济南市信息产业局文件

济信字[2007] 27号

关于印发济南市互联网网络与信息安全应急预案的通知

市直各部门，各县（市）区信息产业局、信息办，各大企业：

根据市政府要求，我局已制定完成《济南市互联网网络与信息安全应急预案》，现印发给你们，请遵照执行。

二〇〇七年四月十五日

济南市互联网网络与信息安全应急预案

目　录

1 总则

1.1 目的

1.2 依据

1.3 基本原则

1.4 适用范围

2 组织指挥体系及职责任务

2.1 网络与信息安全应急领导小组

2.2 应急领导小组办公室

2.3 各成员单位的主要职责

3 预警和预防机制

3.1 信息监测及预警报告
3.2 预防机制
4 应急响应启动条件
5 应急响应流程
5.1 预案启动
5.2 现场应急处理
5.3 安全事件的处理记录
5.4 结束响应
6 演练及维护
7 保障措施
7.1 应急队伍保障
7.2 设备保障
7.3 技术资料保障
7.4 经费保障
7.5 后勤保障

1 总则

1.1 目的

建立健全济南市网络与信息安全应急响应工作机制，科学应对网络与信息安全突发事件，有效预防、及时控制、最大限度地消除各类突发事件的危害和影响。

1.2 依据

依据《山东省网络与信息安全应急预案》（鲁信办字[2006]6号）》文件，《关于进一步加强互联网管理工作的意见》（济办发

[2006]4号），《济南市突发公共事件总体应急预案（试行）》（济政发[2006]23号）制定本预案。

1.3 基本原则

统一领导，协同作战。全市网络与信息安全突发事件应急工作由市网络与信息安全应急领导小组统一领导和协调，相关部门遵照“统一领导、归口负责、综合协调、各司其职”的原则开展工作。

明确责任，依法规范。各有关部门，按照“属地管理、分级响应、及时发现、及时报告、及时处置、及时控制”的要求，依法对网络与信息安全突发事件进行防范、监测、预警、报告、响应、指挥和协调、控制。按照“谁主管、谁负责，谁运营、谁负责”的原则，实行责任制和责任追究制。

防范为主，加强监控。开展安全教育和培训工作，提高全市的互联网网络安全防护意识和水平，积极做好日常安全工作，提高全市上下应对突发网络与信息安全事件的能力。加强对网络与信息安全隐患的日常监测，建立完善的信息系统安全监控和管理机制，保证对网络与信息安全事件做到快速觉察、快速反应、及时处理、及时恢复。

整合资源，条块结合。充分利用现有的网络与信息安全基础设施，依靠各有关部门的网络与信息安全工作力量，进一步完善应急响应救援体系，形成区域网络与信息安全保障工作合力。

1.4 适用范围

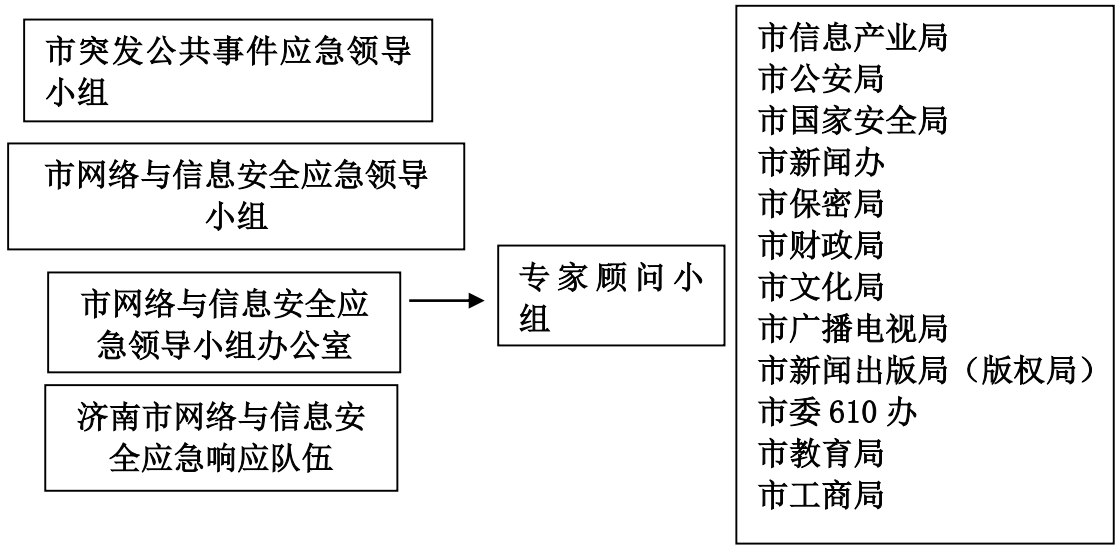
凡在我市范围内发生的严重影响网络与信息系统正常运行，造成系统中断、系统破坏、数据破坏或信息被窃取、泄露，网上涉及

违背宪法原则、危害国家安全、损害国家利益、破坏民族团结、宣扬邪教、宣扬迷信暴力、违背社会公德、散布谣言、侮辱诽谤他人、非法组织集会等违法和不良信息，对国家安全、政治外交、社会稳定或公众利益等方面造成不良影响以及造成一定程度经济损失的重大网络与信息安全事件，适用本预案。

2　组织指挥体系及职责任务

2.1 网络与信息安全应急领导小组

成立济南市网络与信息安全应急领导小组（以下简称应急领导小组），负责应急响应工作的整体规划和决策指挥。应急领导小组成员单位如下图所示:



2.2 应急领导小组办公室

市网络与信息安全应急领导小组办公室（以下简称应急领导小组办公室）设在市信息产业局，主要负责应急领导小组的日常工作，负责建立健全协调机制和信息通报机制，制定相应的应急处理工作流程，明确各部门在应急协调工作中的任务和责任；负责各项

应急准备工作，主要包括制定应急响应规划、应急队伍建设、应急资源准备、灾难恢复准备、发布预警信息、应急响应培训和演练及其他应急响应相关工作；按照应急领导小组的命令和指示，组织协调各成员单位，落实全市网络安全应急保障工作。

2.3 各成员单位的主要职责

市信息产业局：负责网络及信息安全应急支援中心建设，依法对通信网络运营企业、互联网接入服务提供商及互联网信息服务提供者进行监管，对网上有害信息进行监控和封堵；负责推动相关网络与信息安全关键技术和产品研发，组织网络与信息安全应急响应技术队伍与异地容灾备份系统建设，组织全市网络与信息安全认证体系建设。

市公安局：负责打击破坏攻击网络和传播计算机病毒等违法犯罪活动的应急协调工作，加快推进信息网络安全报警处置系统建设工作。会同有关部门，积极开展网络安全等级保护工作，对重要信息系统的安全保护及安全工作进行监督。对互联网接入服务单位、联网单位安全管理制度及安全防控措施的落实情况进行监督检查。

市国家安全局：负责互联网中国家安全事项管理工作，依法对互联网上危害国家信息安全的行为进行监督、查处；对涉及国家安全的网络与信息系统进行技术安全检查、安全评估和安全防护。

市政府新闻办：负责协调、指导、督促有关部门对网上出现的涉及意识形态方面的重大情况进行统一行动，做好应急情况下网上热点敏感问题处理和舆论引导工作。

市保密局：负责涉密信息系统的防范管理和对网上涉密信息的

检查，对涉嫌泄露国家秘密的行为依法进行查处。

市财政局：对网络与信息安全应急工作所需的相关经费（包括设备购置费、应急社会网络的服务费、网络信任体系建设等）给予充分保障。

市文化局：负责对上网服务营业场所经营单位实施经营管理技术措施，对网络游戏服务进行监督管理。

市广播电视局：负责对广播、电视及视听节目的网上传播进行监督管理。

市新闻出版局（版权局）：负责互联网出版的日常管理，依法对网络着作权进行监督管理。

市委610办：负责协调有关网上邪教问题的防范和处理及做好网上反邪教的社会宣传工作。

市教育局：负责对远程教育和校园网信息安全进行监督管理。

市工商行政管理局：负责互联网上网服务营业场所、网络服务上和经营性网站的企业登记管理。

各重要信息系统的应急协调工作由各主管部门负责。

各部门要按照职能分工，牵头制定和完善特定系统预案和各专项应急预案，明确各有关单位在应急工作中的任务和相互配合的工作流程。

3　预警和预防机制

3.1 信息监测及预警报告

公安、国家安全、信息产业等部门应加强网络与信息安全监测、分析和预警工作，建立网络与信息安全重大事故报告制度，发

生网络与信息安全突发事件的单位应当在事件发生后，对发生的事件进行调查核实、保存相关证据，并向应急领导小组办公室报告。应急领导小组办公室应建立和健全信息监测、指挥决策支持及预警发布系统，保证资源共享、运转正常、指挥有力。

3.2 预防机制

在全市范围内积极推行信息安全风险评估。银行、电力、民航、铁路、证券、海关、税务、保险等重要系统建设要充分考虑应急备份与灾难恢复，制定并不断完善网络安全应急处理预案。

4 应急响应启动条件

实施预警信息等级制度，按照事件严重性和紧急程度及对社会影响的大小，分为以下五级:

1级：本级网络与信息安全事件对计算机系统或网络系统所承载的业务以及事发单位利益基本不影响或损害极小;

2级：本级网络与信息安全事件对计算机系统或网络系统所承载的业务以及事发单位利益有一定的影响或破坏；对国家安全、社会秩序、经济建设和公共利益产生一定危害;

3级：本级网络与信息安全事件对计算机系统或网络系统所承载的业务、事发单位利益以及社会公共利益有较为严重的影响或破坏，对国家安全、社会秩序、经济建设和公共利益产生较大危害;

4级：本级网络与信息安全事件对计算机系统或网络系统所承载的业务、事发单位利益以及社会公共利益有极其严重的影响或破坏，对国家安全、社会秩序、经济建设和公共利益产生严重危害;

5级：本级网络与信息安全事件对计算机系统或网络系统所承载

的业务、事发单位利益以及社会公共利益有灾难性的影响或破坏，对国家安全、社会秩序、经济建设和公共利益产生特别严重的危害；

当发生3级和3级以上的网络与信息安全事件时，启动本预案。

特殊情况下，上述标准可酌情降低。

5 应急响应流程

5.1 预案启动

在发生三级以上网络与信息安全事件后，事件发生单位和现场应急处理工作组尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，以确定事件范围和评估事件带来的影响和损害，确认为网络与信息安全事件后，对事件进行定级和上报。由应急领导小组决定启动应急预案（应急响应流程如图1 所示）。并由应急领导小组办公室负责应急处理工作。

5.2 现场应急处理

1、确认阶段：确定应急处理方式

初步确定应急处理方式，如果以自身力量无法处理的事件，应提出应急支援请求，由应急领导小组办公室协调派出应急响应小组进行网络与信息安全应急支援。

（1）确定是否存在针对该事件的特定系统预案，如有，则启动相关预案；如果事件涉及多个专项预案，应同时启动所有涉及的专项预案。

（2）如果没有针对该事件的专项预案，应根据事件具体情况，采取抑制措施，抑制事件进一步扩散，并根除事件影响，恢复系统

运行。

2、遏制阶段：及时采取行动遏制事件发展

抑制事件的影响进一步扩大，限制潜在的损失与破坏，同时要确保封锁方法对涉及相关业务影响最小。

3、根除阶段：彻底解决问题隐患。

在事件被抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

4、恢复和跟踪阶段：

在确保安全问题解决后，要及时清理系统、恢复数据、程序、服务。恢复工作应避免出现误操作导致数据的丢失。另外，恢复工作中如果涉及到机密数据，需遵照机密系统的恢复要求。

5、对于银行、电力、通信等涉及国计民生的重点业务系统，发生问题后在采取技术措施解决的同时，还要加强宣传，公布危害性和解决办法，以避免产生社会恐慌。

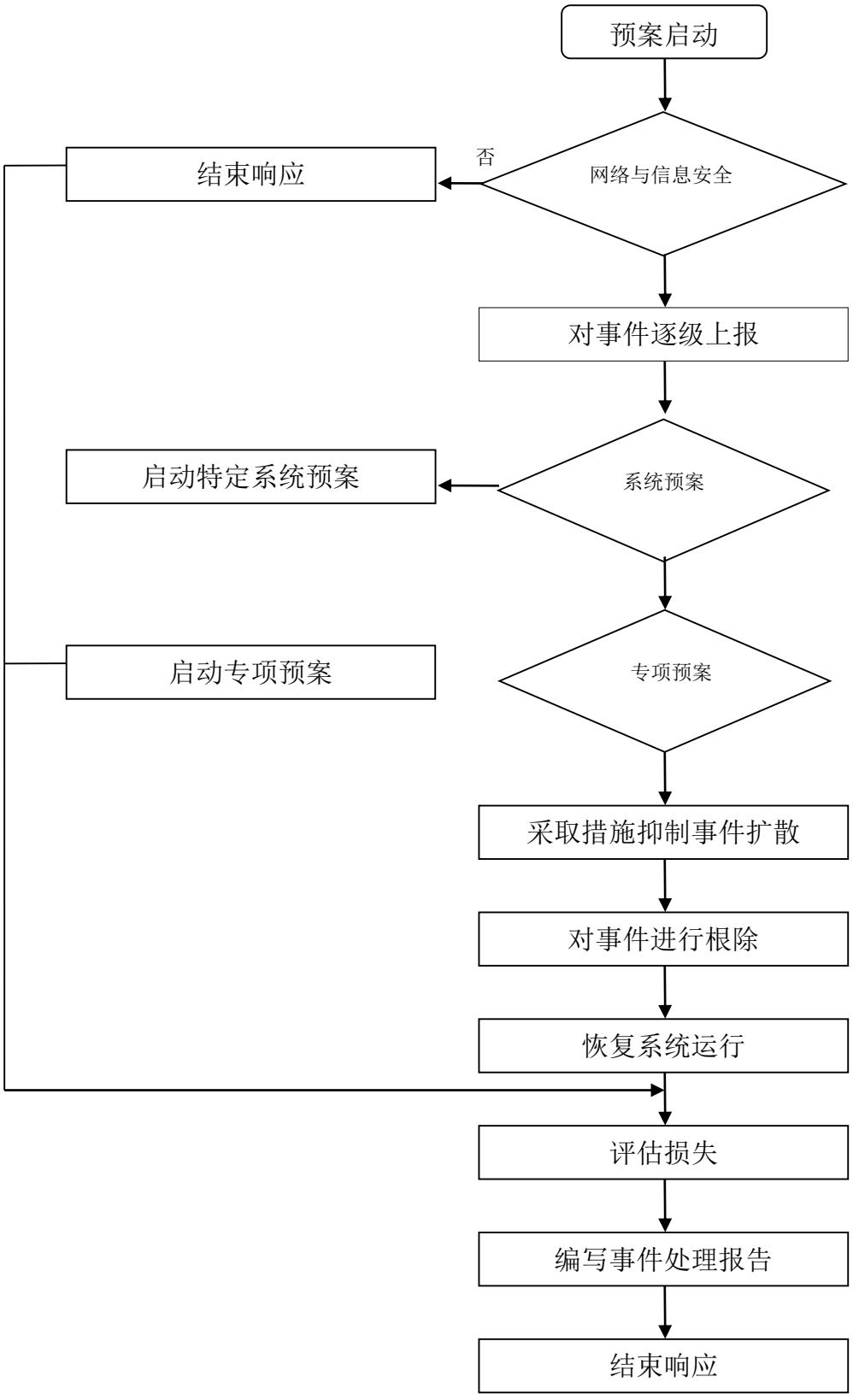

预案启动
网络与信息安全
否
结束响应
对事件逐级上报
系统预案
启动特定系统预案
专项预案
启动专项预案
采取措施抑制事件扩散
对事件进行根除
恢复系统运行
评估损失
编写事件处理报告
结束响应

图 1 应急响应流程

5.3　安全事件的处理记录

在事件的上报、接收和处理过程中，事件接收人、处理负责人应及时作好完整的过程记录。事件处理完成后归档。

5.4 结束响应

系统恢复运行后，应急响应小组对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料，上报相关部门。

对于蠕虫病毒等易造成大范围传播的网络与信息安全事件，应及时向应急领导小组办公室提交预警信息。

因为重大自然灾害而引起的网络与信息安全事件，可根据灾害造成的损失情况参照上述流程进行应对。

6　演练及维护

每年至少组织一次应急行动演练，以提高处理应急事件的能力，检验物资器材的完好情况。

应急响应演练按如下步骤进行:

1)由应急领导小组确定应急响应演练的目标和应急响应演练的范围;

2）按应急领导小组的要求，由应急领导小组办公室和应急响应小组共同制定应急响应演练的方案;

3) 应急领导小组办公室调配应急响应演练所需的各项资源，并协调应急响应演练过程中涉及的部门和单位;

4）应急领导小组办公室组织相关部门和单位进行应急响应演练;

5）应急领导小组对应急演练进行评估，并通报应急响应演练结果;

6）应急领导小组办公室总结经验，根据演练结果对应急预案进行更新，并对有关单位的应急工作进行整改。

应急响应演练结束之后，应急响应小组应针对应急响应工作过程中遇到的问题，分析应急预案的科学性和合理性，针对预案中的问题向应急领导小组办公室提出修改建议。应急领导小组办公室组织对修改意见进行评估，经应急领导小组同意后，发布实施。

在上级预案或相关的法律标准修改后，本预案应进行调整与其保持一致。调整后，应急领导小组办公室应组织专家组进行评审，评审通过后发布实施。

7　保障措施

7.1 应急队伍保障

由应急领导小组办公室组织有关企业、高校等，建立济南市网络与信息安全应急响应技术队伍（包括安全分析员、应急响应人员、灾难恢复人员等），并制定相应的人员培训和演练计划，提高应急响应技术队伍素质。根据工作需要，应急办公室可从有关单位抽调工作人员，各单位工作人员应服从协调和安排。成立应急专家顾问小组，为应急救援决策提供咨询和技术支持。

7.2 设备保障

为保证在发生网络与信息安全事件时应急工具及设备能够立即

投入使用，有效地支持应急响应工作，应急响应技术队伍应加强对应急工具及设备的维护调试，保证其随时处于可用状态。

另外，应急响应技术队伍还应注意跟踪最新的技术发展动态，收集、整理其他应急响应相关工具，包括文件完整性检测工具、木马/后门检测工具等等。对于病毒库、脆弱性评估系统插件库等应及时更新；根据工作需要，应急响应工作缺乏的设备或工具软件应及时采购。

7.3 技术资料保障

全面的技术资料是高效的应急响应工作的前提和基础，应急技术资料是网络和信息系统重要技术信息，包括网络拓扑结构、重要系统或设备的型号及配置（操作系统及版本号、应用软件及版本号等）、主要设备厂商信息等。各重要信息系统应将这些信息建立技术档案并及时更新，以保证与实际系统的一致性。各单位应根据需要对系统进行风险评估，随时掌握系统安全状况。

7.4 经费保障

在应急响应工作中，财政部门应对所需的相关经费给予充分保障。

7.5 后勤保障

在应急响应工作中，应急领导小组办公室应做好充分的后勤保障工作，包括应急人员的饮食，交通工具和通信联络，部门的安全保卫等等，确保应急响应工作的顺利开展。

主题词：互联网　网络　信息安全　预案　通知

抄送：市公安局，市国家安全局，市政府新闻办，市保密局，市财政局，市文化局，市广电局，市新闻出版局（版权局），市委610办公室，市教育局，市工商局。

济南市信息产业局　　2007年4月15日印发