第一篇　总则

一、编制目的

建立健全重庆市地方金融监督管理局（以下简称市金融监管局）网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，维护单位正常工作秩序。

二、编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》、《国家网络安全事件应急预案》和《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定。

三、适用范围

本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对单位正常工作造成负面影响的事件，可分为有害程序事件、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、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

四、事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（一）符合下列情形之一的，为特别重大网络安全事件：

1．重要网络和信息系统遭受特别严重的系统损失，造成系统停机，丧失业务处理能力。

2．重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对本单位业务工作和公众利益构成特别严重影响。

3．其他对单位运转和公众利益构成特别严重威胁，造成特别严重影响的网络安全事件。

（二）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

1．重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2．重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对本单位业务工作或公众利益构成严重威胁。

3．其他对单位运转或公众利益构成严重威胁，造成严重影响的网络安全事件。

（三）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

1．重要网络和信息系统遭受一定的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

2．重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对本单位业务工作或公众利益构成较严重威胁。

3．其他对单位运转或公众利益构成较严重威胁，造成较严重影响的网络安全事件。

（四）除上述情形外，对单位运转或公众利益构成一定威胁，造成一定影响的网络安全事件，为一般网络安全事件。

五、工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

第二篇 组织机构与职责

一、网络安全事件应急处置工作组

牵头人：办公室主任

组　员：机关各处室、发展中心主要负责人

应急处置工作组（以下简称“应急工作组”）在局网络安全工作领导小组领导下开展网络安全事件应急处置工作，主要职责为：统筹协调组织实施网络安全事件应对工作，建立健全跨处室联动处置机制，负责网络安全应急跨处室协调和组织特别重大及重大网络安全事件的预警响应与应急响应工作；配备技术支持人员，指导督促各处室、专业服务公司完成网络安全应急处置工作任务。

二、各处室职责

各处室按照职责和权限，会同发展中心与专业服务公司，负责本处室管理和使用的信息系统网络安全事件的预防、监测、报告和应急处置工作，组织较大及一般网络安全事件的预警响应与应急响应工作。各处室指定信息系统管理人员为系统联络员，联络应急工作组的工作。发展中心按照信息化外包服务协议提供技术服务。

第三篇 监测与预警

一、预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

二、预警监测

应急工作组各处室组员按照“谁主管谁负责、谁使用谁负责”的要求，组织信息系统管理人员、发展中心及专业服务公司对本处室管理和使用的信息系统开展网络日常维护和

安全监测工作。各处室将重要监测信息报应急工作组，应急工作组组织开展跨处室的网络安全信息共享。

三、预警研判和发布

各处室组织对监测信息进行研判，根据研判情况发布黄色及以下预警，认为需要立即采取防范措施的，应当及时会同发展中心和专业服务公司响应。对可能发生特别重大、重大网络安全事件的信息及时向应急工作组报告。应急工作组对上报的网络安全事件组织研判，确定网络安全事件预警等级，并发布橙色及以上预警信息并组织响应。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布处室等。

四、预警响应

（一）红色预警响应

1．应急工作组组织预警响应工作，联系专家和有关专业机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急处置方案，协调组织资源调度和处室联动的各项准备工作。

2．应急工作组将有关重要事项及时通报局网络安全工作领导小组，以及市委网信办、市网安总队等职能部门，协调相关单位开展应急处置和风险控制工作。

3．各信息系统管理人员实行巡网工作制度，并保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，会同发展中心与专业技术服务公司开展风险评估、应急处置准备和风险控制工作，重要情况报应急工作组。

4．专业服务机构保持联络畅通，经常性检查设备、软件工具等，确保处于正常状态。

（二）橙色预警响应

1．应急工作组组织预警响应工作，指导相关处室做好风险评估、应急处置准备和风险控制工作。

2．各处室及时将事态发展情况报应急工作组。应急工作组密切关注事态发展，有关重大事项及时通报局网络安全工作领导小组，以及市委网信办、市网安总队等职能部门。

3．专业服务机构保持联络畅通，检查设备、软件工具等，确保处于正常状态。

（三）黄色预警响应

1．各处室组织预警响应工作，会同发展中心与专业服务机构处理安全隐患，做好应急准备和风险控制工作。

2．各处室及时将事态发展情况报应急工作组。

（四）蓝色预警响应

各处室启动应急预案，会同发展中心与专业服务机构开展预警响应。

五、预警解除

（一）红色预警解除

应急工作组根据实际情况决定解除预警，及时发布预警解除信息。

（二）橙色预警解除

应急工作组根据实际情况决定解除预警，及时发布预警解除信息。

（三）黄色预警解除

事件发生处室根据实际情况决定解除预警，报应急工作组同意后发布预警解除信息。

（四）蓝色预警解除

事件发生处室根据实际情况决定解除预警。

第四篇　应急处置

一、事件报告

网络安全事件发生后，各有关处室立即组织研判网络安全事件等级，同时组织先期处置，控制事态，消除隐患，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急工作组，根据需要报告局网络安全工作领导小组，应急工作组立即组织研判并实施对应等级的应急响应。

二、应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I级为最高响应级别。

（一）Ⅰ级响应

属特别重大网络安全事件的，及时启动I级响应，局网络安全工作领导小组履行应急处置工作的统一领导、指挥、协调职责。

有关处室跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急工作组，应急工作组将有关重大事项及时通报市委网信办、市网安总队等相关部门。局网络安全工作领导小组对应对工作进行决策部署，应急工作组及有关处室负责组织实施。

（二）Ⅱ级响应

网络安全事件的Ⅱ级响应，由应急工作组根据事件的性质和情况确定。

1．事件发生处室进入应急状态，应急工作组指导相关处室按照应急预案做好处置工作。

2．处室将事态发展变化情况报应急工作组，应急工作组将有关重大事项及时通报局网络安全工作领导小组，以及市委网信办、市网安总队等职能部门。

3．处置中需要其它技术支撑队伍配合和支持的，应急工作组予以协调。

4．其它处室根据应急工作组的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

（三）Ⅲ级响应

网络安全事件的Ⅲ级响应，由相关处室根据事件的性质和情况确定。处室会同发展中心与专业服务公司做好处置响应工作，将事态发展变化情况及时报应急工作组。处置中需要其它技术支撑队伍配合和支持的，应急工作组予以协调。

（四）Ⅳ级响应

事件发生处室按预案会同发展中心与专业服务机构响应处置，记录处置情况，并及时向应急工作组汇报进展情况。

三、应急结束

（一）Ⅰ级响应结束

应急工作组提出建议，报局网络安全工作领导小组批准后结束。

（二）Ⅱ级响应结束

由应急工作组决定。

（三）Ⅲ级响应结束

由事件发生处室决定，报应急工作组同意后结束。

（四）Ⅳ级响应结束

由事件发生处室会同发展中心与专业服务机构决定。

第五篇 调查与评估

特别重大与重大网络安全事件由应急工作组组织有关处室、发展中心和专业机构进行调查处理和总结评估，并按程序上报。较大及一般网络安全事件由事件发生处室自行组织调查处理和总结评估，并将网络安全事件相关总结调查报告报应急工作组。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。

第六篇 预防工作

一、日常管理

各处室按职责会同发展中心与专业服务机构做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

二、演练

办公室组织各处室定期进行演练，检验和完善预案，提高实战能力。每年至少组织一次预案演练，并将演练情况报市委网信办。

三、宣传

办公室应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防

和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

四、培训

办公室要定期组织领导干部和有关人员接受网络安全知识和应急预案培训，提高防范意识及技能。

五、重要活动期间的预防措施

在国家、全市重要活动、会议期间，各处室要加强网络安全事件的防范和应急响应，认真落实市委网信办、市网安总队等部门的工作要求，采取有效的技术和管理手段确保网络安全。应急工作组统筹协调网络安全保障工作，各处室安排专人加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持24小时电话畅通，及时发现和处置网络安全事件隐患。

第七篇 保障措施

一、机构和人员

各处室要落实网络安全应急工作责任制，把责任落实到具体岗位和个人，并建立健全应急工作机制。

二、技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。购买网络安全企业必要技术服务、决策咨询和安全服务智力支持，发展中心配备必要的网络安全专业技术人才，加强与市里网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。

三、专家队伍

与市里网络安全应急专家组建立工作联系机制，为我局网络安全事件的预防和处置提供技术咨询和决策建议。

四、社会资源

与教育科研机构、企事业单位、协会加强联系，汇集网络安全技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

五、基础平台

主动对接市委网信办网络安全应急基础平台和管理平台，做到早发现、早预警、早响应，提高应急处置能力。

六、物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

七、经费保障

办公室为网络安全事件应急处置提供必要的资金保障。利用现有政策和资金渠道，支

持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、软硬件物资保障等工作开展。

第八章 附则

一、预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由办公室负责。

二、预案解释

本预案由办公室负责解释。

三、预案实施时间

本预案自印发之日起实施。