中国人民银行上海分行文件

上海银发〔2011〕53号

关于印发《上海市银行业金融机构信息安全报告制度》的通知

各政策性银行、国有商业银行、股份制商业银行、中国邮政储蓄银行上海（市）分行，上海银行、上海农村商业银行，其他城市商业银行上海分行，上海市各外资银行：

根据《中国人民银行关于进一步做好银行业金融机构重大事项报告有关工作的通知》（银发[2011]23号）要求，为及时了解上海市银行业金融机构发生的重大信息安全事件，全面掌握上海市银行业金融机构信息安全状况，防范信息安全风险，切实维护金融稳定，我分行参照《银行计算机安全事件报告管理制度》（银发[2002]280号印发）和《中国人民银行计算机系统信息安全报告制度》（银发[2010]366号印发），制定了《上海市银行业金融机构信息安全报告制度》，现印发你行。请认真组织学习，并严格执行，切实做好信息安全事件报告工作。

特此通知。

附件：《上海市银行业金融机构信息安全报告制度》

二〇一一年三月七日

附件：

上海市银行业金融机构信息安全报告制度

一、总　则

第一条 根据《中国人民银行关于进一步做好银行业金融机构重大事项报告有关工作的通知》（银发〔2011〕23号）文件精神，参照《银行计算机安全事件报告管理制度》（银发〔2002〕280号印发）和《中国人民银行计算机系统信息安全报告制度》（银发〔2010〕366号印发），为加强上海市银行业金融机构计算机系统信息安全（以下简称信息安全）管理，规范计算机系统信息安全报告流程，提高信息安全事件和风险处置效率，制定本制度。

第二条 本制度适用于各政策性银行、国有商业银行、股份制商业银行上海（市）分行，中国邮政储蓄银行上海分行、上海银行、上海农村商业银行，其他城市商业银行上海分行，上海市各外资银行及其他相关单位。

第三条 本制度报告范畴界定为网络与信息系统计算机系统的信息安全，报告事项包括信息安全事件和信息安全风险两类。

第四条 本制度所称信息安全事件，是指由于人为、自然因素或计算机软硬件缺陷等原因，导致网络、信息系统出现异常或数据受到侵害，影响网络与信息系统正常运行或数据安全。

第五条 本制度所称信息安全风险，是指人为、自然的威胁利用网络与信息系统及其管理机制中存在的脆弱性，导致信息安全事

件发生的可能性。

第六条 任何单位和个人均有信息安全报告的义务。按照“谁发现、谁报告”的原则，信息安全事件发生或风险发现单位的计算机系统相关业务部门在向本单位应急办报告的同时，通报本单位科技部门。各单位科技部门按照本单位规定向上级单位科技部门报告的同时，应按本制度规定向人民银行上海分行报告。

第七条 信息安全报告应及时，不得迟报、谎报、瞒报、漏报，报告内容应客观准确，报告格式应符合本制度要求。

二、信息安全事件报告

第八条 根据计算机信息系统的重要性及其遭受损害的程度、范围和造成数据泄漏、丢失、破坏等产生的影响不同，信息安全事件分为特别重大（I 级）信息安全事件、重大（II 级）信息安全事件、较大（III 级）信息安全事件和一般（IV 级）信息安全事件。当信息安全事件满足多个级别定级条件时，按最高级别确定事件等级（具体分级见附件 1）。

第九条 事发单位应依据信息安全事件影响时间、范围和持续时间等因素的变化情况，按照附件 1 的定义进行事件级别的调整。事件等级的最终认定，由相关业务部门会同科技部门在事后综合评估后认定。

第十条 人民银行上海分行负责上海市银行业各级别信息安全事件的接报工作，各单位的上海分行负责本行在上海市各分支机构的各级别信息安全事件的接报工作。

第十一条 一般情况下，信息安全事件报告实行逐级上报，发

生或可能引发重大（II 级事件）及以上事件等紧急情况下，事发单位在向上一级报告的同时，应向人民银行上海分行报告。

第十二条　各单位应按照规定的信息安全事件报告流程（附件 2），在事发、事中与事后三个阶段分别报告。如遇地震、台风和雪灾等重大自然灾害，事发单位可采取各种可行的联系方式，及时报告。对电话方式报告的事件，接报单位应做好电话记录，留存电话记录单（附件 3）。

第十三条　事件发生时，事发单位应立即报告，报告方式包括电话、传真等（如遇紧急情况，可通过短信等方式预报告）。事发报告要素参见附件 4。

第十四条　在事件处置过程中，事发单位应及时报告事件处置进展情况，报告方式包括电话或传真，事中报告要素见附件 5。

（一）本单位或所辖机构发生较大（III 级）信息安全事件后，相关单位应在 4 小时内向人民银行上海分行提交事中报告，并及时更新报告。

（二）本单位或所辖机构发生重大（II 级）或特别重大（I 级）信息安全事件后，相关单位应在 2 小时内向人民银行上海分行提交事中报告，每 3 小时上报一次事件处置进展情况，直至事件处置结束，或按照人民银行上海分行要求的频度持续报告。

第十五条　人民银行上海分行应设立固定值守电话（或手机），并确保通讯联络的有效、畅通。

第十六条　事件处置结束后，事发单位应认真总结事件处置的经验教训，以正式文件形式提交详细的事件总结报告（报告模板见附件 6）。

（一）本单位或所辖机构发生较大（III 级）信息安全事件后，相关单位应在事件处置完毕后 8 个工作日内向人民银行上海分行提交事件总结报告。

（二）本单位或所辖机构发生重大（II 级）或特别重大（I 级）信息安全事件后，相关单位应在事件处置完毕后 5 个工作日内向人民银行上海分行提交事件总结报告。

第十七条　各单位应确保事件报告联络的有效、畅通，保证报告信息的客观性，保证报告信息不外泄。各单位应依据事件级别，启动相应的应急预案，迅速进行应急处置，快速恢复业务。

三、信息安全风险报告

第十八条　本制度将信息安全风险分为重大与一般两级，重大信息安全风险是指可能对国家经济、金融安全、公众利益和人民银行履行职能造成严重影响和损害的风险。

第十九条　各单位应采取管理与技术措施，加强信息系统脆弱性及其面临威胁的监测、评估，及时发现、报告、预警和处置信息安全风险。

第二十条　人民银行上海分行负责上海市银行业重大信息安全风险的接报工作，各单位的上海分行负责本行在上海市各分支机构的各级别信息安全风险的接报工作。

第二十一条　各单位应及时向人民银行上海分行报告所辖机构或本单位的重大信息安全风险（格式见附件 7）；完成风险整改后，应以正式文件形式提交风险整改报告，整改报告内容应包括风险情况、产生原因、采取的整改措施、整改后验证情况等。

四、考核与责任

第二十二条　人民银行上海分行将信息安全报告制度执行情况纳入上海市银行业科技工作竞赛评比。各单位可将制度执行情况纳入年度科技专业考核，对表现突出单位、部门或个人，应予表扬或奖励。

第二十三条　各单位应按照本制度的要求修改和完善本单位的信息安全报告制度，并做好相关组织落实工作。

第二十四条　本制度实行责任追究制，对于执行不力的单位、部门或个人，将给予通报批评；造成重大影响或严重后果的，将依据有关规定追究相关责任人及其领导的责任。

五、附　则

第二十五条　人民银行上海分行信息安全接报通信方式见附件8。

第二十六条　本制度由人民银行上海分行负责解释和修订。

第二十七条　各单位之前发布的其他信息安全报告制度有关条款如与本制度不一致，按本制度执行。

第二十八条　本制度自印布之日起执行。

附件 1

信息安全事件分级

一、信息系统分类

根据银行业信息系统的业务特点、服务对象等，可分为如下几类：

A、基础支撑类系统：主要指为各类信息系统提供基础支撑服务的系统，如机房设施、网络系统、存储系统、共享平台等。

B、联机事务处理系统：主要指具有联机处理特点的业务系统，用于提供金融服务或信息服务，此类业务系统对数据的实时性处理要求很高，服务范围广。

C、管理信息类系统：主要指用于非联机类业务处理及提供重要内部办公支撑的信息系统，此类业务系统对数据的实时处理要求不高。

D、决策分析类系统：主要是指通过采集数据，进行数据加工，对加工结果进行统计、分析、展现，以供决策分析的信息系统，此类信息系统对数据实时性处理要求不高，但在报数期内要求高。

E、其他类系统：是指为实现银行内部管理信息化，便于用户方便快捷的共享信息及协同工作的信息系统。

人民银行上海分行部分信息系统分类表

分类	系统名称	系统分类	备注
A	机房系统	基础支撑类系统	
	存储系统	基础支撑类系统	
	金融业网间互联平台		
B	大额实时支付系统	支付清算类	
	小额批量支付系统	支付清算类	
	境内外币支付系统	支付清算类	
	全国支票影像交换系统	支付清算类	
	电子商业银行汇票系统	支付清算类	
	支付综合业务系统	支付清算类	
	人民币银行结算账户管理系统	支付清算类	
	联网核查公民身份信息系统	综合业务类	
	财政综合业务处理系统	国库类	
	货币发行信息系统	货币金银类	
	数据安全交换平台（SMEP）	数据传输类	
C	支付信息管理系统	支付清算类	
	国库综合业务报表系统	国库类	
	国债报表管理系统	国库类	
	国债兑付业务管理系统	国库类	
	国库现金招投标信息管理系统	国库类	
	金融业机构信息管理系统	综合业务系统	
D	金融统计监测信息系统	综合业务系统	
	调统先行指标时间序列分析数据库	综合业务系统	
	统计数据库查询系统	综合业务系统	
	调统文件上报系统	综合业务系统	
	理财与资金信托数据报送系统	综合业务系统	
E	大屏幕系统	办公系统	
	触摸屏系统	办公系统	
	防病毒系统	其他系统	
	入侵检测系统	其他系统	
	非法外联系统	其他系统	

注：

1. 应用系统的重要程度按照业务优先于办公、对外服务优先于内部管理、实时处理系统高于非实时处理系统、大范围影响高于小范围影响等原则划分。

2. IT 基础设施的重要性取决于所支撑信息系统的重要性。

二、信息安全事件分级

类型	事件系统类型	信息安全事件级别			
		一般（Ⅳ级）事件	较大（Ⅲ级）事件	重大（Ⅱ级）事件	特别（Ⅰ级）重大事件
系统运行安全类	A 类	一个省（自治区、直辖市）无法提供服务达 30 分钟以内的信息安全事件。	一个省（自治区、直辖市）无法提供服务开展达 30 分钟（含）以上、2 个小时以内的信息安全事件 或全国无法提供服务达 30 分钟以内的信息安全事件。	一个省（自治区、直辖市）无法提供服务达 2 个小时（含）以上、4 个小时以内 或全国无法提供服务达 30 分钟（含）以上、2 个小时以内的信息安全事件。	一个省（自治区、直辖市）无法提供服务达 4 个小时（含）以上 或全国无法提供服务达 2 个小时（含）以上的信息安全事件。
	B 类	一个省（自治区、直辖市）业务无法正常开展达 30 分钟以内的信息安全事件。	一个省（自治区、直辖市）业务无法正常开展达 30 分钟（含）以上、2 个小时以内 或全国业务无法正常开展达 30 分钟以内的信息安全事件。	一个省（自治区、直辖市）业务无法正常开展达 2 个小时（含）以上、4 个小时以内 或全国业务无法正常开展达 30 分钟（含）以上、2 个小时以内的信息安全事件。	一个省（自治区、直辖市）业务无法正常开展达 4 个小时（含）以上 或全国业务无法正常开展达 2 个小时（含）以上的信息安全事件。
	C 类	一个省（自治区、直辖市）中断服务达 60 分钟以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 60 分钟（含）以上、3 个小时以内的信息安全事件 或全国中断服务达 40 分钟以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 3 个小时（含）以上、5 个小时以内 或全国中断服务达 40 分钟（含）以上、3 个小时以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 5 个小时（含）以上 或全国中断服务达 3 个小时（含）以上的信息安全事件。
	D 类	一个省（自治区、直辖市）中断服务达 60 分钟以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 60 分钟（含）以上、4 个小时以内的信息安全事件 或全国中断服务达 60 分钟以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 4 个小时（含）以上、6 个小时以内 或全国中断服务达 60 分钟（含）以上、4 个小时以内的信息安全事件。	一个省（自治区、直辖市）中断服务达 6 个小时（含）以上 或全国中断服务达 4 个小时（含）以上的信息安全事件。

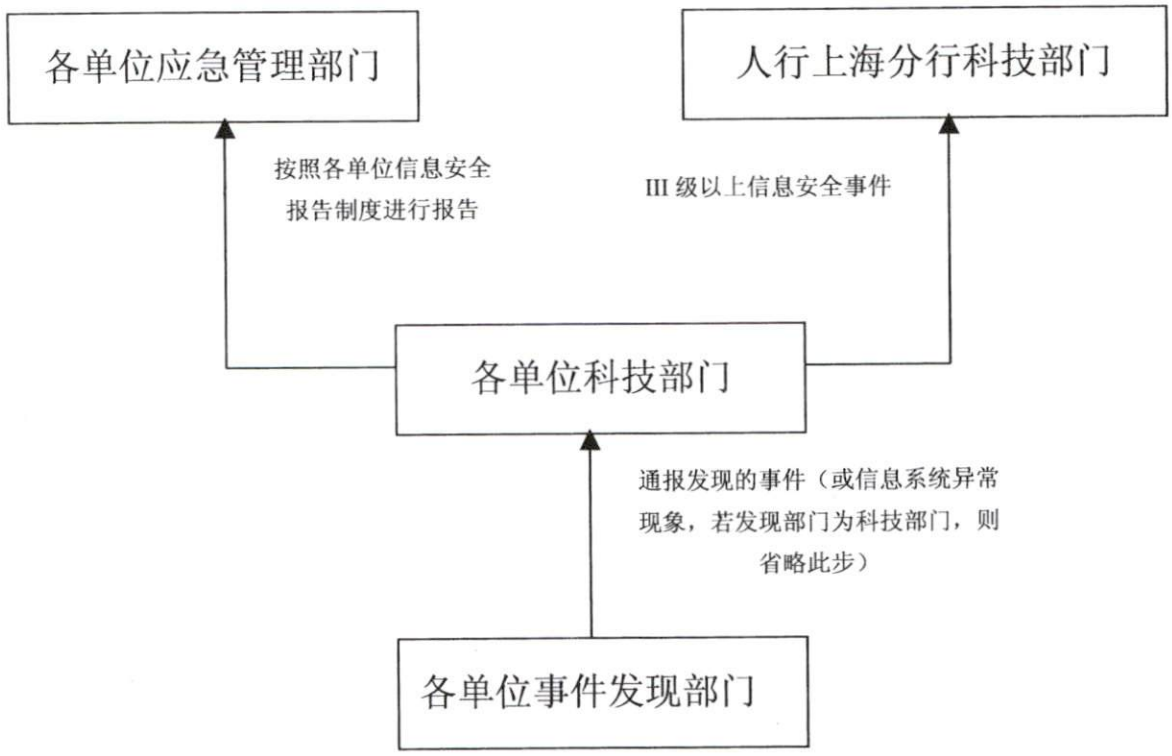
	E类	一个省（自治区、直辖市）中断服务达6小时以内的信息安全事件。	一个省（自治区、直辖市）中断服务达6小时（含）以上的信息安全事件 或全国中断服务达 4 小时以上的信息安全事件。		
数据安全类		信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、金融稳定、公众利益和机构自身造成一般影响的信息安全事件。	信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、金融稳定、公众利益和机构自身造成较大影响的信息安全事件。	信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、金融稳定、公众利益和机构自身造成重大影响的信息安全事件。	信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、金融稳定、公众利益和机构自身造成特别重大影响的信息安全事件。
其他		其他对国家安全、金融稳定、公众利益和机构自身造成一般影响的信息安全事件。	其他对国家安全、金融稳定、公众利益和机构自身造成较大影响的信息安全事件。	其他对国家安全、金融稳定、公众利益和机构自身造成重大影响的信息安全事件。	其他对国家安全、金融稳定、公众利益和机构自身造成特别重大影响的信息安全事件。

注：

表中时间是指连续时间，为影响提供业务或信息服务的时间。对于E类系统，除数据安全类及其他情况外，系统运行安全事件仅限一般和较大两级。

附件 2

信息安全事件报告流程图



注：

1. 本图所示为上海市银行业金融机构信息安全事件的报告和接报流程。
2. 本图所指“事件”为计算机系统信息安全事件。

附件 3

信息安全事件报告电话记录单

<table>
<tr><td>时　间</td><td colspan="5">年　　月　　日　　时　　分</td></tr>
<tr><td>来电单位</td><td></td><td>电话号码</td><td></td><td>发话人</td><td></td></tr>
<tr><td>来电主题</td><td colspan="3"></td><td>受话人</td><td></td></tr>
<tr><td colspan="6">电话内容（按照“信息安全事件事发或事中报告要素”记录）：

电话记录人签名：</td></tr>
<tr><td>备　注</td><td colspan="5"></td></tr>
</table>

附件 4

信息安全事件事发报告要素

事件名称	
事件级别	□一般　□较大　□重大　□特别重大
事发单位	
事发部门	
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*
事件系统名称	
事件系统类别	□A　□B　□C　□D　□E
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	
报告时事件状态	
报告人姓名	
报告人所在单位及部门	
报告时间	*年/月/日/时/分*
联系方式	

附件 5

信息安全事件事中报告单

事件名称	*事件名称应与事发要素中事件名称一致*
报告次数	事中第_____次报告
事件级别	□一般　□较大　□重大　□特别重大
事件状态	
影响业务及数据情况的变化	*事件影响业务、数据等情况的变化*
影响地域情况的变化	*事件影响地域及机构情况（内部、外部机构）的变化*
事件处置措施及处置进展情况	
下一步拟采取的措施	
需总行协调处置事项	
报告部门联系方式	

附件 6

信息安全事件总结报告模板

一、事件基本情况

详述事件的起始时间、发生地点、发现方式、现象、持续时间、处置措施及恢复过程等。

二、事件影响

（一）影响概述。

概述事件对国家、社会、机构自身造成的影响。

（二）影响详述。

1. 影响范围。

详述影响地域及内外部机构的个数、名称。

2. 影响的系统。

详述系统的名称、功能、硬件（事件涉及的设备类别<网络/服务器/存储/外设>、设备品牌、设备型号）、软件（事件涉及的操作系统，数据库，存储，中间件，应用程序的名称、版本号、补丁号）、部署结构图、冗余情况（HA/N+1/数据备份/应用备份/其他）等。

3. 影响的业务。

4. 影响的数据。

5. 其他影响。

三、事件损失评估

（一）资金损失。

（二）数据损失。

（三）其他损失。

四、事件根源详细分析

（一）技术方面。

（二）管理方面。

五、事件责任认定

六、事件处置经验与教训

（一）事件处置经验。

（二）事件处置教训。

七、改进措施

附表：事后报告单

事件名称	*与事发、事中报告要素中事件名称一致*
事件等级	□较大　□重大　□特别重大
事件分类	□有害程序事件 子类：○计算机病毒事件　○蠕虫事件　○特洛伊木马事件　○僵尸网络事件　○混合攻击程序事件　○网页内嵌恶意代码事件　○其他有害程序事件____*（填写具体内容）* □网络攻击事件 子类：○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　○其他网络攻击事件____*（填写具体内容）* □信息破坏事件 子类：○信息篡改事件　○信息假冒事件　○信息泄漏事件　○信息窃取事件　○信息丢失事件　○其他信息破坏事件____*（填写具体内容）* □信息内容安全事件 子类：○违反法律法规的信息安全事件　○针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件　○组织串联、煽动集会游行的信息安全事件　○其他信息内容安全事件____*（填写具体内容）* □设备设施故障 子类：○软硬件自身故障　○外围保障设施故障　○人为破坏事故　○其他设备设施故障____*（填写具体内容）* □灾害性事事件 □其他事件____（不能归为以上 6 个基本分类的信息安全事件）*（填写具体内容）*

事件发现途径	□用户反映 □巡检 □监控 □报警 □日志分析 □检查 □其他____*（填写具体内容）*
事件系统名称	
事件系统功能	*填写主要业务功能*
事件区域	□外联区 □接入区 □交换区 □工作区 □生产区 □安全管理区 □测试区 □互联网应用区 □其他区_____*（填写具体内容）*
事件部位	□网络通信服务 □APP 服务 □DB 服务 □存储服务 □备份服务 □供配电 □空调 □机房 □管理控制服务 □其他_____*（请填写具体内容）*
事件层次	□数据层（业务数据/用户数据/系统配置数据） □应用层（接口/WEB） □服务层（中间件/数据库/共享服务平台） □操作系统层（内存/磁盘/ I/0 设备/外设/进程调度） □硬件层（网络/服务器硬件及其固化程序）
事件组件	□外部接入控制（网络接入/接口程序/接口设备） □用户访问控制（登录界面/用户管理/权限管理/用户视图/报表展现） □应用逻辑执行（例程/管理） □应用逻辑驱动（存取/显示） □数据库控制（查询/操作） □日志审计 □其他____*（填写具体内容）*
事件源定位	□设计（架构/系统/组件） □实现（开发/集成/测试） □运维（业务变更/技术变更） □灾备（传输/复制） □其他___*（填写具体内容）*
事件根本原因	□机房基础设施故障 □通信基础设施故障 □硬件故障 □软件故障 □应用程序缺陷 □业务逻辑缺陷 □资源不足 □网络攻击 □有害程序 □不可抗力 □误操作 □其他___*（填写具体内容）*
报告部门联系人	
报告部门联系方式	

附件 7

重大信息安全风险报告单

风险描述	
风险发生单位及部门	
风险发现途径	□ 用户反映 □巡检 □监控报警 □日志分析 □检查 □ 评估
风险发现时间	*年/月/日/时/分*
风险发现地点	*机房名*
风险系统名称	
风险系统类别	□A □B □C □D □E
风险系统功能	*填写系统主要业务功能*
风险系统硬件	*填写风险涉及的设备类别（网络/服务器/存储/外设）、设备品牌、设备型号*
风险系统软件	*填写风险涉及的操作系统、数据库、存储、中间件、应用程序的名称、开发商、版本号、补丁号*
风险层次	□数据层（业务数据/用户数据/系统配置数据） □应用层（接口/WEB） □服务层（中间件/数据库/共享服务平台） □操作系统层（内存/磁盘/I/0 设备/外设/进程调度） □硬件层（网络/服务器硬件及其固化程序）
风险分析	*从资产、脆弱性、威胁、威胁利用资产的脆弱性导致安全事件的可能性，安全事件发生后可能造成的影响方面详尽描述*
风险产生原因	□设计缺陷（结构/程序） □实现缺陷（集成配置） □维护缺陷（业务与技术变更） □设备缺陷（设计/部件/补丁） □用户误操作 □其他___（*填写具体内容*）
风险危害	*风险可能危害的业务（包括关联业务）及范围（影响地域及内外部机构）情况*
风险控制措施	*已采取措施及拟采取措施*
需总行协调处置事项	
报告部门联系人	
报告部门联系方式	