《上海市网络与信息安全事件专项应急预案》

日前，市政府办公厅正式发布了《上海市网络与信息安全事件专项应急预案》，进一步明确了信息安全事件分类分级方法、应急工作组织体系、事件处置程序和对各重点单位的工作要求。预案由市网安办（市经济信息化委）负责编制、修订、解释和组织实施，现予公布实施。

上海市网络与信息安全事件专项应急预案

（2014 年修订版）

1　总则

1.1　编制目的

建立健全本市网络与信息安全事件应急工作机制，提高应对突发网络与信息安全事件能力，维护基础信息网络、重要信息系统和重要工业控制系统的安全，保障城市安全运行。

1.2　编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国计算机信息系统安全保护条例》、《国家网络与信息安全事件应急预案》、《国家通信保障应急预案》和《上海市实施<中华人民共和国突发事件应对法>办法》、《上海市突发公共事件总体应急预案》等，编制本预案。

1.3　事件分类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、工业控制系统攻击事件、设备设施故障和灾害性事件等。

（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、混合程序攻击事件、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）工业控制系统攻击事件是指对控制生产设备运行的网络、系统、数据进行攻击导致的工业控制系统运行故障。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络和信息系统故障。

1.4 事件分级

网络与信息安全事件分为四级：Ⅰ级（特大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）。

（1）符合下列情况之一的，为特别重大网络与信息安全事件（Ⅰ级）：

① 信息系统中断运行 2 小时以上、影响公共用户数 100 万人以上。

② 信息系统中的数据丢失或被窃取、篡改、假冒，对本市国家安全和社会稳定构成特别严重威胁，或导致 10 亿元以上的经济损失。

③ 其他对本市国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络与信息安全事件。

（2）符合下列情形之一且未达到特大网络与信息安全事件（Ⅰ级）的，为重大网络与信息安全事件（Ⅱ级）：

① 信息系统中断运行 30 分钟以上、影响公共用户数 10 万人以上。

② 信息系统中的数据丢失或被窃取、篡改、假冒，对本市国家安全和社会稳定构成严重威胁，或导致 1 亿元以上的经济损失。

③ 其他对本市国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络与信息安全事件。

（3）符合下列情形之一且未达到重大网络与信息安全事件（Ⅱ级）的，为较大网络与信息安全事件（Ⅲ级）：

① 信息系统中断运行造成较严重影响的。

② 信息系统中的数据丢失或被窃取、篡改、假冒，对本市国家安全和社会稳定构成较严重威胁，或导致 1000 万元以上的经济损失。

③ 其他对本市国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络与信息安全事件。

（4）除上述情形外，对本市国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络与信息安全事件，为一般网络与信息安全事件（Ⅳ级）。

1.5 适用范围

本预案适用于本市行政区域内发生的网络与信息安全事件，以及发生在其他地区且有可能影响上海城市安全运行的网络与信息安全事件的预防和处置工作。其中，有关基础电信网络的通信保障和通信恢复等应急处置工作，适用《上海市通信保障应急预案》。

1.6 工作原则

坚持统一指挥、密切协同、快速反应、科学处置；实行预防与处置相结合和“谁主管谁负责，谁运营谁负责，谁使用谁负责”等。

2 总体评估

随着加快智慧城市建设和城市信息化发展战略的持续推进，本市党政机关和涉及国计民生、城市日常运行等重点领域高度依赖网络与信息系统。但计算机病毒、黑客攻击等安全威胁突出，物联网、云计算等新应用带来新的安全风险，信息安全形势日趋严峻，对城市信息安全保障体系提出了更高要求。

3 组织体系

3.1 领导机构

3.1.1 《上海市突发公共事件总体应急预案》明确，本市突发事件应急管理工作由市委、市政府统一领导；市政府是本市突发事件应急管理工作的行政领导机构；市应急委决定和部署本市突发事件应急管理工作，其日常事务由市应急办负责。

3.1.2 市网络与信息安全协调小组（以下简称“市网安协调小组”）作为市级议事协调机构，主要负责综合协调本市网络与信息安全保障工作，对处置本市网络与信息安全事件实施统一指挥。

3.2 应急联动机构

市应急联动中心设在市公安局，作为本市突发事件应急联动先期处置的职能机构和指挥平台，履行应急联动处置较大和一般突发事件、组织联动单位对特大或重大突发事件进行先期处置等职责。各联动单位在其职责范围内，负责突发事件应急联动先期处置工作。

3.3 市应急处置指挥部

重大、特大网络与信息安全事件发生后，视情将市网安协调小组转为市网络与信息安全事件应急处置指挥部（以下简称“市应急处置指挥部”），统一指挥本市网络与信息安全事件处置工作。同时，根据情况需要，设置联络和处置等专业小组，在市应急处置指挥部的统一指挥下开展工作。

3.4 职能部门

设在市经济信息化委的市网安协调小组办公室（以下简称“市网安办”）承担市网安协调小组日常事务，综合协调本市网络与信息安全事件应急处置工作。

3.5 专家咨询机构

市网安办负责组建处置网络与信息安全事件专家咨询组，为处置网络与信息安全事件提供决策咨询建议和技术支持。

4　预防预警

4.1　预防

各区县和有关部门要做好网络与信息安全事件的风险评估和隐患排查工作，及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害。

4.2　预警分级

按照网络与信息安全事件的紧急程度、可能造成的危害和发展态势，本市网络与信息安全事件预警级别分为四级：Ⅰ级（特别严重）、Ⅱ级（严重）、Ⅲ级（较重）和Ⅳ级（一般），依次用红色、橙色、黄色和蓝色表示。

（1）Ⅰ级预警（红色）：指发现新的网络与信息安全威胁，可能影响本市所有网络和重要信息系统，并有扩散到全国的可能性。

（2）Ⅱ级预警（橙色）：指发现新的网络与信息安全威胁，可能影响本市基础运营网络或 2 个以上重要信息系统的全部业务，并有继续扩散的可能性。

（3）Ⅲ级预警（黄色）：指发现新的网络与信息安全威胁，可能影响本市 1-2 个基础运营网络或 1-2 个重要信息系统的全部业务，无扩散性。

（4）Ⅳ级预警（蓝色）：指发现新的网络与信息安全威胁，可能部分影响本市 1 个基础运营网络或影响 1-2 个重要信息系统的部分业务，无扩散性。

4.3　预警信息发布

市网安办根据危害性和紧急程度，适时在一定范围内，发布网络与信息安全事件预警信息。预警级别可视网络与信息安全事件的发展态势和处置进展情况作出调整。其中，Ⅰ级、Ⅱ级预警信息发布同时报市委总值班室、市政府总值班室。

4.4　预警响应

进入预警期后，有关地区和单位立即采取预防措施，检查可能受到影响的信息系统，做好相关安全漏洞的修复工作。及时掌握本地区、本单位网络与信息系统安全状况，并将最新情况及时报市网安办。市网络与信息安全应急管理事务中心根据事件性质，通知相关应急处置支持队伍处于应急待命状态，并保障所需的应急设备和网络资源处于随时可以调用状态。同时每小时向市网安办报告最新情况。

5　应急响应

5.1　信息报告

5.1.1 发生网络与信息安全事件的单位必须在半小时内口头、1 小时内书面报告市网安办值班室（设在市网络与信息安全应急管理事务中心，值班电话：021-22816787）、市应急联动中心和事发地区县政府。较大以上网络与信息安全事件或特殊情况，必须立即报告。

5.1.2 发生重大网络与信息安全事件，市网安办、市应急联动中心必须在接报后在 1 小时内口头、2 小时内书面同时报告市委总值班室、市政府总值班室；特大网络与信息安全事件或特殊情况必须立即报告。

5.2 响应等级

5.2.1 本市处置网络与信息安全事件应急响应等级分为四级：Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级，分别对应特大、重大、较大、一般网络与信息安全事件。事件的响应等级由市网安办组织实施。

5.2.2 发生Ⅳ级（一般）或Ⅲ级（较大）网络与信息安全事件，由市网安办和市应急联动中心决定响应等级并组织实施；发生Ⅱ级（重大）或Ⅰ级（特大）网络与信息安全事件，由市网安办和市应急联动中心提出处置建议，报市网安协调小组（或市应急处置指挥部）批准后组织实施。

5.3 应急处置

5.3.1 市网络与信息安全应急管理事务中心应在接报后，立即评估事件影响和可能波及的范围，研判事件发展态势，根据需要，组织各专业机构在职责范围内参与网络与信息安全事件的先期处置，并向市网安办报告现场动态信息。必要时，由市网安办牵头成立由市网络与信息安全应急管理事务中心、事发单位、主管机构负责人和相关信息安全专家组成的现场处置工作组，具体负责现场应急处置工作。

5.3.2 一般、较大网络与信息安全事件发生后，事发单位应在第一时间实施即时处置，控制事态发展。市网安办会同市应急联动中心组织协调相关部门、单位和专业机构以及事发地区县政府调度所需应急资源，协助事发单位开展应急处置。一旦事态仍不能得到有效控制，由市网安办报请市网安协调小组决定调整应急响应等级和范围，启动相应应急措施。必要时，由市网安协调小组统一指挥网络与信息安全事件的处置工作。

5.3.3 重大、特大网络与信息安全事件发生后，由市网安办会同市应急联动中心组织事发地区县政府和相关专业机构及单位联动实施先期处置。一旦事态仍不能得到有效控制，视情将市网安协调小组转为市应急处置指挥部，统一指挥、协调有关单位和部门实施应急处置。

5.4 技术实施

5.4.1 处置小组制订具体处置建议方案后，组织相关专业机构、事发单位和有关部门进行检验，检验结果上报市应急处置指挥部。

5.4.2 检验结果经评估后形成处置正式方案，经批准后由联络小组及有关部门按照方案要求，协调、落实所需的应急资源。

5.4.3 处置小组根据市应急指挥部下达的指令，实施应急处置。处置手段主要为：（1）封锁。对扩散性较强的网络与信息安全事件，立即切断其与网络的连接，保障整个系统的可用性，防止网络与信息安全事件扩散。

（2）缓解。采取有效措施，缓解网络与信息安全事件造成的影响，保障系统的正常运行，尽量降低网络与信息安全事件带来的损失。

（3）消除和恢复。根据事件处置效果，采取相应措施，消除事件影响；及时对系统进行检查，排除系统隐患，以免再次发生同类型事件，并恢复受侵害系统运行。

5.5 信息发布

5.5.1 一般或较大网络与信息安全事件信息发布工作，由市网安办负责。

5.5.2 重大或特大网络与信息安全事件信息发布工作，由市政府新闻办负责。

6 后期处置

网络与信息安全事件处置后，市网安办负责会同事发单位和相关部门对网络与信息安全事件的起因、性质、影响、损失、责任和经验教训等进行调查和评估。

7 应急保障

有关部门和重点单位要按照职责分工和相关要求，切实做好应对网络与信息安全事件的物资、通信和经费等保障工作，保证应急处置和救援工作的顺利进行。

7.1 物资保障

各相关部门、专业机构、重点单位要根据实际需要，做好网络与信息系统设备储备工作，并将储备物资清单报市网安办备案。

7.2 通信保障

市经济信息化委、市通信管理局、市文广影视局、市无线电管理局等部门要建立有线和无线相结合、基础电信网络与机动通信系统相配套的应急通信系统，确保应急处置时通信畅通。

7.3 经费保障

依照市政府有关处置应急情况的财政保障规定执行。

8　预案管理

8.1　预案解释

本预案由市网安办（市经济信息化委）负责解释。

8.2　预案修订

市网安办（市经济信息化委）根据实际情况变化，适时评估修订本预案。

8.3　预案实施

本预案由市网安办（市经济信息化委）组织实施。

各重点单位根据本预案，制定具体的工作方案并报市网安办备案。

本预案自印发之日起实施。