重庆市机关事务管理局网络信息安全应急预案

为保证信息系统安全，加强和完善网络与信息安全应急管理措施，层层落实责任，有效预防、及时控制和最大限度地消除网络信息安全突发事件的危害和影响，确保信息系统和网络的通畅运行，结合实际，特制定本应急预案。

一、总则

（一）工作目标

保障信息的合法性、完整性、准确性，保障网络、计算机、相关配套设备设施及系统运行环境的安全，其中重点维护网络系统、业务系统、基础数据库服务器及网站的安全。

（二）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》《互联网信息服务管理办法》《计算机病毒防治管理办法》等相关法规和文件精神，制定本预案。

（三）基本原则

1.预防为主。根据《计算机信息安全管理规定》要求，建立、健全计算机信息安全管理制度，有效预防网络与信息安全事故的发生。

2.分级负责。按照“谁主管谁负责，谁运营谁负责”的原则，建立和完善安全责任制。各相关处室应积极支持和协助应急处置工作。

3.果断处置。一旦发生网络与信息安全事故，应迅速反应，及时启动应急处置预案，尽最大力量减少损失，尽快恢复网络与系统运行。

（四）适用范围

本预案适用于重庆市机关事务管理局。

二、组织体系

成立局网络与信息安全领导小组，为网络与信息安全应急处置的组织协调机构。

1.局网络与信息安全领导小组由局副局长邓清华担任组长， 成员由办公室、安全保卫处负责人及相关人员组成。负责局网络与信息安全应急响应工作的整体规划、组织协调和决策指挥。

2.网络与信息安全领导小组下设办公室，由局办公室主任叶道顺担任。办公室职责：负责和处理局网络与信息安全领导小组日常工作，检查督促局网络与信息安全领导小组决定事项的落实。负责局网络与信息安全应急预案的管理，指导督促重要信息系统应急预案的修订和完善，检查落实预案执行情况。指导全局应对网络与信息安全突发公共事件的预案演习、宣传培训、督促应急保障体系建设。

三、预防预警

（一）信息监测与报告

1.按照“早发现、早报告、早处置”的原则，加强对局系统有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发事件时，按规定及时向应急领导小组报告，初次报告最迟不得超过1小时，重特大的网络与信息安全突发公共事件实行态势进程报告和日报告制度。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等。

2.建立网络与信息安全报告制度。发现下列情况时应及时向局网络与信息安全领导小组报告：利用网络从事违法犯罪活动的情况；网络或信息系统通信和资源使用异常，网络和信息系统瘫痪，应用服务中断或数据篡改，丢失等情况；网络恐怖活动的嫌疑情况和预警信息；其他影响网络与信息安全的信息。

（二）预警处理与发布

1.对于可能发生或已经发生的网络与信息安全突发公共事件，立即采取措施控制事态，并向局网络与信息安全领导小组汇报情况。

2.局网络与信息安全领导小组接到报告后，应迅速召开领导小组会议，研究确定网络与信息安全突发公共事件的等级，根据具体情况启动相应的应急预案，并向相关部门进行汇报。

四、应急预案

（一）网站、网页出现非法言论时的应急预案

1.网站、网页由负责网站维护的管理员随时监控信息内容。

2.发现在网上出现非法信息时，网站管理员立即向局网络与信息安全领导小组办公室通报情况，并作好记录。清理非法信息，采取必要的安全防范措施，将网站、网页重新投入使用；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

3.网站管理员应妥善保存有关记录、日志或审计记录，将有关情况向局网络与信息安全领导小组办公室汇报，并及时追查非法信息来源。

4.事态严重的，立即向局网络与信息安全领导小组组长报告，并向相关部门进行汇报。

（二）黑客攻击或软件系统遭破坏性攻击时的应急预案

1.重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日的备份，并将它们保存于安全处。

2.当管理员通过入侵监测系统发现有黑客正在进行攻击时，应立即向局网络与信息安全领导小组办公室报告。软件遭破坏性攻击（包括严重病毒）时要将系统停止运行。

3.管理员首先要将被攻击（或病毒感染）的服务器等设备从网络中隔离出来，保护现场，并同时向局网络与信息安全领导小组办公室报告情况。

4.局网络与信息安全领导小组办公室负责恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。

5.事态严重的，立即向局网络与信息安全领导小组组长报告，并向相关部门进行汇报。

（三）数据库发生故障时的应急预案

1.主要数据库系统应定时进行数据库备份。

2.一旦数据库崩溃，管理员应立即进行数据及系统修复，修复困难的，要及时向相关部门汇报情况，以取得相应的技术支持。

3.在此情况下无法修复的，应向局网络与信息安全领导小组办公室报告，在征得许可的情况下，可立即向软硬件提供商请求支援。

4.在取得相应技术支援也无法修复的，应及时向局网络与信息安全领导小组组长报告，在征得许可、并可在业务操作弥补的情况下，由日常信息安全岗人员利用最近备份的数据进行恢复。

（四）设备安全发生故障时的应急预案

1.小型机、服务器等关键设备损坏后，管理员应立即向局网络与信息安全领导小组办公室报告。

2.网络安全岗负责人员立即查明原因。

3.如果能够自行恢复，应立即用备件替换受损部件。

4.如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

5.如果设备一时不能修复，应向局网络与信息安全领导小组汇报，并告知各处室（单位），暂缓上传上报数据，直到故障排除设备恢复正常使用。

（五）内部局域网故障中断时的应急预案

1.局办公室平时应准备好网络备用设备，存放在指定的位置。

2.局域网中断后，网络安全岗负责人员应立即判断故障节点，查明故障原因，并向日常应急办公室汇报。

3.如属线路故障，应重新安装线路。

4.如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

5.如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

6.如有必要，应向局网络与信息安全领导小组办公室汇报。

（六）广域网外部线路中断时的应急预案

1.广域网线路中断后，管理员应向局网络与信息安全领导小组办公室报告。

2.网络安全岗负责人员接到报告后，应迅速判断故障节点，查明故障原因。

3.如属可即时恢复范围，由网络安全人员立即予以恢复。

4.如属运营商管辖范围，应立即与运营商的维护部门联系，要求尽快修复。

5.如果恢复时间预计超过两小时，应立即向局网络与信息安全领导小组办公室汇报。经同意后，应通知各处室（单位）暂缓上传上报数据。

（七）外部电中断后的应急预案

1.外部电中断后，值班室应立即向管理员汇报情况。

2.如因局内线路故障，由办公室通知维修人员迅速恢复。

3.如果是局外部的原因，由办公室立即与供电局联系，请供电局迅速恢复供电；如果供电局告知需长时间停电，应做如下安排：

（1）预计停电2小时以内，由UPS供电；

（2）预计停电2-4小时，关掉非关键设备，确保各主机、路由器、交换机供电；

（3）预计停电超过4小时，白天工作时间关键设备运行，晚上所有设备停机。

（八）设备房发生火灾时的应急预案

1.一旦设备房发生火灾，应遵循下列原则：首先保证人员安全；其次保证关键设备、数据安全；第三保证一般设备安全。

2.人员灭火和疏散的程序是：值班人员应首先切断所有电源，同时通过119电话报警。值班人员戴好防护设备，从最近的位置取出灭火器进行灭火，其他人员按照预先确定的路线，迅速从设备房中有序撤出。

五、应急响应

（一）先期处置

1.当发生网络与信息安全突发公共事件时，值班人员应做好先期应急处置工作，立即采取措施控制事态，同时向局网络与信息安全领导小组办公室报告。

2.办公室在接到网络与信息安全突发公共事件发生或可能发生的信息后，应立即向局网络与信息安全领导小组汇报，并加强与有关方面的联系，做好启动本预案的各项准备工作。

（二）应急指挥

预案启动后，要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。

（三）应急支援

预案启动后，立即成立由局网络与信息安全领导小组领导带队的应急响应先遣小组，督促、指导和协调处置工作。并根据事态的发展和处置工作需要，及时增派专家小组，调动必需的物资、设备，支援应急工作。

（四）信息处理

1.应对事件进行动态监测、评估，将事件的性质、危害程度和损失情况及处置工作等情况，及时报告，不得隐瞒、缓报、谎报。

2.明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告和发布工作。

（五）应急结束

网络与信息安全突发公共事件经应急处置后，由事发单位向应局网络与信息安全领导小

组提出应急结束的建议，经批准后实施。

五、后期处置

（一）善后处理

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。

（二）调查评估

在应急处置工作结束后，局网络与信息安全领导小组办公室应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失情况，总结经验教训，写出调查评估报告，报局网络与信息安全领导小组，并根据问责制的有关规定，对有关责任人员作出处理。

六、保障措施

（一）数据保障

重要信息系统均应建立备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。

（二）应急队伍保障

按照一专多能的要求建立网络信息安全应急保障队伍。

（三）经费保障

落实网络与信息系统突发公共事件应急处置资金。

七、监督管理

（一）宣传教育

充分利用各种传播媒介及有效的形式，加强网络与信息安全突发公共事件应急和处置的有关法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高公众防范意识和应急处置能力。加强对网络与信息安全等方面的知识培训，提高防范意识及技能，指定专人负责安全技术工作，并将网络与信息安全突发公共事件的应急管理、工作流程等列为培训内容，增强应急处置工作的组织能力。

（二）责任与奖惩

网络与信息系统的管理部门要认真贯彻落实预案的各项要求与任务，建立监督检查和奖惩机制。局网络与信息安全领导小组将不定期进行检查，对各项制度、计划、方案、人员等进行实地验证。

八、本预案由局网络与信息安全领导小组办公室制定并负责解释。

九、本预案自印发之日起实施。