征信信息安全事件应急处置方案

一、总则

为贯彻落实《中国人民银行关于进一步加强征信信息安全管理的通知〉的通知》（银发〔2018〕102 号）文件精神，切实加强我公司征信信息运行安全与信息安全的防范，做好应对征信信息安全突发公共事件的应急处置工作，进一步提高预防和控制征信信息安全突发事件的能力和水平，最大限度地减轻或消除征信信息安全突发事件的危害和影响，确保征信信息安全，特制定本应急处置方案。

二、应急组织机构及职责

成立征信信息安全事件应急处置领导小组，负责领导、组织和协调公司征信信息安全突发事件的应急保障工作。

领导小组成员：

组长：副总经理

副组长：综合部经理

成员：评审部总监、市场部总监、客服部经理、财务部经理、合规部总监

三、工作原则

（一）积极防御、综合防范

立足安全防护，加强预警，重点保护征信信息安全；从预

防、监控、应急处理、应急保障和打击不法行为等环节，在管理、技术、宣传等方面，采取多种措施，充分发挥各方面的作用，构筑征信信息安全保障体系。

（二）明确责任、分级负责

按照“分级管理、逐级负责”和“谁主管谁负责、谁使用谁负责”的原则，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。切实加强对从业人员的全员征信合规性教育培训，进一步提高从业人员的征信信息安全意识。

（三）统一处置、确保安全

定期对征信管理工作开展检查，因违规查询、非法提供、违规使用以及信息泄漏、盗用、滥用、倒卖等问题引发的征信风险和安全事件，均应遵循“统一指挥、及时响应、依法处置”的原则，对征信信息安全漏洞和隐患进行及时整改。

（四）科学决策，快速反应

加强技术储备，规范应急处置措施和操作流程，征信信息安全突发公共事件发生时，要快速反应，及时获取准确信息，跟踪研判，及时报告，果断决策，迅速处理，最大限度地减少危害和影响。

四、预防预警

（一）完善征信信息安全突发公共事件监测、预测和预警

制度

加强对征信信息安全突发事件和可能引起突发征信信息安全突发公共事件的有关信息的收集、分析、判断和持续监测。当检查到有征信信息安全突发事件发生或可能发生时，应及时对发生事件或可能发生事件进行调查核实、保存相关证据，并立即向应急领导小组报告。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施建议等。

若发现下列情况应及时向应急领导小组报告：利用征信信息从事违法犯罪活动；征信信息系统通信和资源使用异常；征信信息系统瘫痪，应用服务中断或数据篡改、丢失；其他影响征信信息安全的信息。

（二）设定征信信息安全等级保护，实行征信信息安全风险评估

通过相关设备实时监控征信信息安全状况。征信信息系统建设要充分考虑抗毁性和灾难恢复，制定并不断完善征信信息安全应急处理预案。针对征信信息的突发性、大规模安全事件，建立制度优化、程序化的处理流程。

（三）做好服务器及数据中心的数据备份及登记工作，建立灾难性数据恢复机制

一旦发生征信信息安全事件，立即启动应急预案，采取应

急处置措施，判定事件危害程度，并立即将情况向有关领导报告。在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

五、处置流程

（一）预案启动

在发生征信信息安全事件后，应尽最大可能迅速收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围和评估事件带来的影响和损害，一旦确认为征信信息安全事件后，立即将事件上报应急处置领导小组并着手处置。

（二）应急处理

1.电源断电

（1）查明故障原因。

（2）检查 UPS 是否正常供电。

（3）汇报相关领导，确认供电恢复时间。

（4）备份服务器数据、交换机配置。

（5）通知网信办进行电源维修，做好事件记录。

（6）必要时请示应急处置领导小组，主动关闭服务器、交换机、存储等设备，以免设备损坏或数据损失。

2.局域网中断紧急处理措施

（1）信息安全负责人立即判断故障节点，查明故障原因，

及时汇报应急处置领导小组。

（2）若是专线故障，及时通知网络运营商抢修。

（3）若是路由器、交换机等设备故障，应立即从将备用设备取出接上，并调试畅通。

（4）若是路由器、交换机等配置文件损坏，应迅速按照要求重新配置，并调试畅通。

（5）汇报应急处置领导小组，做好事件记录。

3.光缆线路故障

（1）立即联系光纤熔接人员携带尾纤等辅助材料，及时熔接连通。

（2）检查并做好备用光缆或备用芯的跳线工作，随时切换到备用网络。

（3）做好事件记录，及时上报。

4.计算机病毒爆发

（1）关闭计算机病毒爆发网段上联端口。

（2）隔离中病毒计算机。

（3）关闭中病毒计算机上联端口。

（4）根据病毒特征使用专用工具进行查杀。

（5）系统损坏计算机在备份其数据后，进行重装。

（6）通过专用工具对网络进行清查。

（7）做好事件记录，及时上报。

5.服务器设备故障

（1）主要服务器应做多个数据备份。

（2）如能自行恢复，则立即用备件替换受损部件，如：电源损坏更换备用电源，硬盘损坏更换备用硬盘，网卡、主板损坏启用备用服务器。

（3）若数据库崩溃应立即启用备用系统。并检查备用服务器启用情况。

（4）对主机系统进行维修并做数据恢复。

（5）如不能恢复，立即联系系统集成商，要求派维护人员前来维修。

（6）汇报应急处置领导小组，做好事件记录。

6.黑客攻击事件

（1）若通过入侵监测系统发现有黑客进行攻击，立即通知系统集成商和维保单位处理。

（2）将被攻击的服务器等设备从网络中隔离出来。

（3）及时恢复重建被攻击或被破坏的系统

（4）记录事件，及时上报，若事态严重，应及时向信息化主管部门和公安部门报警。

7.数据库安全事件

（1）平时应对数据库系统做多个备份。

（2）发生数据库数据丢失、受损、篡改、泄露等安全事件时，信息安全人员应查明原因，按照情况采取相应措施：如更改数据库密码，修复错误受损数据。

（3）如果数据库崩溃，信息安全人员应立即启用备用系统，并向应急处置领导小组报告；在备用系统运行期间，信息安全人员应对主机系统进行维修并作数据恢复。

（4）做好事件记录，及时上报。

8.发生自然灾害后的紧急措施

（1）遇到重大雷暴天气，可能对机房设备造成损害时，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，恢复计算机网络工作。

（2）确认灾害不会造成人身伤害后，尽快将网络恢复正常，若有设备、数据损坏，及时使用备用设备或备份数据。

（3）及时核实、报损，并将详细情况向应急处置领导小组汇报。

9.关键人员不在岗的紧急处置措施

（1）对于关键岗位平时应做好人员储备，确保一项工作有两人能够操作。对于关键账户和密码进行密封保存。

（2）一旦发生征信信息系统安全事件，关键人员不在岗且

联系不上或 1 小时内不能到达机房的情况，首先应向领导小组汇报情况。

（3）经应急处置领导小组批准后，请求系统集成商技术支援。

（4）做好事件记录。

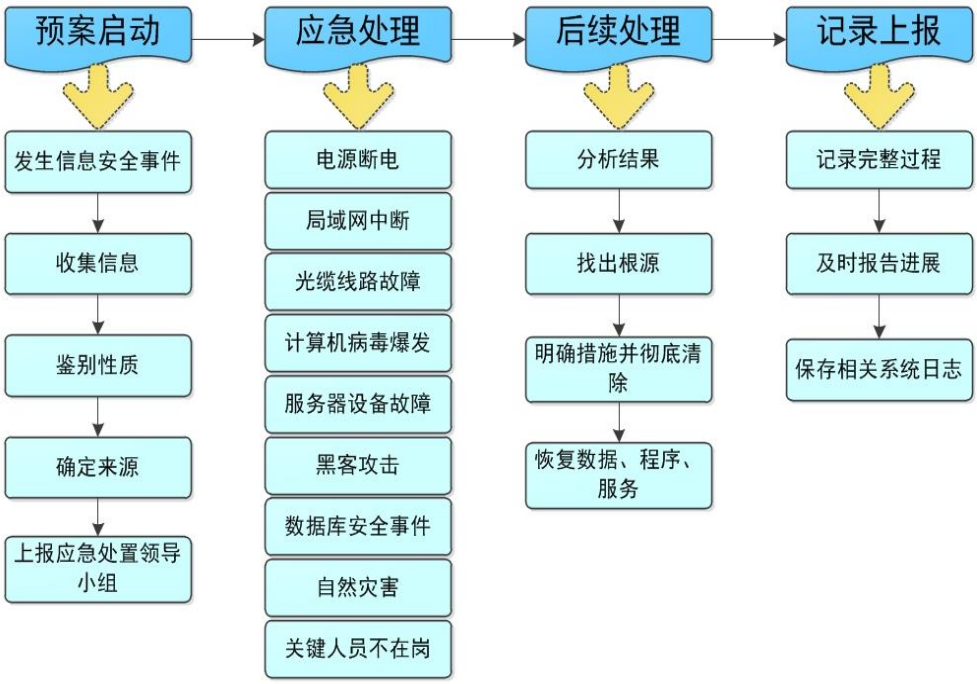
（三）后续处理

征信信息安全事件应急处置以后，应及时采取行动，抑制其影响的进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。安全事件被抑制之后，通过对有关事件或行为的分析结果，找出其根源，明确相应的补救措施并彻底清除。在确保安全事件解决后，要及时清理系统、恢复数据、程序、服务，恢复工作应避免出现误操作导致数据丢失。

（四）记录上报

征信信息安全事件发生时，应及时向征信信息应急处置工作组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

（五）征信信息安全事件应急处置流程图



六、保障措施

（一）应急设备保障

征信信息系统建设应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在征信信息安全突发公共事件发生时，报应急处置领导小组同意后，由应急工作组负责统一调用。

（二）数据保障

征信信息系统应建立容灾备份系统和相关工作机制，保证重要数据在遭到破坏后，可紧急恢复。各容灾备份系统应具有一定的兼容性，在特殊情况下各系统间可互为备份。

（三）组织管理

将征信管理纳入重要的工作议事日程，统筹规划，不断加强对从业人员在征信法律知识和规章制度方面的学习和培训，严格执行《征信业管理条例》《个人信用信息基础数据库管理暂行办法》等法规、规章及征信相关制度，使大家正确理解征信相关制度及要求，提高征信人员业务素质及处理征信问题的能力，依法合规操作，确保征信业务持续健康发展。

七、附则

本制度自发布之日起执行。