安徽国元信托有限责任公司文件

皖国信字〔2019〕164 号　　签发人：许植

关于印发《安徽国元信托有限责任公司信息系统应急处置预案》等两项制度的通知

各部门：

根据监管要求，结合公司业务实际，经总裁办公会审议通过，现将《安徽国元信托有限责任公司信息系统应急处置预案》、《安徽国元信托有限责任公司移动存储介质管理规定》予以印发，请遵照执行。

特此通知。

2019 年 8 月 1 日

抄送：公司领导

安徽国元信托有限责任公司
信息系统应急处置预案

第一章 总　则

第一条　为提高应对信息系统在运行过程中出现的各种突发事件的应急处置能力，有效预防和最大程度地降低信息系统各类突发事件的危害和影响，保障信息系统安全、稳定运行，根据国家《信息安全事件分类分级指南》、《信息技术、安全技术、信息安全事件管理指南》、《银行业重要信息系统突发事件应急管理规范（试行）》及有关法律、法规的规定，结合实际，制定本处置预案。

第二条　本处置预案所称的信息系统，由计算机设备、网络设施、计算机软件等组成。

第三条　信息系统突发事件分为网络攻击事件、信息破坏事件、信息内容安全事件、网络故障事件、软件系统故障事件、灾难性事情、其他事件等八类事件。

（一）网络攻击事件：通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的事件。

（二）信息破坏事件：通过网络或其他技术手段，造成信息

系统中的数据被篡改、假冒、泄漏等而导致的事件。

（三）信息内容安全事件：利用信息网络发布、传播危害国家安全、社会稳定和公共利益的不良信息内容的事件。

（四）网络故障事件：因电信、网络设备等原因造成大部分网络线路中断，用户无法登录信息系统的事件。

（五）服务器故障事件：因系统服务器故障而导致的信息系统无法运行的事件。

（六）软件故障事件：因系统软件或应用软件故障而导致的信息系统无法运行的事件。

（七）灾害性事件：因不可抗力对信息系统造成物理破坏而导致的事件。

（八）其他突发事件：不能归为以上七个基本分类，并可能造成信息系统异常或对信息系统当前运行造成潜在危害的事件。

第四条 按照造成信息系统的中断运行时间，将信息系统突发事件级别划分为一般（IV 级）、较大（III 级）、重大（II 级）、特别重大（I 级）。

（一）一般（IV 级）：信息系统发生可能中断运行 2 小时以内的故障；

（二）较大（III 级）：信息系统发生可能中断运行 2 小时以上、12 小时以内的故障；

（三）重大（II 级）：信息系统发生可能中断运行 12 小时以上、24 小时以内的故障；

（四）特别重大（I 级）：信息系统发生可能中断运行 24 小时以上的故障。

第二章 组织机构和工作职责

第五条 公司组建应急团队，在发生信息系统突发事件时，能够做到及时实施专项应急处置工作。应急团队应包括应急领导小组、应急执行小组、支持保障小组。

第六条 应急领导小组由公司分管信息科技的高级管理人员任应急领导小组组长，各部门的负责人为应急领导小组成员，其职责是：

1、负责信息系统突发事件的应急指挥、组织协调和过程控制；

2、宣布重大应急响应状态的降级或解除；

3、向公司高级管理层报告应急处置进展情况和总结报告。

第七条 应急执行小组由公司信息科技部门组成，对应急领导小组负责，其职责是：

1、实施信息系统突发事件的具体应急处置工作；

2、对信息系统突发事件业务影响情况进行分析和评估；

3、收集分析信息系统突发事件应急处置过程中的数据信息和日志；

4、向应急领导小组报告应急处置进展情况和事态发展情况。

第八条 支持保障小组由人事部门、财务部门、合规管理部门、风险管理部门、内审部门、纪检监察部门、行政事务部门、

战略研发部门、客户管理部门、固有业务部门、信托业务部门等派员组成，对应急领导小组负责，其职责是：

1、提供应急所需人力和物力等资源保障；

2、做好对受影响客户的解释和安抚工作；

3、做好秩序维护、安全保障、法律咨询和支援等工作；

4、建立与电力、通讯、公安和消防等相关外部机构的应急协调机制和应急联动机制；

5、其他为降低事件负面影响或损失提供的应急支持保障等。

第三章 预防与预警机制

第九条 应急执行小组针对各种可能发生的信息系统突发事件，建立和完善预测预警机制。

第十条 预警信息分为外部预警信息和内部预警信息两类。外部预警信息指信息系统外突发的可能需要通信保障、安全防范，或可能对信息系统产生重大影响的事件警报。内部预警信息指信息系统网内的事故征兆或局部信息系统突发事故可能对其他或整个网络造成重大影响的事件警报。

第十一条 应急执行小组要加强对信息系统的日常监测工作。监测的内容主要包括：

（一）局域网通讯性能与流量；

（二）网络设备和安全设备的操作记录、网络访问记录；

（三）服务器性能、数据库性能、应用系统性能等运行状态，以及存储状态等；

（四）服务器操作系统、数据库安全审计记录、业务系统安全审计记录；

（五）计算机漏洞公告、网络漏洞扫描报告；

（六）病毒公告、防病毒系统报告；

（七）其他可能影响信息系统的预警内容。

第十二条 应急执行小组获得外部重大预警信息或通过监测获得内部预警信息后，应对预警信息加以分析，按照早发现、早报告、早处置的原则，对可能演变为严重事件的情况，部署相应的应对措施，通知支持保障小组做好预防和保障应急工作的各项准备工作，并及时报告应急领导小组和风险管理部门。

第四章 应急响应程序

第十三条 信息系统使用部门或人员发现信息系统突发事件后，应及时报告应急执行小组。应急执行小组及时组织相关人员查找故障原因，在短时间内依据故障情形和修复时间进行初步判别，确定故障分类级别，较大（III 级）及其以上的突发事件应报告应急领导小组和风险管理部门。

第十四条 根据不同的事件以及事件的级别，采取相应措施进行应急处理。突发事件处理过程中，可以根据需要调整故障级别。

（一）网络攻击事件应急预案：

1、当发现网络被非法入侵、网页内容被篡改，应用服务器的数据被非法拷贝、修改、删除，或有黑客正在进行攻击等现象

时，使用者或管理者应断开网络，并立即报告应急执行小组。

2、立即切断受攻击计算机和网络的物理连接，封锁或删除被攻破的登录账号，阻断可疑用户进入网络的通道，并及时清理系统、恢复数据和程序，尽快将系统和网络恢复正常。

3、受攻击计算机的设置、账号、口令要及时更改，同时加强监控，随时注意异常情况。

4、如果能追查到攻击者的相关信息，可以对其发出警告，在警告无效的情况下，可以采取进一步的行动，乃至采取法律手段。

（二）信息破坏事件应急预案：

1、当发现信息被篡改、假冒、泄漏等事件时，信息系统使用部门或个人应立即通知应急执行小组。

2、通过跟踪应用程序、查看数据库安全审计记录和业务系统安全审计记录查找信息被破坏的原因和相关责任人。

3、提出修正错误方案和措施，进行相应处理。

（三）信息内容安全事件应急预案：

1、当发现不良信息或网络病毒时，系统使用人员立即断开网线，终止不良信息或网络病毒传播，并报告应急执行小组。

2、根据情况通告局域网内所有计算机用户，隔离网络，指导各计算机操作人员进行杀毒处理、清除不良信息，直至网络处于安全状态。

（四）网络故障事件应急预案：

1、发生网络故障事件后，系统使用人员应及时报告应急执行小组。

2、及时查清网络故障位置和原因，确定是线路故障还是设备故障，并采取相应措施予以解决。

3、不能确定故障的解决时间或解决故障的时间属较大（III级）及其以上的，应报告应急领导小组和风险管理部门。

（五）服务器故障应急预案：

1、服务器故障后，应立即确定故障设备及故障原因，并通知相关厂商提供服务。

2、根据服务器修复和恢复系统所需时间，应急执行小组决定是否启用备份设备。

3、如启用备份设备，在服务器故障排除后，在确保不影响正常业务工作的前提下，利用网络空闲时期替换备用设备。如不启用备份设备，应积极配合相关厂商解决服务器故障事件。

（六）软件故障事件应急预案：

1、发生计算机软件系统故障后，系统使用人员应立即保存数据，停止该计算机的业务操作，并将情况报告应急执行小组，不得擅自进行处理。

2、应急执行小组应立刻派出技术人员进行处理，必要情况下，通知各业务部门停止业务操作和对系统数据进行备份。

3、组织有关人员在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功后，利用备份数据恢复丢失的数据。

（七）灾害性事件应急预案：

1、一旦发生灾害性事件，应急执行小组每一位成员都应有责任在第一时间进入机房抢救服务器及存储设备。

2、及时对服务器及存储设备的损坏程序进行评估。如服务器损坏或存储设备损坏无法使用，立即联系相关厂商，进入维保服务程序。

3、根据服务器或存储设备修复和恢复系统所需时间，由应急执行小组决定是否启用备份设备。

（八）其他突发事件应急预案：应急执行小组立刻派出技术人员进入现场，制定相应措施，根据实际情况灵活处理，并按要求报告应急领导小组，较大（III 级）及其以上的突发事件应报告应急领导小组和风险管理部门。

第五章 后期工作

第十五条 故障排除后，应急执行小组向支持保障小组发出故障解除、系统恢复正常运行通知，支持保障小组向各部门传达通知。

第十六条 系统恢复运行后，相关操作人员对故障发生前所进行过的业务操作进行检查，核对业务数据是否正确或有无丢失，不正确或有丢失的应马上更正或补录，确保数据的正确和完整。对在故障期间采用手工受理的事项，应及时在系统中补充完善。

第十七条 故障排除后，应急执行小组填写《突发安全事件

记录表》，详细记录信息系统应急事件的整个经过和处理过程。

第十八条 应急领导小组组织有关人员及有关技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，总结经验教训，完善信息系统应急处置预案，整改信息系统存在的隐患。

第六章 应急保障

第十九条 应急执行小组应做好系统数据的备份工作，保证重要数据在受到破坏后可紧急恢复。预留一定数量的网络硬件设备和服务器，用于预防或应对信息系统突发事件。

第二十条 公司应建立长效的人员保障机制，确保人员能够胜任应急处置工作。在人员保障方面应达到以下要求：

1、确保应急处置人员具备应急工作必要的技术资质，定期组织人员培训以满足应急处置的要求，并通过应急演练，保证应急处置人员的熟练度；

2、确保主、备岗机制的落实；

3、确保主、备岗人员定期进行互换；

4、避免一人兼过多的岗位。

第二十一条 公司应建立有效的技术保障机制，确保在应急响应过程中不会因技术能力缺乏而导致应急处置中断或延长应急处置时间。在技术保障方面应达到以下要求：

1、建立应急事件预警平台，确保及时发现应急事件，并及时通知有关人员启动应急响应；

2、明确相关厂商的技术支持服务水平，确保应急处置过程中相关厂商能够提供及时有效的技术支持。

第二十二条 公司应采取必要的通讯保障措施，确保应急响应通讯及时有效。在通讯保障方面应达到以下要求：

1、适时更新各级应急管理机构联络人和联络方式；

2、建立多种通讯渠道，避免单一通讯风险，并明确各通讯渠道使用的优先顺序。

第二十三条 强化信息安全宣传教育，提高信息安全防御意识。每年至少组织开展一次全公司范围内的信息网络安全培训，提高全公司员工信息安全防范意识和能力。

第七章 附 则

第二十四条 本预案由信息科技部门负责修订和解释。

第二十五条 本预案经公司总裁办公会审议批准后，自发布之日起施行。

第二十六条 原《安徽国元信托有限公司信息系统应急处置预案》在本制度施行之日起废止。