CFCA 移动证书服务平台应急处置预案

为提高应对移动证书服务系统在运行过程中出现的各种突发事件的应急处理能力，有效预防和最大程度地降低移动证书服务系统各类突发事件的危害和影响，保障移动证书服务系统安全、稳定运行，《信息技术、安全技术、信息安全事件管理指南》及有关法律、法规的规定，结合实际，制定本处理预案。

- 应急处理措施指南：

一、客户处反馈疑似高风险事件

（1） 客户经理定期回访客户，密切关注客户使用产品的情况。

（2） 当有客户反馈有疑似产品技术漏洞出现时，客户经理应及时向产品团队反馈，以便产品团队开展后续工作。

（3） 产品团队在接到客户经理反馈的情况后，应及时与客户联系，了解相关情况，制定下一步计划。

（4） 产品团队应针对客户反馈的情况，对客户描述的具体问题进行问题排查。

（5） 若核实客户反馈的技术安全漏洞确实存在，导致客户因使用产品造成财产损失，我司应进行赔付，并为该客户重新部署一套新系统，避免上次密钥泄露的问题，保障客户的业务连续性。

二、社交平台出现疑似高风险事件

（1） 品牌部、运行部随时监视网络信息内容。

（2） 发现在网上出现移动证书产品相关的信息内容时，密切关注是否为描述产品功能缺陷、技术漏洞等，品牌部、运行部应定期向相关部门发送监视情况，以便产品团队开展后续工作。

（3） 产品团队接到反馈后，应及时核实反馈的问题的真实性，对描述的产品问题进行问题排查，并制定下一步计划。

（4） 若核实反馈的问题真是存在，产品团队应及时采取相应措施，修复产品漏洞，提高安全性。

三、定期漏洞扫描发现疑似高风险事件

（1） 信息安全服务部定期对移动证书服务系统进行漏洞扫描。

（2） 发现移动证书服务系统存在漏洞时，信息安全服务部应立即向产

品团队报告，以便产品团队开展后续工作。

（3） 产品团队对系统漏洞进行风险分析并制定系统更新计划。

- 风险定级

级别	级别定义	级别描述	应对措施
三级	较大	极少数个体客户	对少数客户赔付、重新部署移动证书服务系统
二级	重大	系统漏洞	通知客户关闭移动证书服务、对大面积客户赔付、系统升级
一级	特别重大	破坏性风险	停止移动证书服务

中金金融认证中心有限公司