系统应急预案

编写人：

编写时间：2018年3月

|  |  |
| --- | --- |
| 属性 | 内容 |
| * 用户名称： | 齐鲁银行 |
| * 文档主标题： | 系统应急预案 |
| * 文档副标题： |  |
| * 文档编号： |  |
| * 版本日期： |  |
| * 制度版本 |  |
| * 作者： |  |
| * 密级： |  |

* 文档变更历史

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 修正日期 | 修正人 | 描述 |
| * V1.0 | * 2017.7 |  | * 创建 |
| * V1.1 | * 2018.3 |  | * 修订 |

* 修订内容

|  |  |
| --- | --- |
| 版本 | 修订内容 |
| V1.1 | 更新了组织架构、系统环境、联系方式 |

目 录

[一、 总则 4](#_Toc507679352)

[二、 组织架构和职责 4](#_Toc507679353)

[2.1组织架构 4](#_Toc507679356)

[2.2职责 5](#_Toc507679357)

[三、 系统环境 7](#_Toc507679358)

[3.1系统架构描述 7](#_Toc507679360)

[3.1.1物理架构 7](#_Toc507679365)

[3.1.2逻辑架构 8](#_Toc507679366)

[3.2行内系统与联盟系统关系 9](#_Toc507679367)

[3.2.1. 9](#_Toc507679369)

[3.2.2. 9](#_Toc507679370)

[3.3系统服务器信息 9](#_Toc507679371)

[四、 事件分级和策略 10](#_Toc507679372)

[4.1事件分级定义 10](#_Toc507679373)

[4.2事件应对和上报 11](#_Toc507679374)

[五、 响应和处置流程 12](#_Toc507679375)

[六、 应急通讯 14](#_Toc507679376)

# 总则

本应急预案为了保障系统在突发事件情况下，根据《齐鲁银行业务连续管理政策》和《齐鲁银行信息系统应急预案》制定，本预案对我行系统包含的范围作了相关说明，并对出现异常情况时，对我行在人员、职能、事件等级划分和相应的处置流程进行了定义。

系统根据我行系统的分类标准，归为重要业务系统，出现事件的划分最高级别可以到事件。

系统系统主要包含功能为：

系统主要涉及的主机包括：柜面无纸化系统应用服务器、柜面无纸化系统数据库服务器。

系统时效性要求较高，其恢复时间目标为：

1. 恢复时间目标
2. 恢复点目标

# 组织架构和职责

按照《齐鲁银行业务连续性管理政策》和《齐鲁银行信息系统应急预案》制定齐鲁银行系统应急处置组织架构和职责。



## 2.1组织架构

齐鲁银行系统应急处置组织架构设柜面无纸化应急领导组，其下设业务应急恢复组、IT应急恢复组和支持保障组（本预案重点描述IT应急恢复组工作流程进行定义和描述）。



## 2.2职责

IT应急恢复组

组长：葛萍

副组长：张功臣

组员：王彦、吴有文

职责：

1．组织制定系统应急预案；

2．组织实施系统应急预案的演练；

3．指挥和协调系统应急工作；

4．评估数据损失，向系统应急领导组提供受到影响范围和程度。

5．及时汇总、上报应急处置进展情况和事态发展情况。

6．负责内部信息通报和沟通；

7．监督、检查并参与事后调查分析汇总工作，形成总结报告。

系统执行小组

1．负责灾备中心系统硬件的日常运维，确保TSM备份系统、CDP异地备份系统的正常运行。

2．负责系统故障排除、系统双机切换等应急操作

3．协助配合数据恢复的相关环境准备。

4．负责新增主机硬件设备的安装调试工作。

5．负责系统软件和中间件的安装调试工作。

6．负责对系统应急操作技术手册—系统分册的整理和修改。

数据库执行小组

1．负责日常检查、维护系统数据库正常运行。

2．应急预案启动后，按照恢复操作流程进行数据库的恢复及数据验证

3．对系统数据的恢复点及丢失数据情况做出评估。

4．负责对系统应急操作技术手册—数据库分册的整理和修改。

网络执行小组

1．负责检查、维护、确保同城备份中心、天津异地数据备份中心及所有网点网络的正常运行。

2．应急预案启动后，负责网络、分支机构网络和外联网络的恢复工作，以及网络设备的故障处置工作。

应用执行小组

1．检查评估系统运行情况并提供评估报告。

2．应急预案启动后，完成系统的应用配置和恢复工作。

3．对切换后的灾备系统数据进行验证，对业务系统运行情况进行验证和确认。

4．指导、协助前台业务人员正常开展业务补录和业务运行工作。

5．检查评估受影响其他业务系统运行情况。

6．检查业务系统恢复后运行状态，根据系统运行节点决定是否进行相应的日终处理并完成对业务参数的配置。

7．负责对系统应急操作技术手册—应用分册的整理和修改。

维护支持小组

负责各分行、中心支行及所辖经营行、济南辖内各支行、总行各部门计算机设备的技术支持工作。

基础设施保障小组

1．负责检查维护同城灾备中心、天津异地数据备份中心基础设施，保障基础设备正常运行。

2．应急方案启动后，为其他执行小组提供必要的系统和数据备份介质。

3．协助灾备系统硬件设备的紧急购置和安装调试工作以及必要工具的准备。

# 系统环境



## 3.1系统架构描述



### 物理架构

生产中心：

柜面无纸化系统主要涉及的服务器包括：柜面无纸化数据库环境（192.1.7.166）、应用环境为部署在xindai集群上的虚机（192.1.7.163、164，使用165通过F5访问）。

物理架构参考图如下：





### 逻辑架构



## 3.2行内系统与联盟系统关系



### 独立部署

该系统部署于成员行，独立于联盟系统。

说明

## 3.3系统服务器信息

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 主机名 | 系统名称 | IP地址 | 厂商 | 设备型号 | 序列号 | 硬件配置 | 操作系统版本 | 外部存储 |
| paperless01 | 柜面无纸化 | 192.1.7.163 |  |  |  | 8c/32G/80G | Radhat  6.6 64bit |  |
| paperless02 | 柜面无纸化 | 192.1.7.164 |  |  |  | 8c/32G/80G | Radhat  6.6 64bit |  |
| paperlessdb | 柜面无纸化 | 192.1.7.166 |  |  |  | 8c/32G/80G | Radhat  6.6 64bit |  |

# 事件分级和策略

## 4.1事件分级定义

根据银监会《商业银行业务连续性监管指引》和《齐鲁银行信息科技系统事件处理办法》的相关要求，系统作为重要业务系统（一类系统），按照系统发生突发事件对社会和公众影响程度不同，将事件由高到低分为七个级别。分别为一级事件（特别重大运营中断事件）、二级事件（重大运营中断事件）、三级事件（较大运行中断事件）、四级事件、五级事件、六级事件、七级事件，具体事件定义如下：

（一）一级事件（特别重大运营中断事件）

1．重要信息系统服务中断、或重要数据损毁、丢失、泄露，造成经济秩序混乱或重大经济损失、影响金融稳定，或对公众利益、社会秩序、国家安全造成特别严重的损害的事件；

2．在业务时段导致一个（含）以上省（自治区、直辖市）的多家机构业务无法正常开展达3个小时（含）以上的事件；

3．在业务时段导致一家机构两个以上省（自治区、直辖市）业务无法正常开展3个小时（含）以上，或者一个省（自治区、直辖市）业务无法正常开展达6个小时（含）以上的事件；

4．业务服务时段以外，故障或事件救治未果、可能产生上述1至3类事件的事件。

（二）二级事件（重大运营中断事件）

1．重要信息系统服务中断，或重要数据损毁、丢失、泄露，对银行或客户利益造成严重损害的事件；

2．在业务时段导致一个（含）以上省（自治区、直辖市）的多家机构业务无法正常开展达半个小时（含）以上的事件；

3．在业务时段导致一家机构两个以上省（自治区、直辖市）业务无法正常开展半个小时（含）以上，或者一个省（自治区、直辖市）业务无法正常开展达3个小时（含）以上的事件；

4．业务服务时段以外，故障或事件救治未果、可能产生上述1至3类事件的事件。

（三）三级事件（较大运营中断事件）

1．重要信息系统服务中断，或重要数据损毁、丢失、泄露，对银行或客户利益造成较大损害的事件；

2．在业务时段导致一个（含）以上省（自治区、直辖市）业务无法正常开展达半个小时（含）以上的事件；

3．业务服务时段以外，故障或事件救治未果、可能产生上述1至3类事件的事件。

（四）四级事件

1．业务时段重要信息系统业务无法正常开展15（含）至30分钟的事件；

2．业务时段非重要信息系统业务无法正常开展3个小时（含）以上的事件。

3．业务服务时段以外，故障或事件救治未果、可能造成以上第2类事件的事件。

（五）五级事件

1．业务时段重要信息系统业务无法正常开展15分钟以下的事件；

2．业务时段非重要信息系统业务无法正常开展3个小时以下的事件。

3．业务服务时段以外，故障或事件救治未果、可能造成以上第2类事件的事件。

（六）六级事件

在系统运行期间，未造成信息科技系统服务中断，但对用户的正常使用造成一定不便。

（七）七级事件

在系统运行期间，未造成信息科技系统服务中断，但未能满足信息系统管理相关要求，存在一定的风险隐患的信息系统事件。

## 4.2事件应对和上报

一级事件：

系统应急领导组

科技：IT应急恢复组（分管行长、科技部负责人）

业务：业务应急恢复组（分管行长、相关业务部门负责人）

二级事件：

系统应急领导组

科技：IT应急恢复组（分管行长、科技部负责人）

业务：业务应急恢复组（分管行长、相关业务部门负责人）

三级事件：

系统应急领导组

科技：IT应急恢复组（分管行长、科技部负责人）

业务：业务应急恢复组（分管行长、相关业务部门负责人）

四级事件：

科技：IT应急恢复组（科技部负责人）

业务：业务应急恢复组（相关业务部门负责人）

五级事件：

科技：科技部负责人

六级事件

科技：科技部分管负责人

七级事件

科技：科技部分管负责人

# 响应和处置流程

当系统出现异常后，应急响应和处置流程如下流程图示意。



* 1. 当系统使用人员、科技运行维护人员等发现系统出现异常情况后，进行问题事件上报。
  2. 业务部门人员经过评估为系统问题汇报给IT应急恢复组。
  3. 科技运行维护人员发现系统出现异常后，进行评估上报给IT应急恢复组。
  4. IT应急恢复组根据事件情况，组织相关专业技术人员对事件进行分析和影响评估，并对系统恢复正常提出初步时间判断。根据恢复时间的判断认定事件等级。
  5. 根据事件认定等级为三级（含）以上事件，上报给应急领导组，由应急领导组宣布启动系统应急预案以及业务应急恢复组和支持保障组启动相关应急预案。
  6. 根据事件认定等级为四级（含）以下事件，IT应急恢复组启动系统应急预案。
  7. 启动应急预案后，由IT应急恢复组组织系统执行小组、数据库执行小组、应用执行小组等对讨论事件原因和解决方案。具体处置过程根据原因分别见系统应急操作技术手册—系统分册、系统应急操作技术手册—数据库分册、系统应急操作技术手册—应用分册。
  8. 执行解决方案并对执行结果进行验证。
  9. 系统恢复正常。
  10. 由IT应急恢复组对三级（含）以上事件进行总结并上报。对四级（含）以下事件由IT应急恢复组内部总结，并对应急预案进行总结调整和优化。

# 应急通讯

行内应急人员通讯

|  |  |  |  |
| --- | --- | --- | --- |
| 岗位 | 姓名 | 固定电话 | 手机号码 |
| 组长 | 葛萍 | 86075829 | 15588852255 |
| 副组长 | 张功臣 | 81679526 | 18653139782 |
| 成员 | 王彦 | 86075863 | 13869103812 |
| 成员 | 吴有文 | 82023974 | 13964012980 |
| 系统执行小组 | 武夺 | 86075864 | 18663729918 |
| 岳海真 | 86075864 | 13953155447 |
| 数据库执行小组 | 张瑞举 | 82023064 | 13606409923 |
| 班守峰 | 82023064 | 15866719125 |
| 网络执行小组 | 刘伟 | 82023974 | 15615517087 |
| 王冠一 | 82023974 | 18678772107 |
| 应用执行小组 | 高翔 | 81915681 | 13706419280 |
| 维护支持小组 | 张宇 | 86075855 | 13853199880 |
| 劳建彬 | 86075855 | 18653188764 |
| 基础设施执行小组 | 孙玉明 | 81915609 | 15866796312 |
| 李琛 | 82023064 | 13176447620 |

外部合作单位通讯录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **单位** | **联系人** | **联系方式** | **维护范围** |
| 1 | 人民银行 | 王爱军 | 13706416940 |  |
| 汤子国 | 13220580607 |  |
| 2 | 山东银监局 | 吴作勇 | 0531-86193805 |  |
| 3 | 济南银联 | 王玉玺 | 13905312860 |  |
| 4 | 城商行联盟 | 徐 岩 | 18660810603 | 核心和互联网业务协调人 |
| 程鸿旭 | 18678867829 |
| 5 | 聚和诚 | 李璐 | 18953106788 | Oracle\BEA |
| 6 | 浪潮 | 张国华 | 15069055558 | PC服务器 |
| 7 | 山东神码 | 吴中兴 | 13396415858 | F5 |
| 8 | IBM | 张芬琼 | 13911645760 | 小型机及存储 |
|  |  | 宋笑寒 | 18660166792 |  |
| 9 | 山东华鲁 | 许周敬 | 13335127606 | 小型机及存储 |

附件：

《系统应急操作技术手册—系统分册》

《系统应急操作技术手册—数据库分册》

《系统应急操作技术手册—应用分册》