**xxx银行**

## 业务连续性管理制度

**第一章 总则**

第一条 为规范xxx银行（以下简称“本行”）信息科技系统流程分析，识别可能影响业务连续性的过程，针对影响因素，为保持或及时恢复业务运作，保证业务的连续性，特制定本制度。

第二条 本制度适用于信息科技系统所涉及到的部门、人员及资产。

第三条 本制度所称的业务连续性管理是指本行行为有效应对重要业务运营中断事件，建设应急响应、恢复机制和管理能力框架，保障重要业务持续运营的一整套管理过程，包括策略、组织架构、方法、标准和程序。

**第二章 职责与权限**

**第一节 日常管理组织架构**

第四条董事会是本行业务连续性管理的决策机构，对业务连续性管理承担最终责任。主要职责包括：

（一）审核和批准业务连续性管理战略、政策和程序；

（二）审批经营管理层业务连续性管理职责，定期听取高级管理层关于业务连续性管理的报告，监督、评价其履职情况；

（三）审批业务连续性管理年度审计报告。

第五条 经营管理层负责执行经董事会批准的业务连续性管理政策。主要职责包括：

（一）制定并定期审查和监督执行业务连续性管理政策、程序；

（二）明确各部门业务连续性管理职责，明确报告路线，审批重要业务恢复目标和恢复策略，督促各部门履行管理职责，确保业务连续性管理体系正常运行；

（三）确保配置足够的资源保障业务连续性管理的实施。

第六条 风险管理部为本行业务连续性管理主管部门，其主要职责是：组织开展全行业务连续性管理工作，指导、评估、监督各部门的业务连续性管理工作；组织制定业务连续性计划，协调业务条线部门，汇总、确定重要业务的恢复目标和恢复策略；组织开展业务连续性计划的演练、评估与改进；开展业务连续性管理培训等。

第七条 业务连续性管理执行部门，包括业务条线部门与信息科技部。业务条线部门负责风险评估、业务影响分析，确定重要业务恢复目标和恢复策略，负责业务条线重要业务应急响应与恢复；信息科技部门负责信息技术应急响应与恢复。

第八条 业务连续性管理保障部门，包括行政办公室、人力资源部、计划财务部、合规管理部、安全保卫部等，为业务连续性日常管理提供人力、物力、财力以及安全保障和法律咨询。

第九条 各部门应当负责本部门业务连续性管理工作，制定相关规章制度，制定和执行本部门业务连续性计划，开展本部门业务连续性计划的演练、评估与改进工作。

第十条 本行审计部负责并定期开展全行业务连续性管理审计工作。

第二节 应急处置组织架构

第十一条 本行运营中断事件应急处置的组织架构，包括应急决策层、应急指挥层、应急执行层和应急保障层。

第十二条 应急决策层由本行经营管理层人员组成，负责决定应急处置重大事宜，包括：决定运营中断事件通报、对外报告和公告；批准启动总体应急预案等。

第十三条 应急指挥层由本行业务连续性管理主管部门、执行部门和保障部门负责人组成，负责运营中断事件处置应急指挥和组织协调，督导应急处置实施。

第十四条 应急执行层由本行业务连续性管理执行部门组成，负责业务条线与信息技术应急处置工作。

第十五条 应急保障层由本行业务连续性管理保障部门组成，负责应急处置所需人力、物力和财力等资源的保障，应急处置对外报告、宣告、通报和沟通与协调，以及对外媒体公关、秩序维护、安全保障、法律咨询和人员安抚等相关工作。

**第三章 业务影响分析**

第十六条 本行通过业务影响分析识别和评估业务运营中断所造成的影响和损失，明确业务连续性管理重点，根据业务重要程度实现差异化管理，确定各业务恢复优先顺序和恢复指标。本行每三年开展一次全面业务影响分析，并形成业务影响分析报告。

第十七条 作为业务的支持系统－信息科技系统的连续性需求：

（一）正常工作时间内不超过4个小时或者在正常工作时间外不超过8个小时。

（二）在中断期间，应保持信息科技业务的最低资源需求（如人员、资产等）。

第十八条 可能导致本行系统中断的事件包括：

（一）内外部资源的故障或缺失（如人员、系统或其他资产）。

（二）信息丢失或受损。

（三）外部事件（如战争、地震或台风等）。

第十九条 针对系统中断采取的措施确保系统持续性：

（一）风险转嫁，如购买保险或将风险转嫁给供应商。如与供应商签订服务协议，协议中规定在出现中断情况下，供应商应如何进行积极回应。

（二）风险控制，采取一些预防或检测措施，以避免风险的发生或及时检测。如安装自动灭火系统、敏感信息的异地备份等。

（三）制定业务连续性计划的原则是，既要节省投资和资源，又要确保业务的连续性目标达成。

（四）应采取系统恢复和双机热备处理等措施降低业务中断的可能性，并通过应急方式降低影响。

**第四章 业务连续性计划与资源建设**

第一节 业务连续性计划

第二十条 本行业务连续性计划的主要内容包括：

（一）重要业务及关联关系、业务恢复优先次序；

（二）重要业务运营所需关键资源；

（三）应急指挥和危机通讯程序；

（四）各类预案以及预案维护、管理要求；

（五）残余风险。

第二十一条 本行制定总体应急预案和重要业务专项应急预案。

第二十二条 本行重要业务及信息系统的外部供应商应建立业务连续性计划，证明其业务连续性计划的有效性，其业务恢复目标应当满足本行业务要求。

第二十三条 本行业务连续性计划应与金融同业单位、外部金融市场、金融服务平台和公共事业部门等业务连续性计划的有效衔接；同时，应当积极采取风险缓释及转移措施，有效控制由于外部机构业务连续性管理不充分可能产生的风险。

第二节 业务连续性资源建设

第二十四条 本行设立统一的运营中断事件指挥中心场所，用于应急决策、指挥与联络，指挥场所应当配置办公与通讯设备以及指挥执行文档、联系资料等。

第二十五条 本行建立符合业务连续性管理要求的备用资源，如备用业务和办公场所资源、备用信息系统运行场所资源、备用信息技术资源、备用人力资源等，以及电力、通讯、消防、安保等资源。

第二十六条 本行选择备用场地时，应当确保不会同时遭受同类型风险；应当综合分析备用场地所在地的自然环境、地区配套设施、区域经济环境、交通条件、政策环境和成本等各方面因素，以及灾难恢复所需的金融服务、通讯、设备、技术等外部服务供应商资源情况。

第二十七条 本行在建立备用业务和办公场所时，应当配备业务操作和办公所需资源，并确保其能够迅速启用。

第二十八条 本行建立灾备中心等备用信息技术资源和备用信息系统运行场所资源，并满足银监会关于数据中心相关监管要求。

第二十九条 本行确保关键岗位备份人员可用，降低关键岗位人员无法及时履职风险。

**第五章 业务连续性演练与持续改进**

第一节 业务连续性计划演练

第三十条 本行定期开展业务连续性计划演练，检验应急预案的完整性、可操作性和有效性，验证业务连续性资源的可用性，提高运营中断事件的综合处置能力。

第三十一条 本行每三年对全部重要业务开展一次业务连续性计划演练。在重大业务活动、重大社会活动等关键时点，或在关键资源发生重大变化之前，也应当开展业务连续性计划的专项演练。

第三十二条 本行将外部供应商纳入演练范围并定期开展演练；同时，积极参加金融同业单位、外部金融市场、金融服务平台和公共事业部门等组织的业务连续性计划演练，确保应急和协调措施的有效性。

第三十三条 本行对业务连续性计划的演练过程进行完整记录，及时总结、评估和改进。

第二节 业务连续性管理评估与改进

第三十四条 本行建立业务连续性管理体系持续改进机制。

第三十五条 本行每年对业务连续性管理体系的完整性、合理性、有效性组织一次自评估，或者委托第三方机构进行评估，并向经营管理层提交评估报告。

第三十六条 本行应当每年对业务连续性管理文档进行修订，内容应当包含重要业务调整、制度调整、岗位职责与人员调整等，确保文档的真实性、有效性。

第三十七条 本行在开发新业务产品上线前制定业务连续性计划并实施演练。

第三十八条 本行每年对本行业务连续性管理进行审计，每三年开展一次全面审计，发生大范围业务运营中断事件后应当及时开展专项审计。

审计的内容应当包括：业务影响分析、风险评估、恢复策略及恢复目标的合理性和完整性；业务连续性计划的完整性和可操作性；业务连续性计划演练过程及报告的真实性和有效性；业务连续性管理相关部门及人员的履职情况等。

**第六章 信息系统恢复**

第三十九条 启动恢复计划

（一）计划启动条件：规定在何种条件下启动灾难恢复计划/应急预案。

（二）灾难恢复计划的启动条件，可包括（但不限于）：信息科技系统中断超过多长时间；设施受损并且超过多长时间无法使用；科技信息部应根据所制定《xxx银行信息科技应急预案》的灾难恢复计划/应急预案特点，自行确定其它适当的标准。

（三）灾难恢复计划必备条件/前提条件：

灾难恢复计划的必备条件/前提条件：即确保灾难恢复计划有效开展、达到预期目的必备条件，包括（但不局限于）：

1．信息科技系统安全人员得到在其应急响应和恢复角色方面的培训；能够具备应急响应所需的知识、能力和技能。

2．预防性控制（如监测系统、灭火系统和消防部门的协助等）在灾难期间可以完全发挥作用。

3．计算机中心的设备，包括支持系统的部件连接在不间断电源（UPS）上，该UPS能够在电力故障期间提供较长时间的电力。

4．应用软件和数据的最新备份完整并且在离站（离线或冷备）存储设施中可用。

5．与信息科技系统有关的硬件、软件和通信供应商签订的服务协议可以支持紧急的业务流程恢复等。

第四十条 应急响应小组

本行应按照业务、功能及应急级别要求分层建立应急小组，以对信息安全事故做出及时响应。

第四十一条 报告程序

本行的全体员工均有义务及时报告信息安全事故或隐患。报告的流程为：

第一报告人为直接主管领导，第二报告人为所在部门总经理，部门总经理遇到较大事故需要向分管行领导汇报，重大事故由分管行领导需要向行长汇报，特殊事件需要与外部的联系，如当地公安局、消防局、人民银行、银监分局等。

第四十二条 初步响应

一旦发生信息安全事故，应做出及时响应，以降低事故影响，保障生命财产安全。响应时应遵循“人员安全第一”的原则。

第四十三条 分析与检测

应急响应小组相关人员应通过多种技术和程序机制来获悉安全突发事件的有关信息。

第四十四条 升级程序

（一）应急响应小组负责人应根据检测结果、相关的历史数据及经验对安全事件进行分析和评估，以确定是否符合计划的启动条件，如符合计划的启动条件则启动灾难恢复计划。

（二）应急计划启动根据灾难所影响的范围和所涉及的部门，需要相应的审批流程。对于涉及多个部门的灾难需要金融创新管理委员会负责人审批，对于涉及某一个部门的灾难恢复启动由科技信息部总经理批准，并上报金融创新管理委员会。

第四十五条 取证安排

若需取证，则应做出具体安排：

内部：相关人员应尽量保留信息安全事故的原始记录，以配合取证。

外部：若需要，则应与外部机构及时取得联系，如公安机关或保险公司。

第四十六条 公关管理

发生安全事件之后本行在公共关系管理方面的安排：总行由有关科技信息部门配合行政办公室进行。

公共关系管理方面包括：与顾客、银监局、人民银行、媒体、警察、消防和其他机构等的联系。

第四十七条 回退程序

发生安全事故之后，为了维持信息科技系统基本需求的安排。如使用其他设备临时顶替或从供应商处获得应急响应所需的设备及服务等。

第四十八条 恢复程序

（一）恢复程序：即安全事故发生之后采取相应应急预案中的恢复程序进行恢复，以在本行可容忍的中断时间内恢复正常运作，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。

（二）恢复程序的组织原则上按照相应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。

（三）各系统在制定相应应急程序时，应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。

（四）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。

**第七章 系统连续性管理**

第四十九条 测试、评审与更新

（一）测试

1．应急预案的测试：为验证应急预案的有效性，应定期或不定期地对其进行测试，检测应急预案的可操作性和有效性，在测试过程中，需要根据可操作性和有效性不断进行评审和更新。

2．测试的方法可包括：

（1）计划评审。

（2）采用中断实例讨论业务恢复的安排。

（3）供应商设备和服务测试（确保所提供的外部服务和产品符合合同的承诺）。

（4）全面演习（测试组织、成员、设备、设施和过程是否能应付中断）。

（二）评审与更新

计划的维护与更新：制定相应的维护和更新计划，分配职责，以保持灾难恢复计划持续的有效性。计划的更新一般定期进行，特殊情况下应增加更新的频次。特殊情况包括但不局限于：

1．新增重要信息资产。

2．系统大规模升级。

3．场所、设施和资源的变化。

4．适用法律法规的变更。

5．信息科技系统流程较大变更。

6．组织机构、技术发生重大变更。

7．发生重大信息安全事故。

8．本行认为有必要的其他情况。

第五十条 培训、意识及能力

（一）培训内容包括业务连续性程序培训、应急预案培训、业务流程培训。

（二）培训必须制度化，培训在应急预案发生变化、业务流程发生变化等条件下，需要进行培训。

第五十一条 计划管理

对本行建立的各种灾难恢复计划进行管理，该管理至少应满足以下两个要求：

（一）在需要启动灾难恢复计划时，可以快速获取的灾难恢复计划；

（二）因为灾难恢复计划中包含了本行的一些敏感信息，因此应妥善保管，防止未经授权的泄漏和访问。

第七章 附 则

第五十二条 本制度自通过之日起试行。

第五十三条 本制度未尽事宜，按国家有关法律、法规的规定执行；本制度如与国家日后颁布的法律、法规相抵触时，按国家有关法律、法规的规定执行，并立即修订。

第五十四条 本制度由xxx银行风险管理部负责解释和修订。