急　件

中国人民银行上海分行文件

上海银发〔2011〕249号

关于建立上海市金融业信息安全协调机制的通知

各国有商业银行、股份制商业银行上海（市）分行，交通银行，上海浦东发展银行，上海银行，上海农村商业银行，中国外汇交易中心，中国银联，上海黄金交易所，上海清算所，工商银行上海数据中心，农业银行数据中心，中国银行信息中心（上海），建设银行上海数据中心，兴业银行数据中心：

根据《中国人民银行办公厅关于加快辖区信息安全协调机制建立的通知》（银办发[2011]191号）要求，为促进上海市金融业信息安全管理工作的开展，提高上海市金融业信息安全管理工作水平，我行通过与上海市网络信息安全协调小组办公室、上海市相关职能部门及金融机构积极的沟通协调，决定建立上海市金融业信息安全协调机制。现将相关事项通知如下：

一、成立上海市金融业信息系统应急保障小组，下设协调指挥组、协调工作组和协调联络组，并纳入上海市网络与信息安全应急保障体系。保障小组成员为人民银行上海分行和相关金融机

构，保障小组组织机构见附件1，保障小组名单见附件2。为加强金融机构应急管理的沟通与交流，人民银行上海分行建立了应急管理信息交流平台，保障小组各成员单位应在2011年底前完成接入该平台的工作。

二、建立上海市金融业信息安全联席会议制度，研究上海市金融业信息安全保障工作的方针和策略，制定上海市金融业信息安全相关制度和预案，通报金融业信息安全工作动态。联席会议成员单位为人民银行上海分行和相关金融机构，并邀请上海市相关职能部门参加。联席会议每年举办两次，参会人员为保障小组各成员单位的工作小组人员。

三、编制《上海市金融业（银行业）信息安全协调工作预案》（附件3）。该预案由人民银行上海分行起草，征求了上海市网络与信息安全协调小组办公室、相关金融机构、上海市相关职能部门的意见，并经上海市金融业信息系统应急管理工作协调会议审议并最终定稿。现将该预案正式印发各单位，请各单位认真组织学习，并抓紧做好本单位预案的衔接工作。

特此通知。

附件：1. 金融业信息系统应急保障小组组织机构

2. 金融业信息系统应急保障小组名单

3. 上海市金融业（银行业）信息安全协调工作预案（试行）

二〇一一年十一月二十三日

附件一：

上海市金融业信息系统应急保障小组组织机构

为建立健全上海市金融业信息系统应急保障工作机制，提高应急协调工作效率，加强金融机构应急管理的沟通与交流，决定成立金融业信息系统应急保障小组。保障小组下设协调指挥组、协调工作组和协调联络组，具体职责和成员如下：

一、金融业信息系统应急保障协调指挥组

金融业信息系统应急保障协调指挥组职责包括：

1、组织指挥上海市金融业信息系统应急管理工作；

2、审定上海市金融业信息系统应急处置对策；

3、审定上海市金融业信息安全协调工作预案；

4、审定上海市金融业信息系统应急处置工作报告；

金融业信息系统应急保障协调指挥组组长：人民银行上海总部金融服务二部信息系统应急管理主管领导。

金融业信息系统应急保障协调指挥组成员：各金融机构信息安全和应急管理主管领导。

二、金融业信息系统应急保障小组办公室

保障小组在人民银行上海总部金融服务二部设办公室，办公室职责：

1、负责上海市金融业信息系统应急保障日常工作协调；

2、组织金融业信息系统应急处置工作的办公、文件运转及档案管理；

3、紧急情况下协助协调指挥组召集各成员成立应急指挥部，

做好应急指挥、沟通协调、资源调配以及应急处置工作；

4、收集、反馈金融业信息系统应急处置的相关信息以支持协调指挥组决策；

5、向各成员单位通报、发布金融业信息系统预警和评估等相关信息。

金融业信息系统应急保障小组办公室负责人：人民银行上海总部金融服务二部科技部门信息系统应急管理主管负责人。

三、金融业信息系统应急保障协调工作组

金融业信息系统应急保障协调工作组职责包括：

1、协助协调指挥组组织、协调各项处置工作的实施，维持处置工作正常开展；

2、上海市金融业信息安全协调工作预案的编制和修改；

3、上海市金融业信息系统预警、评估和响应；

4、组织实施上海市金融业信息系统应急处置相关的新闻息工作；

5、向协调指挥组提交上海市金融业信息系统应急处置工作报告；

6、协调指挥组指定的其他工作。

金融业信息系统应急保障协调工作组组长：人民银行上海总部金融服务二部科技部门信息系统应急管理主管负责人。

金融业信息系统应急保障协调工作组成员：各金融机构信息安全和应急管理部门负责人。

四、金融业信息系统应急保障协调联络组

金融业信息系统应急保障协调联络组职责包括：

1、协助协调工作组完成应急联络、协调各项处置工作，维持

处置工作正常开展；

2、协助协调工作组做好日常信息报送、接收、传递等工作；

各单位应指定一名应急联络员，负责信息系统应急保障联络和日常信息的收发。

上海金融业（银行业）信息安全协调工作预案

（试行）

中国人民银行上海分行

目录

1 总则

1.1 编制目的

为建立健全上海市金融业网络与信息安全事件专项应急工作机制，提高应对突发网络与信息安全事件能力，保障基础信息网络和重要信息系统的安全运行，维护金融安全和社会稳定，促进上海国际金融中心建设和发展，结合上海市金融业网络与信息安全管理工作实际情况，编制本预案。

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》、《国家突发公共事件总体应急预案》、《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》、《信息安全事件分类分级指南》(GB/Z20986—2007)、《上海市网络与信息安全事件专项应急预案》（沪府办〔2009〕70号）和《中国人民银行关于进一步加强银行业金融机构信息安全保障工作的指导意见》等法律、法规和相关规定。

1.3 事件分类

上海市金融业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、设备设施故障和灾难性事件等。

（一）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。

（二）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。

（三）信息数据破坏事件分为信息数据篡改事件、信息数据假冒事件、信息数据泄露事件、信息数据窃取事件、信息数据丢失事件和其他信息数据破坏事件。

（四）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。

（五）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

上海市金融业网络与信息安全事件分为四级：Ⅰ级（特别重大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）。

（一）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）事件造成金融机构全国范围内服务中断 2 小时以上或数省范围内服务中断 4 小时以上的。

（2）事件造成信息系统中的数据丢失或被窃取、篡改、假冒，影响的用户数超过 100000，或导致 1000 万元人民币以上的经济损失。

（3）其他对社会秩序、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。

（二）符合下列情形之一且未达到特别重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）事件造成金融机构全国范围内服务中断 30 分钟以上 2 小时以下、数省范围内服务中断 2 小时以上 4 小时以下或一省范围内服务中断 4 小时以上的。

（2）事件造成信息系统中的数据丢失或被窃取、篡改、假冒，影响的用户数超过 50000 不足 100000，或导致 500 万元人民币以上 1000 万元人民币以下的经济损失。

（3）其他对社会秩序、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。

（三）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）事件造成金融机构数省范围内服务中断 30 分钟以上 2 小时以下或一省范围内服务中断 2 小时以上的。

（2）事件造成信息系统中的数据丢失或被窃取、篡改、假冒，影响的用户数超过20000不足50000，或导致200万元人民币以上500万元人民币以下的经济损失。

（3）其他对社会秩序、经济建设和公众利益构成较大威胁、造成较大影响的网络与信息安全事件。

（四）除上述情形外，对金融业网络与信息系统运行构成一定威胁、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

本方案适用于在沪的人民银行直属单位、全国性商业银行总行（数据中心）、各商业银行上海（市）分行等相关单位在发生网络与信息安全事件时的应急协调工作。

1.6 工作原则

坚持统一指挥、密切协同、快速反应、科学处置；坚持预防与处置相结合，以预防为主；坚持“谁主管谁负责、谁运营谁负责、谁使用谁负责”，充分发挥各方面力量，共同做好网络与信息安全事件的预防和处置工作。

2 组织体系

2.1 领导机构

《上海市突发公共事件总体应急预案》明确，上海市突发公共事件应急管理工作由市委、市政府统一领导；市政府是本市突发公共事件应急管理工作的行政领导机构，具体负责部门为市应急办公室。上海市金融业信息安全应急管理工作由中国人民银行上海分行和上海市网络与信息安全协调小组共同领导。

2.2 应急联动机构

金融业信息安全应急联动机构设在人民银行上海分行，作为金融业信息安全事件应急联动先期处置的职能机构和指挥平台。在上海市网络与信息安全事件专项应急预案体系内，通过市网络与信息安全协调小组办公室和市应急办公室对接。

2.3 工作机构

2.3.1 中国人民银行上海分行

中国人民银行上海分行（以下简称“人民银行”），负责在沪人民银行直属单位、全国性商业银行总行等机构的（数据中心）、各商业银行上海（市）分行的应急管理工作，负责发布上海市金融业（银行业）信息安全协调工作预案、维护上海市金融业信息系统应急协调通讯网，中国人民银行上海总部金融服务二部为具

体实施部门。

2.3.2 市网安办

指导上海市金融业相关单位做好信息安全应急管理工作，及时通报应急管理和预警信息，根据上海市金融业应急处置过程中的需求，协调相关职能部门参与应急处置工作。

2.3.3 金融机构

本预案金融机构是指：在沪的人民银行直属单位、全国性商业银行总行（数据中心）、各商业银行上海（市）分行。

负责本单位信息系统监测预警和信息安全事件先期处置，同时向人民银行报告信息安全事件相关情况，提交需要本市相关部门协助解决的应急处置要求，及时反馈应急处置相关情况和处置结果，并向人民银行及时通报和更新本单位应急协调联络名单。

2.3.4 本市相关职能部门

根据与金融机构达成的应急工作预案及提出的应急处置需求，积极参与应急处置工作，并向主管部门和相关金融机构反馈处置结果。

2.4 专家机构

组建金融业网络与信息安全事件处置专家组，并与其他相关专家机构建立联络机制，为应急处置工作提供决策建议和技术指导，必要时参与网络与信息安全事件的应急处置。

3 预防预警

3.1 预防措施

各金融机构应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。

3.2 监测预警

3.2.1 预警分级

按照网络与信息安全事件可能对金融业信息系统安全造成的危害、紧急程度和发展态势，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。

（一）Ⅰ级预警（红色）。指发现新的网络与信息安全威胁，可能影响金融机构所有网络和重要信息系统，并有扩散到全国范围的可能性。

（二）II级预警（橙色）。指发现新的网络与信息安全威胁，可能影响金融机构基础运营网络或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。

（三）III级预警（黄色）：指发现新的网络与信息安全威胁，可能影响金融机构部分基础运营网络或1-2个重要信息系统的全部业务，无扩散性。

（四）IV级预警（蓝色）：指发现新的网络与信息安全威胁，可能部分影响金融机构小部分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。

3.2.2 安全监测

人民银行负责指导和协调上海市金融业监测预警体系建设。

人民银行会同本市相关部门整合各方网络与信息安全监测资源，建立健全应对网络与信息安全事件的信息监测、预警机制，建立全时段、全覆盖的网络与信息安全事件监测预警系统，提高金融业信息系统的监测预警能力。

各金融机构负责本单位网络与信息安全监测预警工作。重要的网络与信息安全监测预警信息要及时报告人民银行。

人民银行汇总上报信息后，定期将有关情况通报金融机构和本市相关部门。

各金融机构应及时汇总监测预警信息，并评估风险等级，编制预警信息，报人民银行。预警信息包括网络与信息安全事件的

类别、预警级别、起始时间、可能影响的范围、警示事项、应采取的措施和发布范围等。

3.3 预警信息发布

人民银行根据网络与信息安全事件的管理权限、危害性和紧急程度，统一发布、调整和解除预警信息。Ⅰ级、Ⅱ级预警信息同时上报市网安办。

3.4 预警响应

金融机构根据预警信息及时做好应急处置准备工作。

3.4.1 Ⅰ、Ⅱ级预警响应

（一）相关金融机构处于应急待命状态;

（二）人民银行根据预警信息协调组织应急处置支持队伍，并协调市网安办组织应急保障支持;

（三）金融机构要针对预警信息采取预防措施，立即检查本单位可能受到影响的信息系统，做好相关安全漏洞的修复工作，并加强网络与信息系统安全状况的监测，及时将最新情况上报人民银行;

（四）相关金融机构每小时向人民银行报告一次预警信息。

3.4.2 Ⅲ级预警响应

（一）相关金融机构要针对预警信息采取预防措施，立即检查本单位可能受到影响的信息系统，做好相关安全漏洞的修复工作，并加强网络与信息系统安全状况的监测；

（二）人民银行根据预警信息协调组织应急处置支持队伍，并协调市网安办组织应急保障支持；

（三）相关金融机构每四小时向人民银行报告一次预警信息。

3.4.3 IV 级预警响应

相关金融机构要针对预警信息采取预防措施，立即检查本单位可能受到影响的信息系统，做好相关安全漏洞的修复工作，并加强网络与信息系统安全状况的监测；

3.5 预警解除

人民银行根据金融机构上报情况，确定是否解除预警，并组织发布。I 级、II 级预警的解除同时报市网安办。

4 应急处置

4.1 信息安全事件报告和处理

4.1.1 信息安全事件信息

金融机构有义务向人民银行报告网络与信息安全事件及其隐患。信息来源主要有以下三类:

（一）监测预警系统发现的网络与信息安全事件信息;

（二）上级机构或相关部门通报的网络与信息安全事件信息;

（三）接到来自社会和各网络与信息安全责任单位的报告信息。

4.1.2 信息安全事件报告

（一）发生 III 级以上网络与信息安全事件，事发单位必须在半小时内向人民银行口头报告，在 1 小时内填写《信息安全事件事发报告表》（附件 3）向人民银行书面报告；较大以上网络与信息安全事件或特殊情况，立即报告。

（二）一旦网络与信息安全事件影响超出金融机构范围，应根据应急处置工作的需要，由人民银行组织应急处置工作，同时由人民银行报请市网安办协助处置。

4.1.3 信息安全事件处理

（一）记录与了解。接到网络与信息安全事件报警后，要详细记录该事件的有关信息，了解事件造成的损失、影响以及现场控制情况，并尽可能全面了解与事件相关的信息。

（二）事件确认与判断。在汇总相关信息的基础上，及时研判事件性质，并根据判定结果，开展下一步工作。

（1）属于网络与信息安全事件的，应参考数据库对该次事件做进一步的事件验证，确认属于网络与信息安全事件的，应进入事件分析流程。

（2）属于误报的，值班人员应对该事件进行记录和处理。

（3）对于与网络与信息安全无关的事件，值班人员也应做好记录，并将事件转交相关主管机构处理。

（三）事件分析。事件确认后，根据掌握的信息，分析事件已经造成的损失并预计损失、事件的严重程度和扩散性等情况。

（四）准备启动应急处置规程。金融机构根据事件分析的结果，按照网络与信息安全事件等级标准拟定事件等级报人民银行，并做好启动相应应急预案处置规程的准备。

4.2 先期处置

（一） 网络与信息安全事件发生后，事发单位必须按职责和规定权限启动相关工作预案和应急处置规程，在第一时间实施即时处置，控制事态发展并及时向人民银行报告。

（二）人民银行应在接到事件报告后，应及时掌握事件的发展情况，评估事件的影响和可能波及的范围，研判事件的发展态势，协调和指导金融机构积极开展前期处置工作，同时根据需要协调市网安办或组织其他专业作机构在各自职责范围内参与网络与信息安全事件的先期处置。

（三） 金融机构负责本单位网络与信息安全事件实施先期处置。

4.3 应急响应

4.3.1 响应等级

根据网络与信息安全事件的可控性、严重程度和影响范围，应急响应级别分为四级：Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级，分别对应特别重大、重大、较大和一般网络与信息安全事件。

4.3.2 分级响应

（一）Ⅰ、Ⅱ级应急响应。发生重大或特别重大信息安全事件，金融机构应立即启动本单位相应应急处置预案，必要时成立应急处置指挥部，统一指挥、协调相关单位或部门实施应急处置，同时应立即向人民银行报告事件情况，并持续报告事件处置情况。人民银行接报后及时掌握事件发展情况，必要时应组织专家机构指导和参与金融机构应急处置工作，同时人民银行应及时协

调市网安办，根据事件发展情况由网安办协调相关职能部门参与应急处置工作。

（二）III级响应。发生较大信息安全事件，金融机构应启动本单位相应应急处置预案，同时应向人民银行报告事件情况，并持续报告事件处置情况。

（三）IV 级响应。发生一般信息安全事件，金融机构应启动本单位相应应急处置预案，事件处置结束后向人民银行报告事件相关情况。

4.4 应急指挥与协调

4.4.1 启动应急响应

一旦发生先期处置仍不能控制的网络与信息安全事件，人民银行、金融机构应及时研判事件等级并上报市网安办，必要时成立应急处置指挥部，下设联络小组和处置小组；

（一）联络小组由市网安办、人民银行、事发金融机构和其他参与处置单位抽调人员组成。主要负责应急处置指挥部的具体事务，传达指令，通报处置情况，协调各参与处置单位的处置工作。

（二）处置小组由人民银行、事发金融机构和其他参与处置单位抽调人员组成。处置小组主要负责制定现场处置方案，执行指挥部的指令，记录现场处置情况。根据处置的需要，可以召集消防、电力、通信等基础营运企业人员参与处置小组。

4.4.2 响应程序

应急响应工作程序如下:

（一）应急资源调配

（1）应急人员协调。金融机构根据事件具体情况，自行组织协调信息安全专家、网络专家、信息系统专家等各类应急响应技术人员，若人员不足可由人民银行协调和组织专家机构成员参与应急处置工作。

（2）相关权限。人民银行和金融机构负责协调和明确参与处置的机构或人员在应急响应过程中的相关权限。

（3）其他必要资源。金融机构根据应急数据库中的信息获取处置事件所必需的资源，如网络与通讯资源、计算机设备、网络设备、网络安全设备与软件、处置案例、解决方案等，为处置小组提供参考。

（二）处置方案选择

处置小组负责根据事件的具体情况选择预先制定的处置方案，处置方案应经过风险评估和可行性检验，处置小组可根据现场情况对处置方案进行适当的调整和修改。

（三）处置决策与资源调度

应急处置方案应报现场指挥部，经确认后实施，参与应急处置的部门按处置方案的要求，协调、落实所需的应急资源。

（四）实施处置

处置小组根据指挥部下达的指令，按照职责和操作权限建立运行机制，实施应急处置。处置手段主要为：

（1）封锁。对于扩散性较强的网络与信息安全事件，立即采取措施，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的扩散。

（2）缓解。采取措施，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。分析网络与信息安全事件的特点，采取措施消除事件。

（4）追踪。对于黑客入侵、DOS 攻击等人为破坏，需要根据现场情况进行取证，采取一定的技术手段追踪对方信息，取证后提交给公安机关处理。

（5）恢复。消除事件之后，对系统进行检查，彻底消除系统的安全隐患，以免再次发生同类型网络与信息安全事件；然后使受侵害系统恢复上线运行，处置方案实施完毕。

（五）处置结果检验

网络与信息安全事件处置方案实施完毕后，处置小组要对处置结果进行检验，并采取以下相应措施：

（1）若故障消除，保存相关证据和处置方案等资料。

（2）若故障缓解，继续跟踪其状态变化，并对后续解决方案提供建议。

（3）若处理失败，封锁事件范围，保持跟踪，注明原因并立即向现场指挥报告，请求支援，并提升响应级别。

（六）处置结果报告。事件危害消除、缓解或现场得到控制后，及时将处置情况报告人民银行。

4.5 应急结束

（一）对于重大和特别重大的网络与信息安全事件，在应急处置工作结束，或者相关危险因素消除后，金融机构应及时报人民银行，经人民银行确认并宣布应急状态结束后，终止实施应急措施，转入常态管理。

（二）对于一般和较大的网络与信息安全事件，应急结束的判断标准为信息系统和业务恢复正常，由该事件衍生的其他事件已经消失，安全隐患已经消除，由金融机构宣布应急状态的结束，转入常态管理。

5 后期处置

5.1 善后处置

市网安办、人民银行、事发金融机构和其他相关单位要积极稳妥、深入细致地搞好善后处置。对参与处置的工作人员，以及紧急调集、征用有关单位、个人的物资，要给予补助或补偿。

5.2 调查和评估

人民银行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、责任、经验教训和恢复重建等问题进行调查和评估，调查评估情况要通报相关单位。

（一）责任确定。应急处置工作结束后，应当分析产生该次事件的原因，对事件进行调查，确定责任人。如涉及违法犯罪行为，由司法机关及时追究当事人的刑事责任。

（二）事件备案和归档。应急处置工作结束后，金融机构应将事件处置的过程和结果在人民银行备案。

（三）预案维护。应急处置工作结束后，需根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改。

5.3 恢复重建

恢复重建工作按照“谁主管谁负责，谁运营谁负责、谁使用谁负责”的原则，由事发单位负责。事发单位和相关职能部门在对可利用的资源进行评估后，制订重建和恢复生产的计划，迅速采取各种有效措施，恢复网络与信息系统的正常运行。

5.4 信息发布

（一） 对于已经发生的重大和特别重大事件的相关信息，由人民银行汇总相关信息后通报给重点单位；一般和较大事件的相关信息，采用简报形式，发到各有关单位。

（二） 对于造成社会影响的网络与信息安全事件，信息发布应当及时、准确、客观、全面。事件发生后，要及时向社会发布信息，并根据事件处置情况做好后续发布工作。需要向社会发布的信息，经市网安办和人民银行核定后，由市网安办协调相关部门具体组织发布。

6 应急保障

金融机构要按照职责分工和相关预案，切实做好应对网络与信息安全事件的人员、经费、物资、通讯、科技等保障工作，保证应急救援和恢复重建工作的顺利进行。

6.1 应急队伍保障

（一）各金融机构应根据本单位实际情况，配备相应的网络信息安全应急力量或引进必要的社会化应急服务。

（二）各金融机构负责组建本单位网络与信息安全事件应急响应专业队伍，培养骨干力量。

（三）人民银行应做好应急响应专家机构的维护工作，加强联系，发生安全事件时根据情况需要组织相应人员参与应急处置工作。

（四）市网安办应加强与相关职能部门的联络与协调，确保发生安全事件时能快速及时的联络相关部门参与应急处置工作。

6.2 经费保障

（一）各金融机构负责落实本单位网络与信息安全事件应急管理工作经费。

（二）各级财政和审计部门要对网络与信息安全事件应急经费的使用进行监管和评估。

6.3 物资保障

各金融机构应根据自己的实际需要做好网络信息系统设备储备工作。

6.4 通信保障

人民银行、金融机构以及本市相关部门，应建立有效的应急联络通信机制，固定电话和移动电话相结合，确保通信畅通。

6.5 科技支撑

（一）各金融机构要积极开展网络与信息安全领域的科学研究，加大网络与信息安全事件预测、预警、预控、预防和应急处置技术研发的投入力度，不断改进技术装备和手段，建立健全网络与信息安全应急技术支撑平台，提高网络与信息安全科技水平。

（二）人民银行、、金融机构应当建立应急处置管理、应急预案管理、应急演练环境、灾难备份等数据系统，为网络与信息安全事件的处置提供科技支撑。

7 监督管理

7.1 宣传教育

各金融机构应当加强应急管理宣传，普及应急知识、强化应急意识、提高应急水平。

7.2 培训

各金融机构应当定期开展应急管理培训，对领导干部、管理人员进行培训，并对应急管理和基层处置人员进行相应的技能培训。

7.3 演练

各金融机构每年组织相关预案的演练，模拟处置影响较大的网络与信息安全事件，组织相关部门和人员参加，提高实战能力，检验和完善预案。

7.4 责任和奖惩

（一） 网络与信息安全事件应急处置工作实行行政领导负责制和责任追究制。

（二） 对在应急处置工作中做出突出贡献的先进集体和个人，给予表彰和奖励。对迟报、谎报、瞒报、漏报网络与信息安全事件重要情况或者应急处置工作中有其他失职、渎职行为的，依法给予有关责任人行政处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案制定

本预案由人民银行上海分行负责编制和解释。

上海市各金融机构要结合本预案制定或修订本单位网络与信息安全工作预案，做好预案之间的衔接，并报人民银行上海分行备案。

8.2 预案修订

人民银行上海分行根据实际情况的变化，及时修订本预案。

8.3 预案实施

本预案由人民银行上海分行负责组织实施。

本预案自印发之日起施行。

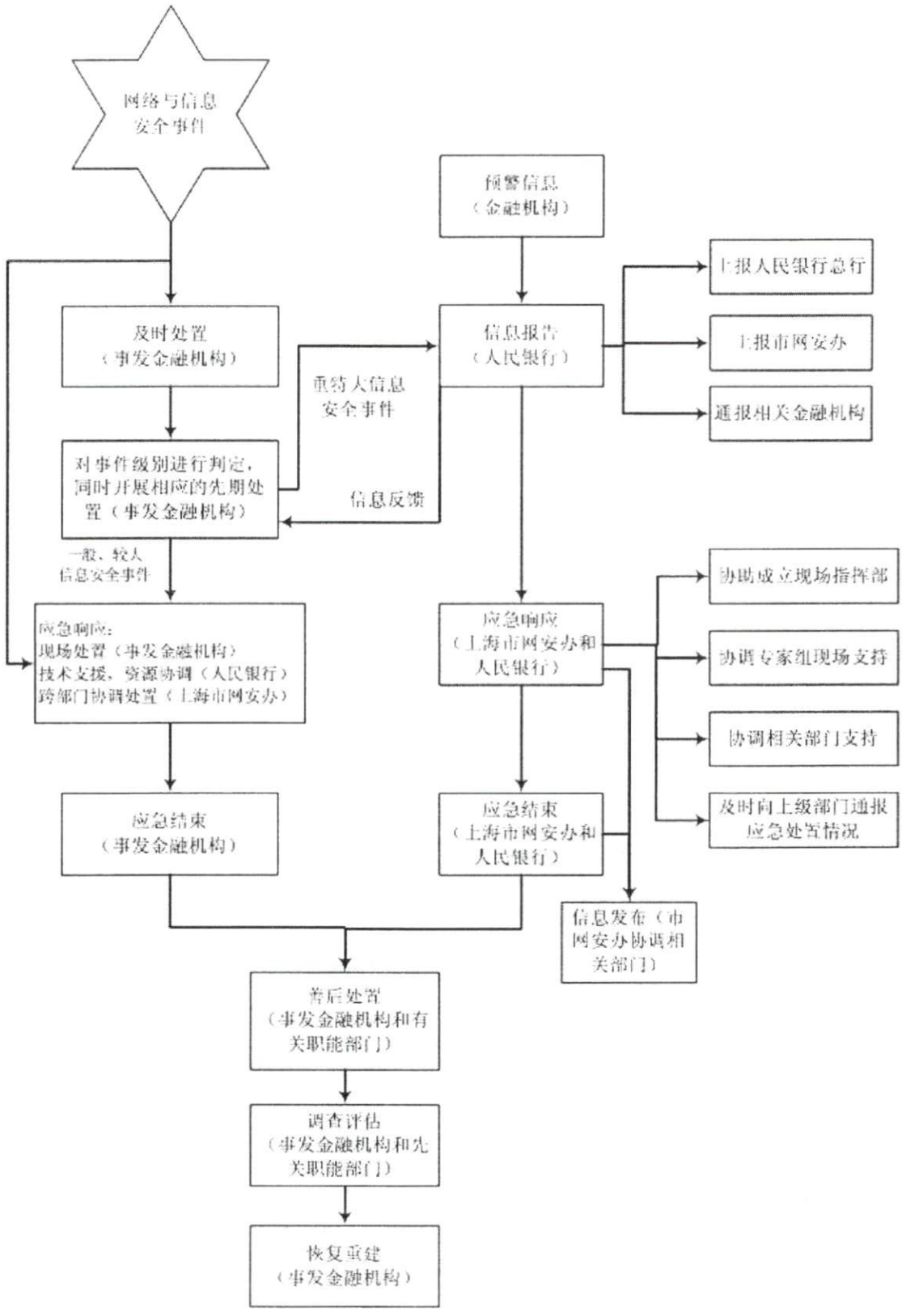
9 附录

（一）上海市金融业网络与信息安全事件应急管理工作流程图（见附件 1）

（二）网络与信息安全事件记录调查表（见附件 2）

（三）信息安全事件事发报告表（见附件 3）

附件 1：上海市金融业网络与信息安全事件应急管理工作流程图



附件 2：网络与信息安全事件记录调查表

事件报告单位			
事件来源		发生时间	
安全事件现象描述（包括事件发生现象、发生位置、影响范围等）			
已经造成的损失和预计损失			
已采取的措施			
记录人		记录时间	

附件 3：信息安全事件事发报告表

事发单位	
事发时间	*年/月/日/时/分*
事发地点	*机房名*
事件概述	*事件发现方式及现象描述*
事件影响系统名称	
影响业务及数据情况	*事件影响业务、数据等情况概述*
影响地域情况	*事件影响地域及机构情况概述（内部、外部机构）*
初步采取的措施	
报告人姓名	
报告人所在部门	
报告时间	*年/月/日/时/分*
联系方式	