

附件 1-6

基于云计算技术的乡村综合金融服务风险应急预案

本应用按照应急处置预案，妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控系統运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。具体应急预案如下：

第一章 总则

第一条 目的

为有效预防、及时控制和消除突发事件对本应用及其支撑的业务应用造成的影响，指导和规范各类突发事件处理工作，最大程度减少突然事件对业务造成的影响，特编制本预案。本预案由建设银行海南分行主导落实。

第二条 工作原则

坚持团队协作、资源共享、快速反应的工作原则，突发事件发生后，立即按照职责分工和相关预案开展应急处置工作。

第三条 事件分类分级

（一）事件分类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等。

1. 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

2. 网络攻击事件分为拒绝服务攻击事件、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、干扰事件和其他网络攻击事件。

3. 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

4. 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

5. 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

6. 灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

（二）事件等级

按照《中国建设银行信息系统生产事件管理规程（2021年版）》中事件等级划分。

第二章 组织架构与职责

第四条 本应用应急团队由开发、运维、架构、安全、业务和其他相关团队组合建立，目标是推进稳定性建设、保障线上系统稳定运行，及时组织排除故障，跟进通报处理进展，回顾追踪遗留问题。

第五条 应急团队工作职责

（一）负责组织实施网络和信息安全突发事件应急预案，承担应急处置组织领导工作。

（二）收集、分析处置信息，及时上报监管部门。

（三）监测舆情并进行声誉风险处置。

（四）协调各部门人员、物力，维持正常工作秩序。

（五）启动和终止系统网络和信息安全突发事件应急预案。

（六）负责组织拟订网络和信息安全突发事件应急预案。

（七）网络与信息安全预警监测、风险评估控制和隐患排查整改工作。

（八）组织因突发事件引起的系统故障的诊断和恢复工作：组织协调网络与信息安全突发事件应急演练。

（九）起草突发事件应急响应工作报告。

第六条 应急团队成员

应急团队：所有人员。

应急基建团队：来自开发、运维、架构、安全的参与者。

应急业务团队：来自业务团队的参与者。

应急值班小组：负责本周的线上保障工作，人员从应急团队中抽调，一般每周轮换一次，在周会上交接，受应急常务委员会领导。

基建小组：运维、架构、安全组成的值班小组。

业务小组：各业务线组成的值班小组

应急组长：一般由运维、架构或其他业务线同事担任，负责本周整个应急值班小组的协调工作。在故障发生时做决策、组织协调排查问题的第一责任人。组长也是对外发布信息的第二责任人（当副组长没有及时发布信息的情况下）。组长同时负责该组团队成员的工作分配和协调，并考核成员的表现。

应急副组长：负责故障处理时对外发布信息，同时兼任组长的 B 角。当故障发生时且组长不能及时作出响应时，应由副组长承担组长职责。

应急组员：非组长和副组长的当周值班成员都是组员，平时组员受组长和副组长协调和安排任务。在组长和副组长

无响应的情况下,每一个组员都有义务承担组长和副组长的职责。

第三章 事件发现与报障

第七条 事件发现包括监控发现、检查发现、员工发现、外联客户发现等方式。

(一) 监控发现

组织建立覆盖基础设施、应用以及业务等多个层面的实时监控工具;业务部门应提出业务监控需求;开发单位应提出应用监控需求并主动配合实现。监控数据应按照一定原则保留,并进行分析挖掘,力争实现智能化监控,快速发现事件。

(二) 检查发现

运行单位、开发单位应建立信息系统风险检查机制,如巡检事件重检等,主动发现事件。

(三) 员工发现

员工发现业务服务异常,应按照员工响应相关规定报告,如确定为事件,一般应通过远程智能银行中心报障。

(四) 外联客户发现

对于外联客户,运营数据中心应组织建立快速、有效的技术问题报障机制和工具,实现客户的快速报障。对于重点客户,运行单位还应与客户建立定期的沟通机制,及时发现隐患。

第八条 发现事件后，应第一时间向运行单位报障，报障内容应准确，并尽可能详细。因未按要求报障导致事件影响扩大，需按照相关规定追责。

第九条 记录中如涉及客户信息、账号等敏感信息应按照信息安全管理要求进行保护。

第四章 事件处置

第十条 一、二级突发事件响应程序：应急团队发现或收到网络与信息安全突发事件报告后应立即启动应急预案，立即对网络与信息安全突发事件作出响应，做好准备，协调各方面人力、物力。

第十二条 三级突发事件应急响应程序：应急团队接到网络与信息安全突发事件报告后应立即通知相关领导，并启动相应预案，尽快恢复系统。

第十三条 四级、五级突发事件应急响应程序：应急团队接到故障报告后应立即检查故障原因，尽快恢复系统正常运行。

第五章 应急处置

第十四条 运行单位应组织预判事件的影响范围、程度、时长以及后续影响态势。对于突发事件应明确预警等级，启动对应的处置策略。根据对事件紧急程度、发展势态、潜在

危害程度的预判，参照突发事件分级标准，分为六个预警级别，其中一级预警最严重。运行单位应在事件处置过程中持续组织开展影响评估工作。

第十五条 运行单位应按照“并行排查”原则，组织开展事件原因定位，从应用、数据库、存储、网络等多个方面，同步分析排查，快速确定事件原因。

第十六条 运行单位应组织制定事件的处置方案并实施，处置过程应全程记录并展现。

（一）突发事件应以快速恢复业务服务为目标，立即启动应急处置流程。

（二）日常事件原则上应在受理后 48 小时内解决。如因客观原因无法在上述时间内解决，运行单位应组织制定发布临时保障措施和后续解决计划。

（三）处置方案应进行必要的测试。突发事件应急结束后测试单位需组织评估应急版本质量，并根据需要补充完成缺失的测试。

第十七条 运行单位应建立预警升降机制，实时向应急组织发布预警等级，针对不同预警级别制定相应的通知和处置策略。预警等级降低时，应按就高原则，仍向降级前最高预警等级对应的应急组织发布通知。

第十八条 运行单位可根据事件处置需要，组织业务部门、关键资源部门、支持保障部门以及外部单位等进行协同处置，相关单位应积极配合。

第十九条 运行单位应在事件处置后组织技术和业务验证并记录结果。对于临时处置措施，在业务恢复后，运行单位应加强系统监控，同时组织制定彻底解决方案，并根据运行情况安排实施。

第二十条 五级及以上预警的突发事件，运行单位应及时上报事件主管单位和运营数据中心。

第二十一条 外部报告机构包括人民银行、银保监会、证监会、公安部、外联单位等。对于外部报告应按照属地原则提交。

（一）突发事件

1. 技术外部报告

特别重大、非常敏感的突发事件（一般为三级及以上预警事件）的监管报告工作由事件主管单位组织。运行单位应力争在 20 分钟内完成书面报告，报事件主管单位；信息首报后，如有进展更新或信息补充，一般应在 24 小时内续报，最迟不超过 72 小时。突发事件应对处置结束或作为常态处理后，不再作为突发事件信息续报，可根据工作需要上报事件主管单位。

其他外部报告由运行单位组织，并报事件主管单位审批后提供。

2. 业务外部报告

业务部门对外报告如涉及技术相关内容，应向运行单位申请，由运行单位组织编写，并报事件主管单位审批后提供。

第六章 事件分析总结

第二十二条 运行单位应整理事件信息，组织分析事件原因、处理过程和影响，主要包括：

（一）原因分析

原因分析包括外部原因分析和内部原因分析。外部原因分析，需与外部单位沟通确定事件的原因。内部原因分析，包括由内部原因直接导致的，或由外部原因引发的内部信息系统异常的事件，应从需求分析、设计、开发、测试和运维等信息系统生命周期各环节，以及技术、方法、流程等多角度进行分析。事件原因可不唯一。

（二）处理过程分析

应分析事件报障和事件处置过程中存在的问题，如：监报告警是否全面准确、报障渠道是否规范、应急预案是否有效、处置是否及时等。

（三）影响分析

应遵循真实、客观、全面的原则，对事件的事中和事后是否带来业务影响，以及业务影响的范围、程度和时长等进行分析和确定。如发生客户投诉、媒体报道等情形，还应关注对建行声誉、消费者权益等的影响。日常事件可根据需要开展影响分析工作。

第二十三条 运行单位应组织编制并发布分析总结报告。五级及以上预警事件的分析总结报告，经事件主管单位

审批后发布。事件分析总结工作应于事件处置结束后 5 个工作日内完成。

第七章 突发事件定级

第二十四条 定级原则

（一）实事求是、客观公正。以事实为依据，以数据为支撑，严格评估，准确定级。

（二）统筹组织、分级审批。运行单位统一组织事件等级和责任单位初定，根据事件等级报相应单位审批

第二十五条 定级流程

（一）初定

1. 运行单位应根据事件分析结果和突发事件等级划分标准，一般在事件分析总结工作结束后的 5 个工作日内，组织完成突发事件等级和责任单位初定。责任单位可不唯一。

2. 初定责任单位对初定结果如有异议，应在初定工作结束后 2 个工作日内向事件主管单位提交申述报告，申请复议。

（二）审批

对于初定为五级及以上的突发事件，事件等级和责任单位初定结果应报事件主管单位审批。对于初定为三级及以上的突发事件，事件主管单位应报有权机构审批。

（三）发布

运行单位应在事件等级和责任单位确定后发布认定结果。

（四）调整

事件定级结果发布后一般不做调整，若事件的影响发生较大变化，可根据需要重新开展突发事件定级工作。

第八章 突发事件责任处理

第二十六条

（一）责任处理包括责任单位处理和责任人处理。内部原因导致的突发事件须进行责任处理；日常事件一般不处理，对于存在重大隐患的日常事件，事件主管单位也可组织责任处理。

（二）主观多次违反规章制度、事件通报、风险提示等要求的，应从严处理。

（三）下列情形之一，导致的突发事件，可从轻处理：

1. 在产品引进、架构决策等过程中，已充分揭示风险、隐患，考虑收益和风险平衡因素，决定接受风险，且决策程序合规。

2. 需求、设计、开发、测试及运维人员主动发现与安全运行相关问题、隐患，及时整改或其责任范围内无法解决，但及时向有关部门揭示了风险，并督促其解决，同时能够提供相关事项的签报、便函、会议纪要等以及其它正式的、可核查的依据。

3. 针对网络和应用系统等恶意攻击行为，已采取业界通用的安全防控措施，且在应急、恢复过程中无失职行为。

4. 在网络系统设计、实施中已充分考虑冗余和备份情况下，对于相互备份的运营商线路同时发生大面积中断后不能及时修复导致的突发事件，已经要求相关运营商做好线路保障，并在合同等法律文件中规定租用线路中断的恢复时间或相应罚责，或者运营商已出具责任承担证明。

5. 供应商的硬件或软件产品（含应用软件）存在不可预知问题或异常而发生突发事件，在硬件或软件维护、故障应急处置等过程中运维人员已尽职尽责，且能提供有关可核查依据。

6. 针对创新类、探索类产品，在需求、设计、开发、测试、投产、运维流程中不存在主观问题，且积极采取有效措施应急处置和关闭风险敞口。

7 对决策、需求、设计、开发、测试、投产、应急和运维过程中有关工作人员已按规定履行职责。

第二十七条 下列责任处理方式，可以单独使用，也可以合并使用。

（一）责任单位处理方式

责任单位处理方式可视情节轻重，采用合规约谈、通报批评、纳入内控评价、暂停业务等方式。

1. 合规约谈。责任单位主要负责人进行口头汇报、书面检查等。

2. 通报批评。在一定范围内对责任单位进行通报批评。

3. 纳入内控评价。依据相关规定对责任单位扣减考核分值或依据合同扣减合同金额。

4. 暂停业务。根据事件严重程度，责令责任单位风险较大的应用暂停投产。

（二）责任人处理方式

责任人处理方式可视情节轻重，采用合规约谈、公开通报、减发绩效工资、行政处分等方式。

1. 合规约谈。责任单位以谈话方式对相关责任人进行教育批评。

2. 公开通报。责任单位在辖内对相关责任人进行通报批评。

3. 减发绩效工资。可视情节严重情况按照绩效管理相关规定扣减责任人绩效。

4. 行政处分。违规性质、情节或影响较重的，按照员工违规处理相关规定及程序对责任人给予行政处分。

第二十八条 突发事件定级工作结束后，根据突发事件等级和责任单位认定结果，开展突发事件责任处理工作。

（一）三级及以上突发事件处理程序

由事件主管单位组织对责任单位和责任人进行责任处理，按照处理方式提出初步处理意见，报有权机构审议，通过后对相关单位和人员进行责任处理。

（二）四级、五级突发事件处理程序

1. 责任单位处理

事件主管单位组织对责任单位进行责任处理。

责任单位对处理结果如有异议,应在收到结果 2 个工作日内向事件主管单位提出书面复议。

2. 责任人处理

责任单位应在突发事件定级结束后的 10 个工作日内启动内部责任处理工作,确定责任人和处理方式,并报备事件主管单位。责任单位依据辖内责任处理细则,进行责任处理。

(三) 六级突发事件处理程序

六级突发事件的责任单位和责任人的责任处理程序,与四级、五级突发事件处理程序一致。

(四) 从轻处理程序

经认定属于从轻处理的,三级及以上突发事件须经有权机构批准,三级以下突发事件经事件主管单位批准,可从轻处理。

(五) 重新责任处理

如发生突发事件等级调整、责任单位变化等情况,可根据需要重新开展事件责任处理工作。

第九章 预案培训、演练和更新

第二十九条 金融科技部组织应急处理相关人员进行应急演练培训。培训内容包括信息安全法规标准、信息安全预案编制风险评估、事件分析处置、容灾备份、处置流程、处置方法等,不断提高人员的风险防范意识和应急处置能力。

第三十条 金融科技部每年至少组织一次应急预案演练，把应急演练工作制度化、规范化。通过应急演练工作提高实战能力，验证应急组织的协调能力、应急预案的正确性、应急流程的合理性以及应急资源的有效性，并不断完善应急预案。

第三十一条 应急演练工作应在不影响业务正常运行的前提下开展，演练场景应包括操作系统故障、软件故障、网络故障、存储故障、硬件故障。演练前应做好前期准备工作，制定完善的应急演练计划、应急演练方案和步骤。演练结束后应及时分析演练过程中暴露出的问题、总结演练经验、编制演练报告并进行备案。

