体系。采用多种技术手段监控和保障单位信息系统安全，不断完善网络安全管理制度。

（2）全面落实网络安全等级保护基本要求。按照网络安全等级保护基本要求制定防护策略，设计防护方案，落实防护措施，检查防护效果，修补防护漏洞，保障网络安全。

（3）有效落实网络安全风险评估制度。在新系统上线、系统升级、网络改造、设备更新等关键信息技术资源发生重大变更及业务发生重大变化时，应重新识别、分析、控制风险。

（4）建设灾难备份系统。完善灾难备份相关制度、操作规范，对重要业务系统数据进行灾难备份，并定期开展灾备恢复演练。

（5）健全网络安全信息报告机制。各专项工作组应建立网络安全信息报告有关工作机制，公布信息报告流程和联系方式。各部门或个人发现校园网网络安全风险隐患和事件，均须

及时向应急响应实施小组报告。各专项工作组收到网络安全信息报告后，应认真研判并及时发布预警和响应通知。

6.2 应急演练

网信办指导各部门组织应急演练，检验和完善预案，提高实战能力。

各部门每年至少组织一次预案演练，并根据演练结果对应急预案进行评审和修订。

发生应急事件并处理完成后，各部门应当对事件进行分析总结，进行风险评估，改进不足，弥补漏洞。

在应急预案更新后或遇有可预见的网络安全事件时，应及时开展应急演练，检验应急预案的可行性，提高有关人员的应急响应熟练程度。

应急演练以应急预案为基础，在演练前应确定演练的目标、范围及方式，制定详细、严谨的应急演练方案，避免对正常业务造成不必要的影响。应急演练如涉及上级部门或其他部门，应事先做好沟通协调工作，避免干扰其正常工作。

6.3 宣传培训

各单位应充分利用各种媒介和其他有效宣传形式，加强突发网络安全事件预防和应急处置的有关法律、法规、政策和应急响应预案的宣传，开展网络安全级别知识和技能的宣传活动。

网信办将网络与信息安全突发事件的应急管理、工作流程等作为网络安全培训内容，增强应急处置工作中的组织能力，加强网络安全特别是网络安全应急预案的培训，提高防范意识和技能。

各单位应当在网信办指导下，每年至少组织一次安全应急培训，对各级应急成员、各专项工作组成员和相关的业务、技术人员进行应急知识培训。

6.4 重要活动期间的预防措施

在国家重要活动、会议等重要敏感时期，要加强网络安全事件的防范和应急响应，确保网络安全。领导小组统筹协调网络安全保障工作，各专项工作组加强网络安全监测和分析，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 责任落实

要落实网络安全应急工作责任制，建立健全网络安全应急工作机制，压实领导责任，把责任落实到具体部门、具体岗位和个人。

对网络安全突发事件工作中做出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的部门或个人，领导小组将给予约谈、通报或依法、依规给予问责或处分。

7.2 人力保障

加强学校信息安全人才培养，强化信息安全宣传教育，培养和建立一支高素质、高技术的信息安全核心人才和管理队伍，提高信息安全防御意识。

7.3 技术保障

加强学校网络安全管理平台建设，建立预警与应急处理的技术平台，进一步提高信息安全事件的发现和分析能力。从技术上逐步实现发现、预警、处置、通报等多个环节和不同的网络、系统、部门之间应急处理的联动机制。

7.4 物资保障

根据全省高校乃至全国网络信息系统安全防治工作所需经费情况，将本年度信息安全应急响应经费纳入年度财政计划和预算，建立校园网专项资金用于校园网安全事件的处置，购买相应的应急设施，避免时间拖延造成不必要的损失，保证应急响应技术装备的及时更新，以确保应急响应工作的顺利进行。

8 附　则

8.1 预案管理

在领导小组领导下，各部门应做好应急预案的维护工作，确保应急预案的完整性、实用性、可行性，有效指导应急响应工作。

（1）将应急预案最新版本分发给相关人员。

（2）根据信息基础设施、人员、业务变动情况及时更新应急预案。

（3）在应急响应或演练结束后，分析评估应急预案的执行效果，根据需要对应急预案进行修订、完善。

（4）原则上应急预案应每年进行评估、修订，发布更新，以确保应急预案的准确性和有效性。

8.2 预案解释

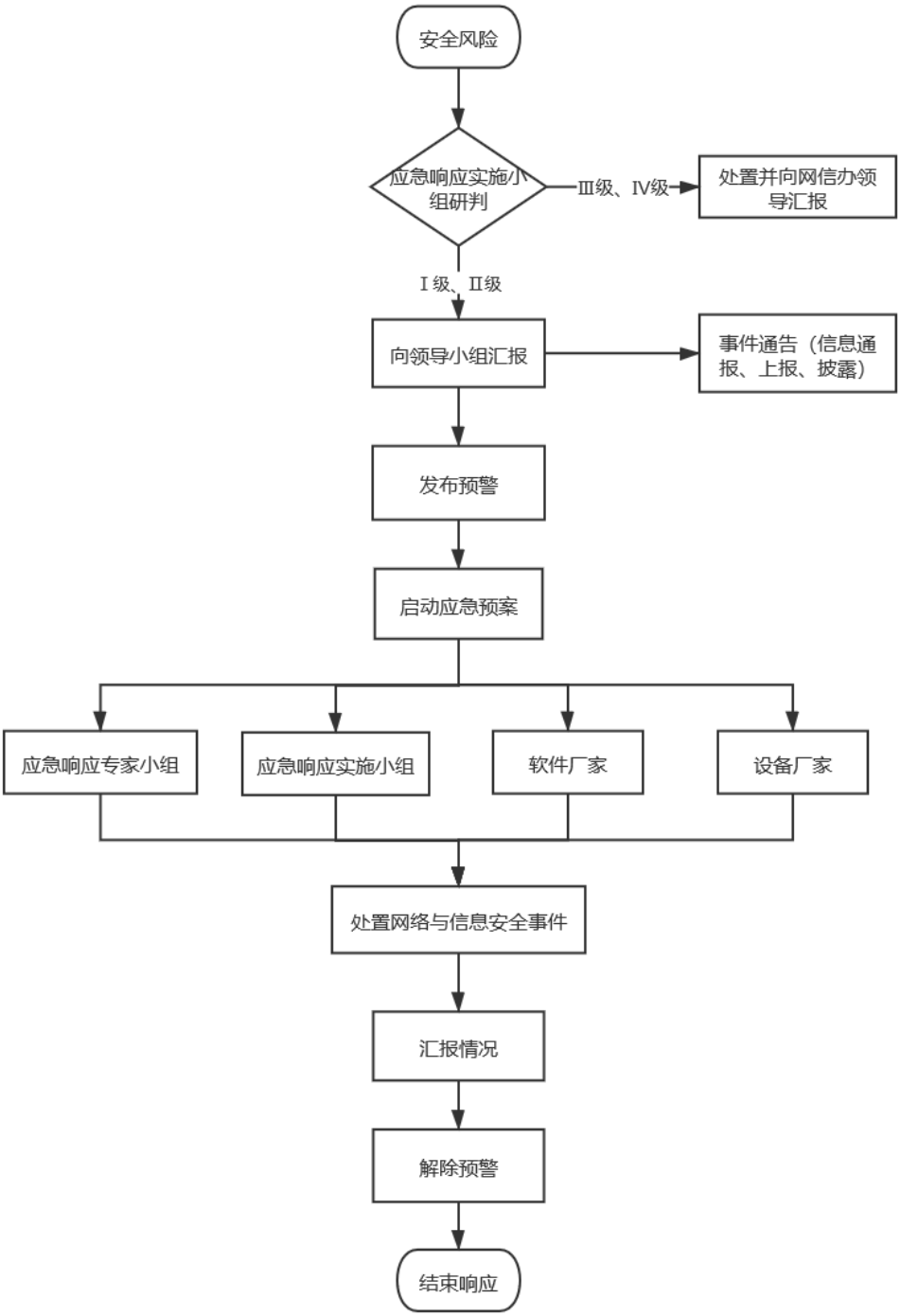
本预案由网络安全与信息化办公室负责解释。

8.3 预案实施时间

本预案自发布之日起施行。

9 附　件

附件 1：应急处置基本流程



附件 2：应急组织机构联系人清单

应急小组名称	姓名	所在部门	工作职责	联络方式	
				手机	紧急联系人及电话
网络安全和信息化领导小组					
应急响应实施小组					
应急响应专家小组					

附件 3：应急物资清单

应急物资清单					
序号	**物品名称**	**数量**	**存放位置**	**负责人/联系电话**	**备注**
1	备用服务器	3	中心机房	XXX 部门/人员	
2					
3					
4					
5					

附件 4：网络安全事件报告表

单位名称：（需加盖单位公章）

报告时间： 年 月 日 时 分

网络安全事件报告表	
发生事件的时间： 年 月 日 时 分	
发现事件的时间： 年 月 日 时 分	
报告人：	联系电话：
传真：	电子邮件：
通讯地址：	
发生网络安全事件的信息系统（设备、网络）或事项名称及用途：	
负责部门：	负责人：
网络安全事件的简要描述（如以前出现过类似情况也应加以说明）：	
网络安全事件的类型： □攻击事件 □故障事件 □灾害事件 □其他类事件	
网络安全事件的级别： □特别重大（Ⅰ级） □重大（Ⅱ级） □较大（Ⅲ） □一般（Ⅳ）	

初步判定的事故原因：
受影响的资产： ☐信息/数据_____. ☐硬件_____. ☐软件_____. ☐通信设施_____. ☐其他_____.
影响范围和严重程度：
已经采取的措施：
计划采取的措施：

附件 5：网络安全事件应急响应结果报告表

单位名称：（需加盖单位公章）

报告时间： 年 月 日 时 分

<table>
<tr><th colspan="6">网络安全事件应急响应结果报告表</th></tr>
<tr><td>报告人</td><td></td><td>联系电话</td><td></td><td>传真</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="2"></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td>系统名称</td><td colspan="2"></td><td>主要用途</td><td colspan="2"></td></tr>
<tr><td colspan="6">信息系统的基本情况（如涉及请填写）
1. 系统网址和 IP 地址：_____
2. 系统主管单位/部门：_____
3. 系统运维单位/部门：_____
4. 系统使用单位/部门：_____
5. 是否定级 □是 □否，所定级别：_____
6. 是否备案 □是 □否，备案号：_____
7. 是否测评 □是 □否
8. 是否整改 □是 □否</td></tr>
<tr><td colspan="6">网络安全事件描述</td></tr>
<tr><td colspan="6">最终判定事件原因及责任人（可加页附文字、图片以及其他文件）</td></tr>
<tr><td colspan="6">事件影响状况评估</td></tr>
</table>

事件级别	□特别重大（Ⅰ级） □重大（Ⅱ级） □较大（Ⅲ） □一般（Ⅳ）
影响时间	
影响范围	
事件后果	
主要处理过程及结果	
存在问题及建议	
网信办处理意见 签字： 日期：　　年　　月　　日	
领导小组审批意见 签字： 日期：　　年　　月　　日	

附件 6：应急演练方案（模板）

应急演练方案（模板）

一、方案概述

（1）目的

（2）时间

（3）范围

（4）内容

（5）应急场景

二、应急演练人员

（1）领导人员

（2）应急演练成员

三、应急演练过程

（1）……

（2）……

（3）……

四、应急资源

（1）……

（2）……

（3）……

附件 7：应急演练记录单

<table>
<tr><td colspan="4">应急演练记录单</td></tr>
<tr><td>演练名称</td><td></td><td>演练时间</td><td></td></tr>
<tr><td>组织人</td><td></td><td>演练地点</td><td></td></tr>
<tr><td colspan="4">记录内容：</td></tr>
<tr><td colspan="4">改进建议：</td></tr>
<tr><td colspan="4">记录人：</td></tr>
<tr><td>参加部门/人员：</td><td colspan="3"></td></tr>
</table>