**xxx银行**

信息系统事件管理办法

**第一章 总 则**

第一条 为规范xxx银行(以下简称 “本行”) 信息系统事件管理工作，明确各单位在信息系统事件管理工作中的职能，有效应对信息系统各种紧急事件，保障信息系统安全、稳定、持续运行，依据《中华人民共和国计算机信息系统安全保护条例》、《商业银行信息科技风险管理指引》及省联社相关规定中关于事件管理的相关要求，特制订本办法。

第二条 信息系统事件是指影响或可能影响业务应用、系统环境、网络通信、机器设备、机房设施正常有效运行的事件。

第三条 信息系统事件可分为一般事件和紧急事件：

（一）一般事件是指可能导致较小影响或破坏的信息系统事件。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。比如：办理业务的设备发生故障等。

（二）紧急事件是指可能导致较严重影响或破坏的信息系统事件。一般性的技术故障，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。比如：通信设备问题、电信线路问题、电信线路问题、网点所用的UPS故障或UPS电池用电完结，造成网点不能正常办理业务等。

第四条 事故是指已发生的事件，对业务系统运行已经造成了一定影响，例如：主机系统或中心主交换机故障,导致全辖所有网点业务不能办理；电信线路问题,与大部分网点不能连通；总行后备电源不能正常供电,而造成主机、中心前置服务器、网络设备掉电停机；中心多台中间业务前置服务器发生故障等。事故可分为：较小影响事故，较大影响事故，重大影响事故。

（一）较小影响事故，导致单个用户的业务系统服务不可用（或服务质量下降），对整个业务系统的运行影响很小。

（二）较大影响事故，导致某个部门或某个区域用户的业务系统服务不可用（或服务质量下降）的事故。

（三）重大影响事故，导致一项或多项重要业务系统服务对其所有用户不可用（或服务质量下降）的事故。

**第二章 职责与权限**

第五条 发现事件人员职责：

本行全体员工都有责任和义务将已发现的或可疑的事件、故障和薄弱点及时报告给相关部门或人员。其职责为负责发现事件，报告事件，确认事件进展情况。在事件受理人到来处理之前，发现事件人员尽量不要改变现状。

第六条 信息科技部门IT服务台工作人员职责：

（一）负责对事件发生报告的接收；

（二）负责对事件进行记录、分析、分发；

（三）负责生产环境事故报告的接收；

（四）负责生产环境事故症状的记录和初步诊断；

（五）负责生产环境事故的初始分类，根据影响范围向不同层级报告；

（六）负责生产环境事故的一线处理（有标准解决方案的事故）；

（七）负责对被分配到其它部门的事故处理进展的跟踪；

（八）负责向客户/用户报告事故处理的进展情况；

（九）事故解决关闭后，负责事故的归档和整理，并对事故进行跟踪观察。

第七条 信息科技部门技术支持人员职责：

（一）负责对发现事件进行分析确定其紧急程度及影响级别；

（二）制定合理的事件解决方案并上报信息科技部门负责人；

（三）对发现事件依照事件解决方案实施解决；

（四）负责对已解决的安全事件进行复核；

（五）负责较小影响事故的处理；

（六）负责建立系统运维事件/事故知识库；

（七）负责生产环境事故的诊断；

（八）负责向IT服务台工作人员提供关于事故处理的标准解决方案和培训；

（九）负责向信息科技部门负责人报告较大事故及重大事故。

第八条 信息系统应急处置领导小组职责：

按《xxx银行计算机信息系统应急处置管理办法》执行。

第九条 信息科技部门负责人职责：

（一）对发现事件的紧急程度及业务影响分析结果进行审核；

（二）对制定的事件解决方案进行审核；

（三）依据事件的紧急及影响程度汇报高级管理层；

（四）负责协调本部门管理人员对已经上升至事故的事件进行事故处理；

（五）负责协调本部门管理人员对需要进行紧急变更的事故进行变更处理；

（六）对事件解决方案的实施过程进行管理与监督，保证事件及时、有效解决；

（七）负责对较大事故处理方案进行审批；

（八）负责通知事故相关人员、应急领导小组响应事故，启动应急预案；

（九）负责将重大事故上报高级管理层。

第十条 安全管理岗职责：

（一）负责接受事件报告，组织进行事件调查，分析原因、涉及范围；

（二）评估信息系统事件的严重程度，提出信息系统事件防范措施；

（三）负责事件的跟踪，判断事件是否真正解决；

（四）及时向信息科技部门负责人报告发生的重大信息系统突发事件，按应急预案快速响应，并协助相关部门及时进行处理。

**第三章 基本规定**

第十一条 IT 服务台工作人员应具有对上报事件或事故的初步分析能力，信息科技部门负责人定期组织对IT服务台工作人员的培训。

第十二条 信息科技部门应建立知识库，知识库将完整记录事件及事故的名称、详细描述、解决方案等内容。

第十三条 信息系统事件

（一）信息系统事件

1．信息系统事件发生后，事件发现人员必须通过有效途径及时向 IT 服务台工作人员报告，IT 服务台工作人员进行事件记录并在自身拥有的资源范围内解答用户技术上的问题，若有解决不了的问题，服务台会向内部技术人员或外部集成商寻求解决方案；

2．支行发生紧急事件时，除向IT服务台工作人员报告外，还需通知本单位主管领导以及受影响的单位；

3．信息系统事件要素包括：事件人、事件发生单位、事件发生时间、事件类别、事件紧急程度、事件影响范围、事件描述等。

4．系统管理人员应在日常工作中定期检查硬件设备的系统日志和硬件运行状态，发现并分析问题，及时进行故障申报和处理；并对处理结果进行归档分类。

（二）信息系统事件受理

1．IT服务台工作人员负责7×24小时受理事件；

2．IT 服务台工作人员对事件受理后，首先对事件内容进行记录、分析，然后报告技术支持人员，由其判定事件级别，并根据事件级别及时组织、指定事件处理人员，并协调事件处理人员立即解决事件；

3．如果事件无法解决，事件处理人员应负责将事件提交信息科技部门负责人。

（三）信息系统事件处理

1．事件处理人员需在接到IT服务台提交的事件单后20分钟内到达处理现场，及时处理各类事件；

2．事件处理人员接到IT服务台工作人员提交的事件后，依据事件级别及紧急程度，落实解决方案，及时解决或规避解决事件；

3．对于需要跨单位提供解决方案的事件，事件处理人员接到事件后，对事件进行判断分析，确定影响程度，及时报告信息科技部门负责人，由信息科技部门负责人组织内部事件处理人员提供解决方案；

4．对于需要技术支持单位现场提供技术支持的事件，事件处理人员提出申请，经信息科技部门负责人批准后统一向支持单位事件管理负责人提出申请，事件管理负责人要组织协调有关工作；

5．对于需要协调本行业务部门解决的事件，本行业务部门负责人需配合信息科技部门协调工作，直到事件解决；

6．对于需要通过变更解决的事件，由本行业务部门负责提出变更申请，依据《xxx银行信息系统变更管理办法》相关规定实施；

7．对于在操作、维护或应急手册中有明确操作方法的情况可以直接参照处理，无需进行变更审批；对于无明确操作方法的情况，要对解决方案组织进行必要的风险评估，并按照相关制度实施；

8．对于必须通过远程登陆方式解决的突发性紧急事件，要通过部门领导同意后进行远程技术支持。远程登陆后，支持单位事件处理人员必须双人操作；

9．发生紧急事件并需要启动应急处理时，要按照《xxx银行应急预案--业务系统》相关规定启动应急流程。

（四）信息系统事件反馈

1．对于一般事件，技术支持人员应在2天内（遇节假日在节后第一工作日内）向 IT 服务台工作人员答复事件解决情况或进展情况；

2．对于紧急事件，技术支持人员应在4小时内向IT服务台工作人员明确答复事件解决情况或进展情况；

3．信息系统事件关闭时，应反馈以下信息：

（1）事件基本信息:

a)涉及主要系统；

b)影响范围（包括业务种类、下属分支行和网点数量等，下属分支行、网点、用户）；

c)事件级别（一般事件、紧急事件）。

（2）事件处理情况包括：事件处理人员；故障实际开始时间；实际恢复时间；解决方案、实施计划及跟踪结果；最终解决程度（完全解决/临时规避解决/未解决）；

（3）事件原因；按事件原因分类（管理操作事件/产品事件/ 版本事件/第三方原因导致事件/其他事件）。

（五）信息系统事件汇总、统计、分析

1．IT 服务台工作人员要收集、跟踪事件处理情况，及时更新知识库；

2．事件负责人应编制事件简报，上报信息科技部门负责人。事件简报内容应包括评价内容。

第十四条 信息系统事故

（一）信息系统事故

1．信息系统事件或薄弱点对业务系统运行造成了一定影响后，信息系统事件处理应立即升级到信息系统事故处理；

2．支行发生事故时，事故发现人员将辖内事故通过有效途径通知本单位主管领导、IT服务台工作人员，同时通知受影响的单位；

3．信息系统事故要素包括：事故人、事故发生单位、事故发生时间、事故类别、事件影响程度、事故影响范围、事故描述等。

（二）信息系统事故受理

1．IT服务台工作人员需要7×24小时受理事故报告；

2．IT 服务台工作人员对受理的内容进行记录、初步诊断，并上报信息科技部门负责人，由其判断事故影响程度，并及时组织、指定人员处理；

3．信息科技技术人员需制定事故解决方案。

（三）信息系统事故处理

1．事故处理人员需要在IT服务台工作人员提交事故报告单后30分钟内到达处理现场，及时处理各类事故；

2．处理人员依据事故级别，落实解决方案，及时解决事故；

3．对于需要现场提供技术支持的事故，事故处理人员提出申请，经信息科技部门负责人批准后统一向事故发生单位提出申请；

4．对于需要协调本行业务部门解决的情况 ，本行信息科技部门负责人需配合事故处理人员落实本行业务部门的协调工作，直到事故解决；

5．对于事故处理过程中需要进行变更操作的，由我行业务部门负责提出变更申请，依据《xxx银行信息系统变更管理办法》相关规定实施；

6．对于在操作、维护或应急手册中有明确操作方法的情况可以直接参照处理，无需进行变更审批；对于无明确操作方法的情况，要对解决方案组织进行必要的风险评估，并按照相关制度实施。

（四）信息系统事故反馈

1．事故处理人员应根据事故影响程度定时向IT服务台工作人员汇报进展情况：

1)较小影响事故汇报周期至少为2小时；

2)较大影响或重大影响事故回报周期至少为1小时。

2．信息系统事故关闭时，应反馈以下信息：

1)基本信息：

a)涉及主要系统；

b)影响范围（包括业务种类、网点数量、网点、用户）；

c)事故级别（较小影响、较大影响、重大影响）。

2)处理情况包括：处理人员；故障实际开始时间；实际恢复时间；解决方案、实施计划及跟踪结果；最终解决程度（完全解决/ 临时规避解决）；

3)原因；按原因分类（管理操作/产品/版本/第三方/其他）。

（五）汇总统计分析

1．IT服务台工作人员要根据反馈结果及时更新知识库；

2．信息科技技术人员要收集、跟踪事故处理情况，编制简报，上报本行信息科技部门负责人。简报内容应包括评价内容。

（六）跟踪与复核

为确定变更的影响度和紧急度，以及监控事故解决进展情况和方案实施情况，同时监控变更请求执行情况，安全管理岗需要在事故整个生命周期内对其进行监控，并对关闭状态的事件或事故不定期进行复核，避免事件或事故再次发生。

**第四章 操作流程**

第十五条 信息系统事件处理流程

（一）事件发现人员发现事件之后，将发现事件及时向IT服务台工作人员报告；

（二）IT服务台工作人员负责记录/报告发现人员报告的事件；

（三）技术支持人员负责及时判断所接受的事件是否为紧急事件，并采取相应措施。

1.若为一般事件：

1)技术支持人员启动一般事件管理流程；

2)技术支持人员判断一般事件是否演变成紧急事件，若演变成紧急事件，则需转入紧急流程管理；若没有演变成紧急事件，则匹配知识库；

3)技术支持人员将该事件与知识库进行匹配。

2.若为紧急事件：

1)信息科技部门负责人启动紧急事件管理流程；

2)技术支持人员判断事件是否升级为事故，若升级为事故，则需转入事故管理流程；若没有升级为事故，则匹配知识库；

3)技术支持人员将该紧急事件与知识库进行匹配。

（四）技术支持人员查看知识库中是否存在该事件解决记录：

1．若存在解决记录，则执行变更管理操作；

2．若不存在解决记录，则由信息科技部门负责人判断是否紧急变更。

3.若需要启动紧急变更，则由信息科技部门负责人启动紧急变更；

4.若不需要启动紧急变更，则由技术支持人员启动一般变更。

（五）IT服务台工作人员负责变更后的问题管理；

（六）安全管理岗负责问题管理后续跟踪；

（七）IT服务台工作人员进行配置知识库管理、将解决问题录入问题知识库。

**第五章 附 则**

第十六条 本办法由xxx银行信息科技部负责解释和修订。

第十七条 本办法自发文之日起施行。