**xxx银行**

信息科技应急预案

第一章 总 则

第一条 为预防或最大程度地减少信息科技突发事件给xxx银行（以下简称“本行”）带来的经济损失，提高本行信息科技水平和应急处理能力，防范信息科技风险，根据《中华人民共和国计算机信息系统安全保护条例》、《国家信息化领导小组关于加强网络与信息安全保障工作的意见》以及省联社、银监部门的要求，并结合《xxx银行计算机信息系统应急处置管理办法》，特制定本预案。

第二条 信息科技突发事件应急预案是针对本行科技信息系统运行期间可能出现的故障而建立的快速反应机制，确保系统出现故障后迅速恢复。

第三条 本预案所指的网络与信息安全突发事件，是指重要网络与信息系统突然遭受不可预知外力的破坏、毁损、故障，发生对社会、公众造成或者可能造成重大损失的紧急事件。

第二章 突发事件分类和分级

第四条 根据网络与信息安全突发公共事件的发生过程、性质和特征，网络安全突发事件是指自然灾害、事故灾难和人为破坏引起的网络与信息系统的损坏。具体的分类为：

（一）自然灾害是指地震、台风、雷电、火灾、洪水等。

（二）事故灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

（三）人为破坏是指人为破坏网络线路、通信设施、黑客攻击、病毒攻击、恐怖袭击等事件。

第五条 根据信息科技突发事件的可控性、严重程度和影响范围，将信息科技突发事件分为四级：

一级：最严重的级别。具有以下两个重要标志：一是全局性，二是特别紧急性。全局性指涉及到辖内所有网点或者大多数网点，全部或者大多数交易不正常且短时间内难以恢复。特别紧急性是指可能影响到人身安全或资金安全的情况。

二级：较严重的级别。涉及部分主要设备、部分网点、所有网点的部分交易，以及虽然严重但短时间内能够处理的情况。同时还包括网点工作正常但主要设备出现严重问题的情况。

三级：一般性的技术故障。部分网点的部分交易、个别网点的故障错误以及软、硬件的非严重性问题。

四级：轻微的技术故障。个别的、非主要设备或者个别的数据、程序错误。

信息科技突发事件分级对照表具体如下：

**信息科技突发事件分级对照表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 级别 | 主机系统 | 网络系统 | 软件系统 | 基础设施 |
|  |  |  |  |  |
| 一级：最 | 1.虚拟化服务器损 | 1.两条主干网 | 1.系统升级出 | 1.精密空调故 |
| 坏 | 通讯均中断 | 现错误，全部 | 障、电力中断 |
| 严重的级 |
| 2.磁盘阵列损坏 | 2.主备交换机 | 网点无法办理 | 2.两台 UPS 均 |
| 别 |
| 3.光纤交换机损坏 | 均损坏 | 业务 | 损坏、电力中 |
|  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 4.应用服务器损坏 | 3.主备路由器 | 2. | 中间业务无 | 断 |
|  |  | 均损坏 | 法办理 | | 3.水、火等原 |
|  |  | 4.到yy分中 | 3. | 数据仓库损 | 因需要切断电 |
|  |  | 心网络中断 | 坏 |  | 源 |
|  |  |  |  |  |  |
|  | 1. 虚拟化服务器单 | 1.技术支持电 | 1. | 系统升级错 | 1.精密空调电 |
|  | 台损坏 | 误但可完全恢 | | 力中断 |
|  | 话中断 |
| 二级：较 | 2.磁盘阵列两块及 | 复 |  | 2.UPS 损坏但 |
| 2.主备设备单 |  |
| 严重的级 | 以上硬盘损坏 | 2. | 个别网点系 | 电力未中断 |
| 台损坏 |
| 别 | 3.光纤交换机告警 | 统损坏可恢复 | | 3.发电机损坏 |
| 3.主备线路单 |
|  | 4.应用服务器硬件 | 3. | 个别网点中 | 4.消防系统故 |
|  | 线路损坏 |
|  | 告警 | 间业务中断 | | 障 |
|  |  |
|  |  |  |  |  |  |
|  |  |  |  |  | 1.中心机房出 |
|  | 1.虚拟服务器控制 | 1.内部网络中 | 1. | 个别网点可 | 现水漫溢 |
|  | 台告警 | 2.门禁系统故 |
|  | 断 | 办理核心业务 | |
|  | 2.磁盘阵列个别硬 | 障，无法正常 |
|  | 2.楼层交换机 | 但部分业务无 | |
| 三级：一 | 盘有坏道 | 进入机房 |
| 故障 | 法办理 | |
| 般性的技 | 3.DB2、INFOMAX 等 | 3.监控系统故 |
| 3.内、外部网 | 2. | 省联社系统 |
| 术故障 | 进程失效 | 障 |
| 站损坏 | 升级故障但短 | |
|  | 4.应用服务器故障 | 4.消防系统误 |
|  | 4.OA 办公系统 | 时间内可恢复 | |
|  | 导致非生产期间重 | 告警 |
|  | 损坏 |  |  |
|  | 启系统 |  |  | 5.电力中断但 |
|  |  |  |  |
|  |  |  |  |  | 发电机正常 |
|  |  |  |  |  |  |
|  |  |  | 1. | 个别网点无 | 1.楼层停电但 |
| 四级：轻 | 1.数据备份失败 | 1.内、外部网 | 法签退 | | 机房供电正常 |
| 站故障 | 2. | 个别网点操 | 2.办公区电力 |
| 微的技术 | 2.系统日志有错误 |
| 2.OA 办公系统 | 作出错 | | 中断 |
| 故障 | 或警告信息 |
| 故障 | 3. | 个别网点帐 | 3.UPS 一般性 |
|  |  |
|  |  |  | 务处理出错 | | 告警 |
|  |  |  |  |  |  |

第三章 组织架构体系及其职责

第六条 建立应急处置团队，在发生灾难时，能够做到及时实施专项应急处置工作。应急处置团队包括应急处置领导小组、执行小组和保障小组。

（一）应急处置领导小组

领导小组成员：由组长、若干人员组成，组长由分管科技的副行长担任，成员由信息科技部、行政办公室、计划财务部、运营管理部、信贷管理部、授信管理部、合规管理部、风险管理部、审计部、安全保卫部等部门负责人组成。

领导小组工作职责：

1.制订应急管理制度，统一组织、协调、指导、检查本行信息系统突发事件应急管理工作。

2.负责信息系统突发事件的应急指挥、组织协调和过程控制。

3.审核并批准应急恢复预案的测试方案和应急演练方案。

4.组织对应急演练预案结果进行评审。

5.负责及时向董事会及高级管理层汇报本行信息系统应急及备份状况分析、应急恢复预案的实施情况以及应急演练的结果。

6.灾难发生后，对应急恢复执行小组提交的解决方案及应急备份预警评估报告进行评估并发出灾难宣告。

7.组织协调有关工作，并与银监部门、人民银行、其他金融机构就信息系统突发事件的处置进行信息交流和沟通。

8．做好秩序维护、安全、咨询和后勤保障等工作，与电力、通讯、公安和消防等相关外部机构建立应急协调机制和应急联动机制。

9.及时向省联社、yy银监分局汇报处置进程及应急处置的相关工作。

10.负责其他信息系统应急备份及恢复的管理。

（二）应急处置执行小组

执行小组成员：由组长、若干人员组成，组长由分管信息科技的副行长担任，成员由信息科技部、行政办公室、计划财务部、运营管理部、审计部、安全保卫部等机关各部室负责人及信息科技部、外包服务公司技术人员组成。

执行小组工作职责：

1.信息系统应急恢复的需求分析。

2.结合本行信息系统应急备份管理实际情况，制定、修改各信息系统应急子预案。

3.应急备份系统运行维护、技术支持、检查、变更等。

4.应急恢复预案的培训和应急。

5.应急备份系统灾难预警、评估、汇报和解决方案的制定。

6.灾难发生后信息系统和业务功能的恢复。

7.灾难发生后风险评估报告的撰写。

8.灾难发生后的外部协作。

9.信息系统应急恢复的实施。

（三）应急处置支持保障小组

支持保障小组成员：由组长、若干人员组成，组长由分管信息科技的副行长担任，成员由行政办公室、计划财务部、合规管理部、人力资源部、安全保卫部等机关各部室负责人组成。

支持保障小组工作职责：

1.信息系统应急保障的需求分析。

2.结合本行信息系统应急备份管理实际情况，负责联系涉及基础保障方面的第三方机构。

3.参与应急恢复预案的培训和应急演练。

4.参与应急备份系统灾难预警、评估、汇报和解决方案的制定。

5.参与灾难发生后信息系统和业务功能的恢复。

6.参与灾难发生后风险评估报告的撰写。

第四章 预防和预警机制

第七条 相关部门人员要熟练掌握本部门的业务范围、软硬件故障检查、修复技能，每季度进行一次应急演练。

第八条 信息科技部负责对每次安装的程序进行详细记录，对配置、参数调整前后的数据进行详细登记，对于配置、参数调整出现的问题须及时恢复。

第九条 信息科技部负责对全部软件的安装介质、说明文档妥善保管，对系统每次更新、安装新程序之后要及时做好备份工作，同时妥善保管备份介质。

第十条 信息科技部每日记录系统运行情况，在业务高峰期随时监控主机运行状况（如内存、交换空间、页面调度等），发现异常情况，及时向部门领导及分管行长反映和建议。

第十一条 信息科技部负责备份全部网络设备的配置参数，对配置、参数调整前后的数据进行详细登记，对于配置、参数调整出现的问题须及时恢复。

第十二条 信息科技部在调整参数配置、调整网络配置、安装程序时，应充分考虑到备份机的安装、调整，并在安装、调整日志上进行记载。

第十三条 信息科技部在软件安装前应进行充分测试，每季度对数据库、日志等备份数据进行恢复测试。

第十四条 信息科技部负责严格执行业务数据备份管理办法，保证业务数据备份的完整性、可靠性。

第五章 应急程序和技术保障措施

第十五条 突发事件发生时，涉事部门和相关人员在领导小组组长组织下启动预案自救，同时上报领导小组，情况特别严重的，将有关情况上报上级管理部门和当地政府。

第十六条 应急处置团队对突发事件应急处置做好组织、协调工作，帮助各营业网点恢复正常营业秩序，并做好正面宣传报道工作。

第十七条 信息科技部应确保系统的计算机设备及网络系统有足够的软硬件技术保证，有关重要信息有完整备份。

第十八条 核心账务数据应实现异地备份，建立数据备份中心。

第十九条 加强应急处置人员的队伍建设,确保在任何情况下，都不会因人员的缺岗而影响整个系统的正常运行。

第二十条 保持和系统集成商、软件供应商、硬件供应商的紧密联系，确保其在突发事件后能在第一时间内能提供技术支持或赶赴现场。

第六章 责任追究及处罚

第二十一条 突发事件处置结束后，总行组织有关部门人员对事件的原因及全过程进行调查，根据对有关人员的责任调查结果，视情节轻重程度，追究相关人员的责任。可分别采取经济处罚、行政处分乃至移送司法机关处理等处罚措施。

第二十二条 小组成员未按照相关规定履行相关职责的，依法给予行政处分；构成犯罪的，移交司法机关、依法追究刑事责任。

第二十三条 对突发事件应急管理工作中作出突出贡献的成员，应予以表彰和奖励。

第七章 附 则

第二十四条 本预案由xxx银行信息科技部负责解释和修订。

第二十五条 本预案和《xxx银行计算机信息系统应急处置管理办法》互为补充，如与应急处置管理办法相冲突，以应急处置管理办法为准。

第二十六条 信息科技部制订计算机网络系统应急预案、外包服务管理应急预案、基础设施应急预案、业务系统应急预案、主机系统应急预案等相关子预案，作为对本预案的补充和细化。

第二十七条 本预案自发文之日起施行。

附件：1.小组成员联系方式统计表

2.xxx银行应急预案--基础设施

3.xxx银行应急预案--外包服务

4.xxx银行应急预案--网络通讯

5.xxx银行应急预案--业务系统

6.xxx银行应急预案--主机系统

***附件 1***

小组成员联系方式统计表

|  |  |  |  |
| --- | --- | --- | --- |
| 组内职务 | 姓名 | 职务 | 联系方式 |
|  |  |  |  |
|  | **应急处置领导小组** | |  |
|  |  |  |  |
| 组长 | 韩阳 | 信息科技分管行长 | 13615165869 |
|  |  |  |  |
| 成员 | 王劲松 | 信息科技部总经理 | 13805110370 |
|  |  |  |  |
|  | 吴海兵 | 行政办公室总经理 | 13813235598 |
|  |  |  |  |
|  | 陈爱忠 | 计划财务部总经理 | 15189297140 |
|  |  |  |  |
|  | 吴斌 | 运营管理部总经理 | 13615165889 |
|  |  |  |  |
|  | 张银兵 | 信贷管理部总经理 | 13615167206 |
|  |  |  |  |
|  | 梁磊 | 授信管理部总经理 | 13962036789 |
|  |  |  |  |
|  | 陶建军 | 合规管理部总经理 | 13770267038 |
|  |  |  |  |
|  | 陶建军 | 风险管理部总经理 | 13770267038 |
|  |  |  |  |
|  | 汤林 | 审计部总经理 | 13815542350 |
|  |  |  |  |
|  | 于俊涛 | 安全保卫部总经理 | 13770256006 |
|  |  |  |  |
|  | **应急处置执行小组** | |  |
|  |  |  |  |
| 组长 | 韩阳 | 信息科技分管行长 | 13615165869 |
|  |  |  |  |
| 成员 | 王劲松 | 信息科技部总经理 | 13805110370 |
|  |  |  |  |
|  | 吴海兵 | 行政办公室总经理 | 13813235598 |
|  |  |  |  |
|  | 陈爱忠 | 计划财务部总经理 | 15189297140 |
|  |  |  |  |
|  | 吴斌 | 运营管理部总经理 | 13615165889 |
|  |  |  |  |
|  | 汤林 | 审计部总经理 | 13815542350 |
|  |  |  |  |
|  | 于俊涛 | 安全保卫部总经理 | 13770256006 |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 杨凯 | 信息科技部副股级 | 13912510582 |
|  |  |  |  |
|  | 丁志祥 | 外包公司技术人员 | 13584767607 |
|  |  |  |  |
|  | **应急处置支持保障小组** | |  |
|  |  |  |  |
| 组长 | 韩阳 | 信息科技分管行长 | 13615165869 |
|  |  |  |  |
| 成员 | 吴海兵 | 行政办公室总经理 | 13813235598 |
|  |  |  |  |
|  | 陈爱忠 | 计划财务部总经理 | 15189297140 |
|  |  |  |  |
|  | 陶建军 | 合规管理部总经理 | 13770267038 |
|  |  |  |  |
|  | 于俊涛 | 安全保卫部总经理 | 13770256006 |
|  |  |  |  |
|  | 于俊涛 | 人力资源部总经理 | 13770256006 |
|  |  |  |  |

附件 2

xxx银行

信息科技应急预案——基础设施

第一章 总 则

第一条 为确保xxx银行（以下简称“本行”）中心机房基础设施的正常运行，保障全辖业务系统安全、稳健、高效运作，根据《中华人民共和国计算机信息系统安全保护条例》、《银行业重要信息系统突发事件应急管理规范》和《江苏xx农村商业银行机房管理制度》等有关法律、法规，制定本预案。

第二条 中心机房基础设施应急预案是针对中心机房各类基础设施运行期间可能出现的故障而建立的快速反应机制，确保出现故障后能迅速恢复。

第三条 本行成立了由分管科技副行长任组长的应急处置领导小组，负责本行应急预案的制定、实施和管理，信息科技部负责制定辖内计算机信息系统应急处置预案。

第二章 应急事件分类

第四条 应急事件技术分类

(一)电源系统故障

1.市电供电故障

2.UPS 供电故障

3.应急发电机供电故障

(二)空调故障

(三)消防、防雷故障

(四)自然灾害和盗抢故障

第三章 应急处理

第五条 当发生系统故障时，与应急处置有关的所有人员应服从修复故障的需要，全力以赴解决问题、协调处理相关事宜。

第六条 应急事件发现人员根据故障的情况，判断故障的级别和技术分类，向应急处置领导小组建议启用相应的应急机制。

第七条 所有人员须按本单位应急预案制定的岗位职责及操作要求，力争在最短的时间内排除故障。

第八条 预案参与人员应冷静处理，及时通报实际情况和遇到的问题，必要时要求合作公司远程或现场支持。同时通知各联网网点对客户做好解释工作。

第九条 根据不同的故障技术分类启用相应的应急响应机制：

（一）一级故障

1.须在第一时间通知应急处置领导小组全体成员。若在 4 小时内未能排除故障，应向所在地银行业监督管理局汇报。

2.分管领导责成应急处置领导小组立即召集相关技术部门负责人制定故障排除方案，并通知上、下级相关部门协同完成故障恢复，努力把影响降低到最低程度。

（二）二级故障

1.对于二级故障，应立即根据技术分类，在第一时间通知各相关部门，在 20 分钟之内未能排除故障，及时报告分管领导，请示处理意见；在 20 分钟之内排除故障，则由相关部门负责人于事后向分管领导汇报具体情况。

2.主线路故障由综合负责联系供电部门及时进行恢复，中心机房供电故障，由厂商、综合部、科技部门共同负责解决，具体方案为：

（1）建立各部门通讯联络机制，将厂商、供电部门、综合部等部门通讯方式及联系人员及时通知到位。

（2）应确保备用发电机及 UPS 设备随时能够启用，故障设备自身不能恢复的应与设备维保商取得联系，要求对方远程或在规定的时间内到达现场技术支持，解决相关问题。

（三）三级故障

1.根据技术分类，在第一时间通知相关负责人。

2.排除故障期间，由各部门负责人决定是否向分管领导汇报；问题解决后，由相关部门负责人向分管领导汇报具体情况。

（四）四级故障

值班人员自行解决，或者通知相关人员解决，并向部门责人进行汇报。

第十条 故障具体处置方法

1.电源系统应急预案

定期检查机房供电设备的运行状况和电路线缆器材情况，当发生下列突发事件时，按照以下方案进行处置：

（1）当发生市电供电突然停电或是突发性电力异常故障时，首先应和当地供电局联系确认是否是正常停电，以及预计停电的时间。立即检查不间断电源的电池可供电时间，确保设备的正常运行。如遇到突然断电，应及时将接入 UPS 电源供电范围内的，不影响正常业务运行的大功率设备和电感性设备，如扎钞机、ATM 机、捆钞机等，及时断电，预防突然来电时瞬间电流过大导致设备或 UPS 电源损坏等现象。

（2）当确定停电时间后，首先确定停电的范围以及受影响的设备范围。并及时通知相关的各部门做好停电应急准备。然后通知机房维护相关岗位和单位负责人到达现场，如果是网点机房停电的同时联系外包服务人员立即配送发电机，启用备用发电机开始发电。

（3）当确定停电原因是机房本身供电系统出现故障的，应根据影响范围大小，立即汇报给信息科技部总经理或分管领导，并及时联系相关维护人员达到现场进行检修。对于恢复时间无法预计的，要通知各部门做好备份工作。

（4）恢复供电后，应严格按照操作程序逐步恢复机房设备和 UPS 的供电，停止备用发电机工作，以防瞬间电流过大造成设备损坏。

2.空调故障

机房空调不能正常工作(包括断电)，则即时向信息科技部总经理及时汇报，落实人员，采用降温设备（依情采用临时性家用空调（发电机供电）、电风扇以及冰块），除、增湿设备（依情采用临时性家用干燥剂、增湿器）等临时设备，尽可能满足中心设备运作环境要求；并与设备保修（供应）厂商联系，在最短时间内解决。

3.消防、防雷故障

（1）一旦发现火情（听到消防报警声或目睹火情），当班人员要以最快速度判明起火点位置，按照流程进行处理。在场员工应在避免人员伤亡的前提下全力以赴，奋勇扑救。灭火的同时，当班人员要立即报告信息科技部总经理。若火势较大，当班人员应迅速报警（119），并报告安全保卫部门。

（2）火情结束之后，机房相关人员应全体赶赴现场，并向省中心相关部门汇报。同时立即联系电信、联通、移动等相关网络中心和设备相关厂家，及时评估事故损失情况，研讨恢复网络系统正常运行的最佳解决方案。

（3）遇雷暴天气或接上级部门雷暴气象预警，应关闭所有服务器，切断电源，暂停内部计算机网络工作。雷暴天气结束后，及时开通服务器，恢复内部计算机网络工作。因雷击造成的损失，应及时进行核实、报损，并将详细情况向部门领导汇报。

4.自然灾害和盗抢故障

（1）发生自然灾害后，首先应该组织人员撤离现场。当确认灾害不会造成人身伤害后，再回到机房检查设备，立刻向上级领导汇报，并联系相关网络和设备厂家，积极做好灾后恢复工作，确保在最短时间内恢复机房正常运行。

（2）发生盗抢事件后，要保护好现场然后报警，并向领导汇报情况。待现场处理完毕后，要组织相关人员估计损毁情况，并联系相关网络和设备厂家，积极做好恢复工作。

第十一条 信息科技部人员对出现的问题作认真记录,填写《应急事件登记表》。

第十二条 所有问题解决之后形成的文档，均要在本部门内传阅，或在本部门的会议上传达，建立故障恢复数据库，共同学习故障的解决方法和预防措施。

第五章 应急预防

第十三条 信息科技部的应急预案只针对于各种突发事件的处理，各单位的工作重点是积极预防各种可能发生的问题，力争把问题消灭在萌芽状态，同时，对于本规定中提及的各种问题定时进行演练，确保在出现问题时有条不紊地排除故障，具体要求如下：

（一）计算机系统应急处置领导小组应召集相关人员熟悉本预案中提及的各种应急方案，做到熟练掌握本部门范围内的软硬件故障检查、修复技能，每年进行一次预案演练。

（二）信息科技部要定期对 UPS 供电和发电机组进行放电测试，详细记录设备运行状态，以便及时进行检修。

第六章 责任追究及处罚

第十四条 突发事件处置结束后，总行应组织有关部门人员对事件的原因及全过程进行调查，根据对有关人员的责任调查结果，视情节轻重程度，追究相关人员的责任。可分别采取经济处罚、行政处分乃至移送司法机关处理等处罚措施。

第十五条 小组成员未按照相关规定履行相关职责的，依法给予行政处分；构成犯罪的，移交司法机关、依法追究刑事责任。

第十六条 对突发事件应急管理工中作出突出贡献的成员，应予以表彰和奖励。

第七章 附 则

第十七条 本预案由xxx银行信息科技部负责解释和修订，并根据我行实际情况进行修订。

第十八条 本预案自发布之日起施行。

附件 1：相关的服务和支持单位人员联系方式

附件 2：应急事件登记表

**附件 1：**

**相关的服务和支持单位人员联系方式**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **序号** | |  |  |  |  | **联系人** | |  |  | **联系电话** | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 1 | |  |  |  |  |  | 空调维保工程师 | |  |  | 13915969069 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 2 | |  |  |  |  |  | UPS 维保工程师 | |  |  | 13770908561 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **附件 2：** | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **应急事件登记表** | | | |  |  |  |  |
|  |  |  |  | |  | |  |  |  | |  |  |  |  |  |
|  |  | 系统名称 | | |  | |  |  | 日期 | |  |  | 年 月 | 日 |  |
|  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | **事件上报审批** | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 上报人 | |  |  |  |  |  | 上报时间 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | | |  |  |  |  |
|  |  | 协调人 | |  |  |  |  |  | 信息发布时间 | | |  |  |  |  |
|  |  |  |  | | | |  |  |  | | |  |  |  |  |
|  |  | 技术批准人 | | | | |  |  | 技术批准时间 | | |  |  |  |  |
|  |  |  |  | | | |  |  |  | | |  |  |  |  |
|  |  | 业务批准人 | | | | |  |  | 业务批准时间 | | |  |  |  |  |
|  |  |  |  | | | |  |  |  | | |  |  |  |  |
|  |  | 执行批准人 | | | | |  |  | 执行批准时间 | | |  |  |  |  |
|  |  |  |  | | | |  |  |  | | |  |  |  |  |
|  |  | 启动原因 | | | | | （本栏可为附件） | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | **处理过程** | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 执行处理人 | | | | |  |  | 执行处理时间 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 执行 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 处理 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 步骤 |  | （本栏可为附件） | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | **恢复及反馈** | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 恢复正常时间 | | | | |  |  | 验证人 | |  |  |  |  |  |
|  |  |  | | | | |  |  |  |  |  |  |  |  |  |
|  |  | 反馈时间 | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 备注 | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |

附件 3

xxx银行

外包服务管理应急预案

第一章 总 则

第一条 为确保xxx银行（以下简称“本行”）各业务系统的持续、稳定运行，预防因外包管理的原因造成业务系统服务中断或外包协议的意外终止，并将外包风险可能造成的损失控制在最小范围内，依据《商业银行信息科技风险管理指引》以及《商业银行外包风险管理指引》和《xxx银行信息科技外包管理办法》的要求，制定本预案。

第二条 本预案适用于外包服务商在服务中可能出现的重大缺失，尤其是考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止时应急管理。

第二章 外包的定义和预案范围

第三条 本预案所指的外包是在风险可控的前提下，本行以合同或协议的形式，与信息技术服务商（简称外包商）建立合作关系，委托外包商为本行提供信息科技服务。服务提供商包括独立第三方、商业银行或其所属集团设立在中国境内或者境外的子公司、关联公司或附属机构。

第四条 本行不得将信息科技管理责任和信息风险管控责任外包。

第五条 外包应急预案范围为外包服务商在服务中可能出现的重大缺失。尤其需要考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止。

第三章 外包应急处置程序—预警

第六条 业务主管部门和运行管理部门与系统开发商及设备供应商定期联系，分析系统开发商及设备供应商的经营状况，重点关注系统开发商及设备供应商的技术实力及对系统后期的技术支持服务的承载能力。发现异常情况，应分析其对系统运行的影响程度，并采取相应措施。对可能产生严重危害的状况，应通知有关单位加强预防，并做好应急处置的准备。对已经产生一定危害的状况，应及时采取积极的补救措施，并按应急管理程序报告，通知有关单位作好进一步应急处置的准备。

第四章 外包应急处置程序—报告

第七条 外包服务发生突发事件后，事件发现人应该立即向其部门领导报告，部门领导应依据突发事件的影响程度决定是否向应急处置领导小组报告，同时根据事件性质报相关职能部门，并立即组织应急执行小组进行处置。

第五章 外包应急处置程序—决策

第八条 决策原则：

依据外包中断事件发生的严重程度逐级上报并进行应急决策。应急决策的上报路线为：事件发现人上报其部门负责人，部门负责人上报应急处置领导小组。

外包中断事件发生后，应急处置领导小组应该立即召开会议，研究对策，优先考虑组织技术力量对其进行处置，尽可能在短时间内恢复正常。

外包中断事件不能在短时间内难以恢复的，应急处置领导小组应果断决策，启动相应的应急处置预案。

第九条 决策程序：应急处置领导小组接到外包中断事件报告后，应立即召开小组会议，分析中断事件原因、影响、决策处置措施等，对影响特别严重的，应组织专家会议研究，必要时提请上级领导决策。

第六章 外包应急处置程序—指挥

第十条 外包中断事件应急处置应该遵循“统一指挥、分类管理、分级处置、快速响应”的原则，在应急处置领导小组统一指挥下高效有序应对。应急处置领导小组了解事件基本情况后，应立即下达应急处置指令和要求，根据事件性质安排主要应急执行人员立即赶赴现场，并负责现场统一指挥，采取必要措施，进一步掌握事件状况，防止事态恶化。

第七章 外包应急处置程序—响应

第十一条 获得应急批准后，应急执行小组须立即与新的公司进行联系，并由应急处置领导小组与新的人员或公司进行合同谈判，在谈判中，要求外包公司在时间、项目周期、人员上能充分保证，并充分考察新公司的财务、技术能力、项目管理能力，这一切必须在最短时间内完成。

第八章 外包应急处置程序—恢复

第十二条 安全事故发生之后应采取应急预案中的恢复程序进行恢复，恢复过程中严格按照相应的应急流程进行恢复，以防止在恢复过程中新的安全问题出现。

第十三条 恢复程序在组织原则上按照应急预案建立相应的组织结构，一种方式为：在涉及多个部门的情况下，简单地列出所有的恢复目标，根据每一目标进行计划分解，同时明确相应的部门/人员的责任以及任务。另一种方式为：在某部门内根据相应的功能，明确相应的部门/人员的责任以及任务。

第十四条 各系统在制定相应应急程序时，须明确恢复步骤和指令，部门/人员按照这些指令进行恢复操作。各种操作之间的相互关系也必须加以明确说明。所有的指令和说明必须明白无误，以免因可能引起误解或不明了而导致时间损失。

第十五条 恢复程序中还包括报告阶段。这个阶段的目的是回顾并整理安全事件的各种相关信息，尽可能地把所有情况记录在文档中。这些记录的内容，不仅对有关部门的其它工作具有重要意义，而且对将来应急工作的开展也是非常重要的积累。

第九章 外包应急处置程序—危机处理

第十六条 本行已建立危机处理机制，从维护客户关系、履行告知义务、维护客户合法权益出发，运用公共关系策略、方法，加强与客户、媒体的沟通，适时向公众发布信息，消除或降低危机所造成的负面影响。

第十七条 本行指定专门部门负责危机处理工作，加强舆情监测、信息沟通和发布。

第十八条 本行制定针对社会公众、媒体、股东、客户等相关各方的预案，在运营中断事件发生时及时、准确披露信息，防止因信息不对称可能产生的负面影响。

第十九条 本行实时关注舆情信息，及时澄清虚假信息或不完整信息，消除社会疑虑，化解纠纷。

第十章 附则

第二十条 本预案由xxx银行信息科技部负责解释和修订，并根据本行实际情况进行修订。

第二十一条 本预案和《xxx银行信息科技外包管理办法》互为补充，如与外包管理办法相冲突，以外包管理办法为准。

第二十二条 本预案自发布之日起施行。

附件：服务提供商联系方式

附件：

**服务提供商联系方式**

|  |  |  |  |
| --- | --- | --- | --- |
| 公司名称 | 联系人 | 联系方式 | 备注 |
|  |  |  |  |
| 银科金典 | 丁志祥 | 13584767607 | 网点的日常服务 |
|  |  |  |  |
| 神州数码 | 钱存网 | 13770096605 | ATM 运行维护 |
|  |  |  |  |
| 怡化 | 韩义军 | 15805109572 | ATM 运行维护 |
|  |  |  |  |
| 南大智慧城市 | 邢华健 | 13851477870 | 机房网络 |
|  |  |  |  |
| 华际 | 左宁军 | 13770661591 | 小型机维护 |
|  |  |  |  |
| 南京佳力图 | 工程师 | 13915969069 | 空调维保 |
|  |  |  |  |
| 无锡科士达 | 工程师 | 13770908561 | UPS 维保 |
|  |  |  |  |

附件 4

xxx银行

信息科技应急预案——网络通讯

第一章 总 则

第一条 为确保xxx银行（以下简称“本行”）计算机业务系统安全、稳健地运行，根据《中华人民共和国计算机信息系统安全保护条例》、《银行业重要信息系统突发事件应急管理规范》和《xxx银行计算机网络管理办法》等有关法律、法规，制定本预案。

第二条 计算机网络系统应急预案是针对计算机网络系统运行期间可能出现的故障而建立的快速反应机制，确保系统出现故障后能迅速恢复。

第三条 本行成立由分管科技副行长任组长的应急处置领导小组，负责本级机构应急预案的制定、实施和管理，信息科技部负责制定辖内计算机信息系统应急处置预案。

第二章 网络应急事件分类、分级及网络配置

第四条 通讯网络应急事件分类：

1.网络设备故障；

2.网络线路故障；

3.网络配置故障；

4.网络安全故障。

第五条 通信网络系统突发事件级别分为四级：一般(IV 级)、较大(III 级)、重大(II 级)和特别重大(I 级)，对应颜色依次为蓝色、黄色、橙色和红色。

IV 级：支行范围或个人出现并可能造成损害的通信网络系统安全事件。

Ⅲ级：支行的网络系统、软件系统、电力系统和通信设施受到严重破坏或损坏，对分行业务造成无法正常运营的通信网络系统安全事件。

II 级：总行重要信息系统、数据系统，软件系统瘫痪导致业务中断，纵向或横向延伸可能造成严重影响或较大经济损失的通信网络系统安全事件。

I 级：黑客利用网络信息进行有组织的大规模的入侵破坏活动，或者多个支行的基础网络、重要信息系统、多个软件系统瘫痪，导致业务中断，造成或可能造成巨大经济损失的通信网络安全事件。

第六条 网络配置清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **大类** | **种类** | **品牌** |  |  | **型号** | **供应商** |
|  |  |  |  |  |  |  |
|  | 骨干网路 | Cisco |  | 3900 | Series | 南大智慧城市 |
|  | 由器 |  |  |  |  |  |
|  | Cisco |  | 3900 | Series | 南大智慧城市 |
|  |  |  |  |  |  |  |
|  |  | Cisco |  | 3900 | Series | 南大智慧城市 |
|  |  |  |  |  |  |  |
|  | 非骨干网 | Cisco |  | 3900 | Series | 南大智慧城市 |
|  |  |  |  |  |  |
|  | Cisco |  | 7200 | Series VXR | - |
|  | 路由器 |  |
|  |  |  |  |  |  |
|  | Cisco |  | THERM 7606-S | | 南大智慧城市 |
|  |  |  |
|  |  |  |  |  | |  |
|  |  | Cisco |  | 2800 series | | - |
|  |  |  |  |  |  |  |
| 网络设备 | 核心交换 | Cisco |  | Catalyst 4503 | | 南大智慧城市 |
| 机 |  |
|  |  |  |  |  |  |
|  |  |  |  |  | |  |
|  |  | Cisco |  | Catalyst 3750X | | 南大智慧城市 |
|  |  |  |  |  | |  |
|  |  | Cisco |  | Catalyst 3750X | | 南大智慧城市 |
|  |  |  |  |  | |  |
|  | 非核心交 | Cisco |  | Catalyst 3750 | | 南大智慧城市 |
|  |  |  |  |  |  |
|  | Cisco |  | Catalyst 3750 | | 南大智慧城市 |
|  | 换机 |  |
|  |  |  |  |  |  |
|  | Cisco |  | Catalyst3750 Series | | - |
|  |  |  |
|  |  |  |  |  | |  |
|  |  | Cisco |  | Catalyst 3650 | | - |
|  |  |  |  |  | |  |
|  |  | Cisco |  | Catalyst 3650 | | - |
|  |  |  |  |  | |  |
| 存储设备 | 存储光纤 | Brocade |  | Brocade 300 | | 江苏华龙 |
|  |  |  |  |  |  |  |
|  |  |  |  | |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **大类** | **种类** | **品牌** | **型号** | **供应商** |
|  |  |  |  |  |
|  | 交换机 | Brocade | Brocade 300 | 江苏华龙 |
|  |  |  |  |  |
|  |  | Brocade | Brocade 300 | 江苏华龙 |
|  |  |  |  |  |
|  |  | Brocade | Brocade 300 | 江苏华龙 |
|  |  |  |  |  |
|  |  | 山石 | FW | 南大智慧城市 |
|  |  |  |  |  |
|  | 防火墙 | 山石 | FW | 南大智慧城市 |
|  |  |  |  |
|  | 山石 | FW | 南大智慧城市 |
|  |  |
|  |  |  |  |  |
| 安全设备 |  | 天融信 | FW | - |
|  |  |  |  |
| 入侵检测 | 天融信 | IPS | 南京普建维斯 |
|  |
|  | 设备 |
|  |  |  |  |
|  |  |  |  |  |
|  | 安全隧道 | 深信服 | VPN | 南京科颐 |
|  | 设备 |
|  |  |  |  |
|  |  |  |  |  |

第三章 应急处理

第七条 当发生系统故障时，与应急处置有关的所有人员应服从修复故障的需要，全力以赴解决问题、协调处理相关事宜。

第八条 应急事件发现人员根据故障的情况，判断故障的级别和技术分类，向应急处置领导小组建议启用相应的应急机制。

第九条 所有人员须按本单位应急预案制定的岗位职责及操作要求，力争在最短的时间内排除故障。

第十条 预案参与人员应冷静处理，及时通报实际情况和遇到的问题，必要时要求合作公司远程或现场支持。同时通知各营业网点对客户做好解释工作。

第十一条 根据不同的故障技术分类启用相应的应急响应机制：

（一）一级故障

1.须在第一时间通知应急处置领导小组全体成员。若在 4 小时内未能排除故障，应向所在地银行业监督管理局汇报。

2.分管领导责成应急处置领导小组立即召集信息科技部负责人制定故障排除方案，并通知上、下级相关部门协同完成故障恢复，努力把影响降低到最低程度。

（二）二级故障

1.对于二级故障应立即根据技术分类，第一时间通知各相关部门，在 20 分钟之内未能排除故障，及时报告分管领导，请示处理意见；在 20 分钟之内排除故障，则由相关信息科技部负责人于事后向分管领导汇报具体情况。

2.网络系统，骨干网络通讯故障由省中心负责应急恢复，分中心和本行信息科技部现场协助。网点通讯故障由本行信息科技部恢复，具体方案为：

（1）建立省、市、县三级沟通协调机制。

（2）应确保备用网络设备随时能够启用，故障设备自身不能恢复的应与设备维保商取得联系，要求对方远程或在规定的时间内到达现场技术支持，解决相关问题。

（3）通讯线路中断应立即启用备份线路并及时请求线路运营商予以解决。

（三）三级故障

1.根据技术分类，在第一时间通知相关负责人。

2.排除故障期间，由信息科技部负责人决定是否向分管领导汇报。问题解决后，由信息科技部负责人向分管领导汇报具体情况。

（四）四级故障：

值班人员自行解决，或者通知相关人员解决，并向信息科技部负责人进行汇报。

第十二条 故障具体处理方案：

1.网络设备故障

（1）值班人员负责收集网络设备的工作状况，一旦发现设备发生故障，应及时报告网络管理员判断对业务的影响程度。若对业务不产生影响或轻微影响，由值班人员登记情况并向信息科技部负责人汇报，由信息科技部负责人（或责成网络管理员）与保修（供货）商联系并及时处理故障。

（2）若对业务产生重大影响，热备份设备应自动切换至备机工作（冷备份设备由网络管理员手动切换至备机工作），此时网络管理员应严密监测切换情况，在确保业务正常开展的同时，及时报告信息科技部负责人。若热备份设备未能自动切换至备机，由值班人员即时汇报信息科技部负责人，由信息科技部负责人调集网络管理员等人员及时当场查明原因手工切换至备机工作，并与保修（供货）商联系，要求立即解决故障，同时逐级上报。

（3）若出现灾难性事故，主、备机同时不能工作，网络管理员即时报告信息科技部负责人，逐级上报，同步联系设备保修（供货）商临时调用备用机；由信息科技部负责人联系相关部门，请求相应的技术支持；由应急处置领导小组据情决定是否上报省联社，确定是否启用手工应急措施。

2.网络线路故障

（1）局域网中断紧急处置措施

A、局域网中断后，管理员在检查本机的网卡工作正常情况下，ping 网关不通时，应采用测线仪测试线路，迅速排除故障。急用时通报网络管理员和信息科技部负责人，由信息科技部负责人调集相关人员采用临时拖线处理，事后采用标准布线方式恢复。

B、如属线路故障，更换新线路或重新安装线路；或从最近飞线至故障设备；

C、如属路由器、交换机等网络设备（光模块）故障，应立即查找是否有相关备件可以替换，或与设备提供商联系更换设备，并调试畅通；

D、如属路由器、交换机配置文件破坏，应迅速按照备份配置文件重新配置，并调试畅通；如遇无法解决的技术问题，立即向有关厂商请求支援；

E、情况严重的，根据突发事件级别应及时向有关上级部门汇报。

（2）广域网线路中断紧急处置措施

A、链路出现问题后，网络维护人员应立即向信息科技部负责人报告，迅速判断故障，查明故障原因；确定为线路故障的，应及时联系网络运营商进行故障修复，以降低全局风险发生几率。若主、备线路同时出现故障，且网络运营商短时间内无法修复的，要求网络运营商采取临时紧急布线方式，并向应急处置领导小组汇报，确定是否启用手工应急措施。

B、如属本行管辖范围，由双方技术人员立即配合予以恢复。如遇无法恢复情况，立即进行备件更换或向有关厂商请求支援；如属运营商管辖范围，立即与运营商维护部门申报故障，请求修复；

D、根据突发事件级别应及时向有关上级部门汇报。

3.网络配置故障

（1）如防火墙、路由配置信息故障或崩溃，系统会自动切换到备用网络配置系统，值班人员迅速通知网络管理员检查设备和网络配置故障原因，并立即向厂商请求支援，直至设备恢复正常。

（2）如网络管理员和厂商短期内无法恢复网络配置，根据突发事件级别立即向科技部负责人报告相关情况，科技部负责人据情向应急处置领导小组汇报，确定是否启用应急措施。

4.网络安全故障

(1)黑客攻击时的紧急处置措施

A、当发现网页内容被篡改、Internet 接入路由器有未知用户登录或通过其他方式发现有黑客正在进行攻击时，应立即向信息科技部相关人员通报情况；

B、在信息科技部人员授权下，立即备份当时的 log 日志并采用端口限制方式阻断外部的入侵，观察被攻击的服务器等设备状态，同时向信息科技部负责人汇报情况；

C、协调相关应用部门，与信息科技部技术人员一同负责被破坏系统的恢复与重建工作；

D、协助信息科技部人员协同有关部门共同追查非法信息来源；

E、情况严重的，根据突发事件级别应及时向有关上级部门汇报。

(2)病毒安全紧急处置措施

A、当发现计算机感染病毒后，应立即将该机从网络上隔离出来；或从网络设备状态发现病毒爆发应采取定位或 IP 查询将病毒机器所在的网络设备端口关闭；

B、通知维护人员对该设备的硬盘进行数据备份；

C、启用杀病毒软件对该机进行杀毒处理，同时采用病毒检测软件对其他机器进行病毒扫描和清除工作；

D 如发现杀毒软件无法清除该病毒，应立即通知用户并向信息科技部负责人报告，经信息科技部技术人员确认无法查杀该病毒并同意格式化硬盘后，作好相关记录，并格式化硬盘；

E、机器恢复后重新开启网络设备的相应端口；

F、认为情况极为严重，根据突发事件级别应及时向有关上级部门汇报。

第十三条 信息科技部人员对出现的问题作认真记录,填写《应急事件登记表》。

第十四条 所有问题解决之后形成的文档，均要在本部门内传阅，或在本部门的会议上传达，建立故障恢复数据库，共同学习故障的解决方法和预防措施。

第四章 协调人员及联系方式

第十五条 针对系统应急工作要求列出相关服务和支持单位人员联系方式，以确保在最短时间内对系统进行恢复。

|  |  |  |  |
| --- | --- | --- | --- |
| 公司名称 | 联系人 | 联系方式 | 备注 |
|  |  |  |  |
| xx电信局 | 吴咏梅 | 15312892055 | 电信线路报修 |
|  |  |  |  |
| xx移动公司 | 章竟 | 13921801627 | 移动线路报修 |
|  |  |  |  |
| xx联通公司 | 童立里 | 15651554996 | 联通线路报修 |
|  |  |  |  |
| 南大智慧城市 | 邢华健 | 13851477870 | 机房网络 |
|  |  |  |  |

第五章 应急预防

第十六条 该应急预案只针对于各种突发事件的处理，各单位的工作重点就是积极预防各种可能发生的问题，力争把问题消灭在萌芽状态，同时，对于本规定中提及的各种问题要定时进行演练，确保在出现问题时有条不紊地排除故障，具体要求如下：

（一）计算机系统应急处置领导小组应召集相关人员熟悉本预案中提及的各种急方案，做到熟练掌握本部门范围内的软硬件故障检查、修复技能，每年进行一次预案演练。

（二）信息科技部要对每次网络配置变更进行详细记录，对配置参数调整前后的数据进行详细登记，对于系统配置、参数调整出现的问题可予以及时恢复。

（三）信息科技部要对全部软件的安装介质，说明文档妥善保管，对系统每次更新、安装新程序之后要及时做好备份工作，同时妥善保管备份介质。

第六章 责任追究及处罚

第十七条 突发事件处置结束后，总行应组织有关部门人员对事件的原因及全过程进行调查，根据对有关人员的责任调查结果，视情节轻重程度，追究相关人员的责任。可分别采取经济处罚、行政处分乃至移送司法机关处理等处罚措施。

第十八条 小组成员未按照相关规定履行相关职责的，依法给予行政处分；构成犯罪的，移交司法机关、依法追究刑事责任。

第十九条 对突发事件应急管理工中作出突出贡献的成员，应予以表彰和奖励。

第七章 附则

第二十条 本预案由xxx银行信息科技部负责解释和修订，并根据我行实际情况进行修订。

第二十一条 本预案自发布之日起施行。

附件：应急事件登记表

附件

**应急事件登记表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 系统名称 |  |  | 日期 |  | 年 | 月 | 日 |  |
|  |  |  |  |  |  |  |  |  |
|  |  | **事件上报审批** | | |  |  |  |  |
| 上报人 |  |  | 上报时间 | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| 协调人 |  |  | 信息发布时间 | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| 技术批准人 |  |  | 技术批准时间 | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| 业务批准人 |  |  | 业务批准时间 | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| 执行批准人 |  |  | 执行批准时间 | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| 启动原因 |  | （本栏可为附件） | | |  |  |  |  |
|  |  |  | | |  |  |  |  |
|  |  | **处理过程** | | |  |  |  |  |
| 执行处理人 |  |  | 执行处理时间 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

执行

处理

步骤

（本栏可为附件）

|  |  |  |  |
| --- | --- | --- | --- |
|  | **恢复及反馈** | | |
| 恢复正常时间 |  | 验证人 |  |
|  |  |  |  |
| 反馈时间 |  |  |  |
|  |  |  |  |
| 备注 |  |  |  |
|  |  |  |  |

附件 5

xxx银行

信息科技应急预案——业务系统

第一章 总 则

第一条 为确保xxx银行（以下简称“本行”）各类业务信息系统安全、稳健地运行，根据《中华人民共和国计算机信息系统安全保护条例》、《银行业重要信息系统突发事件应急管理规范》和《xxx银行计算机信息系统应急处置管理办法》等有关法律、法规，制定本预案。

第二条 业务信息系统应急预案是针对各类业务信息系统运行期间可能出现的故障而建立的快速反应机制，以确保系统出现故障后能迅速恢复。

第三条 本行成立了由分管科技副行长任组长的应急处置领导小组，负责本级机构应急预案的制定、实施和管理，信息科技部负责制定辖内计算机信息系统应急处置预案。

第二章 应急事件技术分类及分级

第四条 应急事件技术分类（一） 业务信息系统主要是指核心系统、中间业务平台、信贷系统、支付系统、网上银行系统，其他业务系统根据实际情况和发展需要确定恢复范围。业务信息系统方面的故障包括：

1.业务信息系统的运行硬件出现故障，包括服务器和网络；

2.业务信息系统的支撑软件出现故障，包括软件 BUG、操作

系统、中间件、数据库等；

3.业务信息系统的网络出现故障，包括网卡、交换机、路由器、防火墙、网线等组成网络的软硬件；

4.省级联网系统出现故障；

5.业务信息系统操作人员操作出错；

（二）其他方面的故障：

主要运行支持设施方面故障，包括火灾、水灾、电力系统等。

第五条 按照突发事件的性质、严重程度、可控性和影响范围，将其分为一般（IV 级）、较大（III 级）、重大（II 级）、特别重大（I 级）；

一般（IV 级）：信息系统中单个系统故障，但未影响业务系统运行，也未造成社会影响或经济损失的突发事件；

较大（III 级）：信息系统单个系统故障导致业务中断，可能造成较大业务影响或较大经济损失的突发事件；

重大（II 级）：信息系统单个系统故障引起多个业务系统长时间中断，可能造成重大社会影响和巨大经济损失的突发事件；

特别重大（I 级）：特指发生不可预见的灾难性事故，如火灾、水灾等。

第三章 应急处理

第六条 当发生业务信息系统故障时，事件发现人应该立即向其部门负责人报告，由其部门负责人向应急处置领导小组报告，应急处置领导小组接到突发事件报告后，应立即召开领导小组会议，分析突发事件原因、影响、决策处置措施等，对影响特别严重的，应组织专家会议研究，必要时提请上级领导决策。

第七条 业务信息系统故障的应急处置应遵循“统一指挥、分

类管理、分级处置、快速响应”的原则，在应急处置领导小组统一指挥下高效有序应对。

第八条 应急处置领导小组了解事件基本情况后，应立即下达应急处置指令和要求，根据事件性质安排主要应急执行人员立即赶赴现场，并负责现场统一指挥，采取必要措施，进一步掌握事件状况，防止事态恶化，同时安全保卫部门应该保护现场和维护治安秩序。

第九条 预案参与人员应冷静处理，及时通报实际情况和遇到的问题，必要时要求合作公司远程或现场支持。同时通知各营业网点对客户做好解释工作。

第十条 根据不同的故障技术分类启用相应的应急响应机制：

（一）一级故障

发生故障后，应立刻报应急处置领导小组，所有小组成员需立即赶赴现场，由应急处置领导小组启动应急预案，并通知上、下级相关部门协同完成故障恢复，努力把影响降低到最低程度。若在 4小时内未能排除故障，应向所在地银行业监督管理局汇报。

（二）二级故障

对于二级故障，值班人员或事件发现人在发现系统故障后，向系统主管部门报告故障情况，系统主管部门应立即上报应急处置领导小组，应急处置领导小组组织应急执行人员 1 小时内到达现场，查找、分析故障原因，制定故障处理方案并实施，处理情况报应急处置领导小组。如果故障在 3 小时内没有得到解决，或情况进一步恶化，则升级到一级事件。

（三）三级故障

1.值班人员或事件发现人在发现系统故障后，向系统主管部门报告故障情况，系统主管部门组织技术人员查找、分析故障原因，制定故障处理方案并实施。如果故障在 48 小时内无法解决或情况迅速恶化，升级为二级事件或者一级事件。

2.排除故障期间，由各系统主管部门负责人决定是否向分管领导汇报；问题解决后，由相关部门负责人向分管领导汇报具体情况。

（四）四级故障：

值班人员自行解决，或者通知相关技术人员协助解决，并向部门负责人进行汇报。

第十一条 具体应急措施

（1）总体要求本应急预案适用于柜台营业系统、综合业务管理系统、财务管理系统、办公自动化系统等。为了在排除故障过程中不影响正常营业，要求各部门事先按一定的比例准备 PC 机、打印机、UPS、网络设备等备机或备件，各岗位要熟悉预案的内容和应急处理办法，将要岗人员的电话手机等联系方式放置于显要位置以备使用，并进行必要的系统演练。故障完全排除恢复正常业务后，总结故障的产生原因，指导以后故障排除工作，并写出事件的详细报告，记录备案。

（2）计算机设备损坏或计算机操作系统崩溃的应急处理当柜台营业系统计算机、打印机、UPS、网络设备等出现故障时，柜台操作人员发现故障后，应先排除外部故障，在排除外部电源问题和插接问题仍然不能正常运行时，应填写计算机操作日志，详细描述故障现象和特征，并马上向本行系统管理员报告，由系统管理员根据故障的原因判断能否在短时间修复，如不能及时解决，则用备机更换，保证业务的正常运行，然后再对损坏的设备进行修复，如本行系统管理员仍不能修复，应及时送到指定维修地点维修，检修期间要有具备计算机基本知识的本行内部人员在场，不能现场修复的，应带回含数据的硬盘和设备。

（3）通讯设备和线路故障的应急处理本行的计算机业务系统，实行的是服务器带终端的联网模式，涉及服务器、网络设备和联网线路运行安全等问题，本方案所指的网络设备及线路故障的概念，是指由于运营商的线路或中心机房的网络设备出现故障，机房管理员和操作员应牢记各种设备的操作流程、技术服务电话、技术人员的联系方式，以便及时得到技术支持，正确撑握运营商的线路与中心设备之间的联接方法，了解运营商提供的信号指示含义。如果是网络运营商的线路问题，应重新启动交换机，并通过指示灯的状态判断故障出现原因，如是主机死机应重新启动主机，如线路灯不正常，应与网络运营商取得联系维修，如不能判断故障情况应及时与本行系统管理员联系解决。

（4）供电系统中断的应急处理如网点供电线路中断，UPS 电源自动供电，如长时间供电中断，要与供电单位联系确定恢复供电时间，检查应急电源设备，并与供电部门联系，准备使用发电机供电。

（5）由于误操作或帐务处理错误导致故障的应急处理业务操作人员在操作过程中，发生误操作或帐务处理错误导致不能继续工作或可能造成帐务混乱、系统崩溃的，按照系统权限的设定，在权限范围内进行处理，超过自身权限时，应通知相应权限的系统管理员或业务主管进行处理。

（6）应用程序出现非正常问题的应急处理应用程序是正在使用的各种业务软件，对业务系统的数据及时维护、备份和恢复，是系统出现灾难性问题时的重要复原手段，在日常单机和网络的运行中有着后备安全的重要作用，绝不能忽视。本行系统管理员对所辖的应用软件和业务系统数据必须双重备份异地保存；业务系统的应用程序，本行要有备份的各业务系统，并指定专人保管，系统管理员必须对所辖的所有应用程序的安装、使用、维护非常熟悉。当发现有应用程序确实有误，不能进行正常的营业；计算机操作系统出现故障，并且不能在短时间内判断出原因和加以解决重新安装系统的，应报告本行系统管理员及时修复，若需要重新安装应用程序，必须确认恢复故障前的数据，并由操作员核对后确认。

（7）重要数据备份及其应急处理重要数据的备份和恢复，是系统出现灾难性问题的重要复原手段，在日常单机和网络的运行中有着后备安全的重要作用，绝不能忽视。备份数据万一出现问题，在特定情况下就可能带来毁灭性的灾难。每天营业终了，必须进行数据的安全备份，保证备份的可靠性、完整性和及时性，并保证两份以上，有明确标识，异地保管。对所有备份数据的操作和保管指定有明确的责任人。

当发现有数据确实有误，不能进行正常营业的，或数据有错误，并且不能在短时间判断出原因和加以解决的，由掌握系统密码的超级用户介入，进行数据恢复，由操作员确认数据的一致性。

（8）反病毒应急处理

计算机病毒对于计算机的软硬件能带来巨大的损伤，对于一些重要数据的侵害可能是无法逆转和弥补的。对于计算机病毒侵害首要的是抓好预防工作，要求设备安装杀毒软件、防病毒防火墙，同时及时升级病毒库。针对一些比较重要的数据资料应使用其他磁介质（U 盘、软盘、光盘、磁带等）另行备份。当发现计算机病毒后，首先断开网络、备份数据，然后杀毒，如果正常则继续运行，不正常则将备份数据移植到备用机器上先行工作，感染病毒机器处理完后换回，并检查与染毒设备接触过的相关设备。当重要软件或数据由于病毒原因损坏，要尝试修复，不能修复的要恢复最后一次备份数据并补录损失数据。

（9）机房安全应急处理

切实做好机房及其网络设备的防雷、防火、防盗和防信号非法接入。若有以上情况发生，在向应急处置领导小组及时报告的同时，本行计算机网络安全保护工作职能部门还应向公安网监部门报告。机房配置安全管理人员，严格执行本行计算机网络安全管理制度，规范业务人员进入计算机机房操作的管理，落实机房登记制度和日志留存。

（10）信息科技部人员对出现的问题作认真记录,填写《应急事件登记表》。

第十二条 所有问题解决之后形成的文档，均要在本部门内传阅，或在本部门的会议上传达，建立故障恢复数据库，共同学习故障的解决方法和预防措施。

第四章 协调人员及联系方式

第十三条 列出相关服务和支持单位人员联系方式，以确保在最短时间内对系统进行恢复。

|  |  |  |  |
| --- | --- | --- | --- |
| 公司单位名称 | 联系人 | 联系方式 | 备注 |
|  |  |  |  |
| 财政局 | 韦迟 | 13770252976 | 财政集中支付系统 |
|  |  |  |  |
| 财政局 | 韦迟 | 13770252976 | 财政非税收入系统 |
|  |  |  |  |
| 人社局 | 殷海华 | 18905110506 | 社会保险业务系统 |
|  |  |  |  |

第五章 应急预防

第十四条 信息科技部的应急预案只针对于各种突发事件的处理，各单位的工作重点就是积极预防各种可能发生的问题，力争把问题消灭在萌芽状态，同时，对于本规定中提及的各种问题要定时进行演练，确保在出现问题时有条不紊地排除故障，具体要求如下：

（一）计算机系统应急处置领导小组应召集相关人员熟悉本预案中提及的各种应急方案，做到熟练掌握本部门范围内的软硬件故障检查、修复技能，每年进行一次预案演练。

（二）信息科技部要对系统变更进行详细记录，对配置参数调整前后的数据进行详细登记，对于系统配置、参数调整出现的问题可予以及时恢复。

（三）信息科技部要对全部软件的安装介质，说明文档妥善保管，对系统每次更新、安装新程序之后要及时做好备份工作，同时妥善保管备份介质。

第六章 责任追究及处罚

第十五条 突发事件处置结束后，总行应组织有关部门人员对事件的原因及全过程进行调查，根据对有关人员的责任调查结果，视情节轻重程度，追究相关人员的责任。可分别采取经济处罚、行政处分乃至移送司法机关处理等处罚措施。

第十六条 应急处置领导小组成员未按照相关规定履行相关职责的，依法给予行政处分；构成犯罪的，移交司法机关、依法追究刑事责任。

第十七条 对突发事件应急管理工中作出突出贡献的成员，应予以表彰和奖励。

第七章 附则

第十八条 本预案由xxx银行信息科技部负责解释和修订，并根据我行实际情况进行修订。

第十九条 本预案自发布之日起施行。

附件：应急事件登记表

**应急事件登记表**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 系统名称 | |  |  |  |  | 日期 |  | 年 | 月 | 日 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | **事件上报审批** | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 上报人 | | |  |  |  | 上报时间 | |  |  |  |
|  |  | |  |  |  |  | |  |  |  |
| 协调人 | | |  |  |  | 信息发布时间 | |  |  |  |
|  |  | |  |  |  |  | |  |  |  |
| 技术批准人 | | |  |  |  | 技术批准时间 | |  |  |  |
|  |  | |  |  |  |  | |  |  |  |
| 业务批准人 | | |  |  |  | 业务批准时间 | |  |  |  |
|  |  | |  |  |  |  | |  |  |  |
| 执行批准人 | | |  |  |  | 执行批准时间 | |  |  |  |
|  |  | |  |  |  |  | |  |  |  |
| 启动原因 | | |  | （本栏可为附件） | | | |  |  |  |
|  |  |  |  |  |  | | |  |  |  |
|  |  |  |  |  | **处理过程** | | |  |  |  |
|  |  | | |  |  |  | |  |  |  |
| 执行处理人 | | |  |  |  | 执行处理时间 | |  |  |  |
|  |  | |  |  |  |  |  |  |  |  |
| 执行 |  | | |  |  |  |  |  |  |  |
| 处理 |  | | |  |  |  |  |  |  |  |
| 步骤 |  | | |  |  |  |  |  |  |  |
|  | （本栏可为附件） | | | | | | |  |  |  |
|  |  |  |  |  |  | | |  |  |  |
|  |  |  |  |  | **恢复及反馈** | | |  |  |  |
|  |  | | |  |  |  | |  |  |  |
| 恢复正常时间 | | | |  |  | 验证人 |  |  |  |  |
|  | | | |  |  |  |  |  |  |  |
| 反馈时间 | | | |  |  |  |  |  |  |  |
|  | | | |  |  |  |  |  |  |  |
| 备注 | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

附件 6

xxx银行

信息科技应急预案——主机系统

第一章 总 则

第一条 为确保xxx银行（以下简称“本行”）计算机业务系统安全、稳健地运行，根据《中华人民共和国计算机信息系统安全保护条例》、《银行业重要信息系统突发事件应急管理规范》和《xxx银行计算机信息系统应急处置管理办法》等有关法律、法规，制定本预案。

第二条 主机系统应急预案是针对主机系统运行期间可能出现的故障而建立的快速反应机制，以确保系统出现故障后能迅速恢复。

第三条 本行成立了由分管科技副行长任组长的应急处置领导小组，负责本级机构应急预案的制定、实施和管理，信息科技部负责制定辖内计算机信息系统应急处置预案。

第二章 应急事件分类及分级

第四条 应急事件技术分类

1.主机硬件故障：

（1）主机系统主、备两套设备同时发生故障；

（2）包括存储、CPU、主板、内存等；

2.主机软件系统故障：

（1）操作系统软件故障，系统无法运行；

（2）核心业务的数据库系统出现无法使用的故障；

（3）应用系统软件故障，系统无法运行。

3.主机安全方面故障。

主机受到网络攻击造成系统缓慢，数据流失和系统崩溃。

第五条 应急事件情况按其对业务的影响程度进行分级：

一级：最严重的级别，具有以下两个重要标志：一是全局性，二是特别紧急性。全局性指涉及到辖内所有网点或者大多数网点，全部或者大多数交易不正常且短时间内难以恢复。特别紧急性是指可能影响到人身安全或资金安全的情况。

1.重大火灾、地震等自然灾害导致中心机房主要生产设施遭受毁灭性破坏，形成灾难性故障，持续 6 小时以上不能修复。

2.关键设备的重大故障引起的业务中断。如业务系统主机、存储设备同时故障，持续 6 个小时以上无法修复。

3.由于严重的存储设备故障或数据库崩溃等原因，造成业务数据丢失。

二级：较严重的级别，它涉及部分主要设备、部分网点、所有网点的部分交易，以及虽然严重但短时间内能够处理的情况。它同时还包括虽然网点工作正常但主要设备出现严重问题的情况。

1.主机系统主、备两套设备同时发生故障。

2.磁盘故障，破坏数据的完整性。

3.软件系统故障：

（1）操作系统软件故障，系统无法运行；（2）核心业务的数据库系统出现无法使用的故障；（3）应用系统软件故障，系统无法运行。

三级：一般性的技术故障是指部分网点的部分交易、个别网点的故障错误以及软、硬件的非严重性问题。

1、 主机、应用系统故障：

（1）业务系统主机需切换到备份机；（2）业务服务器需由备份机接管服务；（3）应用系统软件故障，系统无法运行。

四级：轻微的技术故障，指个别的、非主要的设备或者个别的数据、程序错误。

第三章 应急处理

第六条 当发生系统故障时，与应急处置有关的所有人员应服从修复故障的需要，全力以赴解决问题、协调处理相关事宜。

第七条 应急事件发现人员根据故障的情况，判断故障的级别和技术分类，向应急处置领导小组建议启用相应的应急机制。

第八条 所有人员须按本单位应急预案制定的岗位职责及操作要求，力争在最短的时间内排除故障。

第九条 预案参与人员应冷静处理，及时报告实际情况和遇到的问题，必要时要求合作公司远程或现场支持。同时通知各联网网点对客户做好解释工作。

第十条 根据不同的故障技术分类启用相应的应急响应机制：

（一）一级故障

1.须在第一时间通知应急处置领导小组全体成员。若在 4 小时内未能排除故障，应向所在地银行业监督管理局汇报。

2.分管领导责成应急处置领导小组立即召集相关技术部门负责人制定故障排除方案，并通知上、下级相关部门协同完成故障恢复，努力把影响降低到最低程度。

（二）二级故障

1.对于二级故障：立即根据技术分类，在第一时间通知各相关部门，在 20 分钟之内未能排除故障，及时报告分管领导，请示处理意见；在 20 分钟之内排除故障，则由相关部门负责人于事后向分管领导汇报具体情况。

2.主机系统故障，立即通知计算机部门负责人，由计算机部门负责人组织技术人员进行维修，具体方案：

（1）技术人员查明故障原因为程序问题，则立即进行程序修复和更新，如果仍然不能解决问题，立即切换到备份机。

（2）生产系统出现硬件致命损坏，立即启用备份机。

（3）如果经以上处理故障仍然不能排除，则立即请求相关软、硬件、集成公司远程或现场支持。

（4）若在 4 小时内未排除故障，也应向所在地银行业监督管理局汇报。

（三）三级故障

1.根据技术分类，在第一时间通知相关负责人。

2.排除故障期间，由各部门负责人决定是否向分管领导汇报；问题解决后，由相关部门负责人向分管领导汇报具体情况。

（四）四级故障

值班人员自行解决，或者通知相关人员解决，并向部门负责人进行汇报。

第十一条 具体应急步骤

1.主机硬件故障

（1）后台主机硬件故障值班人员一旦发现主机发生故障，应及时报告系统管理员判断对业务的影响程度。若对业务不产生影响或轻微影响，则登记情况并与保修（供货）商联系并及时处理故障。若对业务产生重大影响，系统应手动切换至备机工作，此时系统管理员在严密监测切换情况，确保业务正常开展的同时，及时逐级上报。

若出现灾难性事故，主、备机同时不能工作，则即时报告部门负责人和应急处置领导小组，同步联系相关部门临时调用备用机；并报告省中心，请求相应的技术支持；由应急处置领导小组决定上报上级监管部门，恢复硬件系统后，继续按软件故障应急方案处理。

（2）磁盘阵列故障如若单个硬盘故障不影响业务正常开展的，则登记情况并及时向部门负责人汇报。并与保修（供货）商联系，要求立即更换硬盘。

多个硬盘或阵列出现故障，视为严重故障，则应即时报告部门负责人和应急处置领导小组，同步联系设备保修（供货）商现场支持，恢复硬件系统后，继续按软件故障应急方案处理。

2.主机软件故障

包括主机系统软件故障、数据库故障、中间件故障主机若发生故障，首先判断对业务的影响程度，若对业务不产生影响或轻微影响，登记情况并向部门负责人汇报。自行不能解决的立即与系统服务商联系并及时处理故障。

若对业务产生重大影响，系统应切换至备机工作，此时系统管理员在严密监测切换情况，确保业务正常开展的同时，逐级上报；若系统未能切换至备机，则即时汇报部门负责人，由部门负责人调集人员及时当场查明原因手工切换至备机工作，并与系统服务商联系，要求立即解决故障，由部门负责人据情确定是否上报总行领导。

若出现灾难性事故，主、备机同时不能工作，系统管理员即时报告信息科技部负责人，由信息科技部负责人联系省联社，请求相应的技术支持；由应急处置领导小组据情决定是否上报省联社，确定是否启用手工应急措施。

3.主机安全故障。

(1)黑客攻击时的紧急处置措施

A、当发现网页内容被篡改、Internet 接入路由器有未知用户登录或通过其他方式发现有黑客正在进行攻击时，应立即向信息科技部相关人员报告情况；

B、在信息科技部人员授权下，立即备份当时的 log 日志并采用端口限制方式阻断外部的入侵，观察被攻击的服务器等设备状态，同时向信息科技部负责人汇报情况；

C、协调相关应用部门，与信息科技部技术人员一同负责被破坏系统的恢复与重建工作；

D、协助信息科技部人员协同有关部门共同追查非法信息来源；

E、情况严重的，根据突发事件级别应及时向有关上级部门汇报。

(2)病毒安全紧急处置措施

A、当发现计算机感染有病毒后，应立即将该机从网络上隔离出来；或从网络设备状态发现病毒爆发应采取定位或 IP 查询将病毒机器所在的网络设备端口关闭；

B、通知维护人员对该设备的硬盘进行数据备份；

C、启用杀病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作；

D、如发现杀病毒软件无法清除该病毒，应立即通知用户并向及信息科技部负责人报告，经信息科技部技术人员确认无法查杀该病毒并同意格式化硬盘后，作好相关记录，并格式化硬盘；

E、机器恢复后重新开启网络设备的相应端口；

F、认为情况极为严重，根据突发事件级别应及时向有关上级部门汇报。

4.水灾、供电、空调系统等故障应实施以下步骤：

（一）发生火灾、水灾时关闭机房外的供电总闸，必要时关闭计算机中心所有机器设备和电源。

（二）启用灭火设备进行灭火，并打火警电话 119。

（三）全力保护重要的数据备份，并转移到安全地点。

（四）尽量保护好火灾现场，协助有关方面勘察分析火灾发生的原因、造成的损失、提出防范和整改措施。

（五）供电故障按照以下步骤操作：

1.突发性停电时，关闭不影响业务正常运行的所有用电设备以减轻 UPS 载荷。

2.有发电机的机构立即使用发电机供电以防 UPS 电能耗尽。

3.供电线路出现问题，及时联系电力部门尽快恢复供电。

4.空调系统停机时：

（1）值班人员应立即通知相关部门协助解决。

（2）关闭不影响业务正常运行的所有用电设备以减少热量散发。

（3）密切监视设备运行状况以防设备过热而损坏。

（六）对发生突发性事件造成的损失、原因等做好记录，经部门负责人、单位领导审阅后，向本行领导或上级主管部门全面汇报。

第十二条 信息科技部人员对出现的问题作认真记录,填写《应急事件登记表》。

第十三条 所有问题解决之后形成的文档，均要在本部门内传阅，或在本部门的会议上传达，建立故障恢复数据库，共同学习故障的解决方法和预防措施。

第四章 协调人员及联系方式

第十四条 列出相关服务和支持单位人员联系方式，以确保在最短时间内对系统进行恢复。

|  |  |  |  |
| --- | --- | --- | --- |
| 公司名称 | 联系人 | 联系方式 | 备注 |
|  |  |  |  |
| 华际 | 左宁军 | 13770661591 | 小型机维护 |
|  |  |  |  |

第五章 应急预防

第十五条 信息科技部的应急预案只针对于各种突发事件的处理，各单位的工作重点就是积极预防各种可能发生的问题，力争把问题消灭在萌芽状态，同时，对于本规定中提及的各种问题要定时进行演练，确保在出现问题时有条不紊地排除故障，具体要求如下：

（一）计算机系统应急处置领导小组应召集相关人员熟悉本预案中提及的各种急方案，做到熟练掌握本部门范围内的软硬件故障检查、修复技能，每年进行一次预案演练。

（二）信息科技部要对系统变更进行详细记录，对配置参数调整前后的数据进行详细登记，对于系统配置、参数调整出现的问题可予以及时恢复。

（三）信息科技部要对全部软件的安装介质，说明文档妥善保管，对系统每次更新、安装新程序之后要及时做好备份工作，同时妥善保管备份介质。

第六章 责任追究及处罚

第十六条 突发事件处置结束后，总行应组织相关部门人员对事件的原因及全过程进行调查，根据对有关人员的责任调查结果，视情节轻重程度，追究相关人员的责任。可分别采取经济处罚、行政处分乃至移送司法机关处理等处罚措施。

第十七条 小组成员未按照相关规定履行相关职责的，依法给予行政处分；构成犯罪的，移交司法机关、依法追究刑事责任。

第十八条 对突发事件应急管理工中作出突出贡献的成员，应予以表彰和奖励。

第七章 附则

第十九条 本预案由xxx银行信息科技部负责解释和修订，并根据我行实际情况进行修订。

第二十条 本预案自发布之日起施行。

附件：应急事件登记表

附件

**应急事件登记表**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 系统名称 | |  |  |  | 日期 |  | 年 | 月 | 日 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | **事件上报审批** | | |  |  |  |
| 上报人 | | |  |  | 上报时间 | |  |  |  |
|  |  | |  |  |  | |  |  |  |
| 协调人 | | |  |  | 信息发布时间 | |  |  |  |
|  |  | |  |  |  | |  |  |  |
| 技术批准人 | | |  |  | 技术批准时间 | |  |  |  |
|  |  | |  |  |  | |  |  |  |
| 业务批准人 | | |  |  | 业务批准时间 | |  |  |  |
|  |  | |  |  |  | |  |  |  |
| 执行批准人 | | |  |  | 执行批准时间 | |  |  |  |
|  |  | |  |  |  | |  |  |  |
| 启动原因 | | | （本栏可为附件） | | | |  |  |  |
|  |  |  |  |  | | |  |  |  |
|  |  |  |  | **处理过程** | | |  |  |  |
| 执行处理人 | | |  |  | 执行处理时间 | |  |  |  |
|  |  | |  |  |  |  |  |  |  |
| 执行 |  | |  |  |  |  |  |  |  |
| 处理 |  | |  |  |  |  |  |  |  |
| 步骤 | （本栏可为附件） | | | | | |  |  |  |
|  |  |  |  |
|  |  |  |  |  | | |  |  |  |
|  |  |  |  | **恢复及反馈** | | |  |  |  |
| 恢复正常时间 | | |  |  | 验证人 |  |  |  |  |
|  | | |  |  |  |  |  |  |  |
| 反馈时间 | | |  |  |  |  |  |  |  |
|  | | |  |  |  |  |  |  |  |
| 备注 | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |