为建立健全本局（馆）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，根据《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》《重庆市突发事件应对条例》《重庆市网络安全事件应急预案》《重庆档案信息网安全管理办法》《重庆市档案局（馆）机房管理办法》《重庆市档案局（馆）计算机及网络安全管理办法》《重庆市档案局（馆）档案数据资源管理办法》等法律法规和相关规章制度，并结合局（馆）工作实际制定本预案。

一、工作原则

（一）坚持统一领导、分级负责；在局（馆）统一领导下，各处室协调配合，统一行动，各司其职，令行禁止，共同完成预防和应对网络安全事件的处置工作。

（二）坚持一岗双责；局（馆）及各处室领导既是本局（馆）及各处室行政管理负责人，又是所在岗位预防和处置网络安全事件责任人。

（三）坚持预防为主，预防和应急相结合；相关处室按职责做好网络安全事件日常预防管理工作，做好网络安全检查、隐患排查、风险评估和容灾备份，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，提高应对能力。

（四）坚持谁主管谁负责、谁运行谁负责。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。

二、组织机构与职责

（一）成立重庆市档案局（馆）网络安全事件应急处置领导小组。组长由局（馆）长担任 ，副组长由分管信息技术处的副局（馆）长担任；各处室负责人任小组成员。主要职责：负责本部门网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。必要时成立局（馆）应急指挥组，接受市网络安全事件应急指挥部的指挥和协调。

（二）重庆市档案局（馆）网络安全事件应急处置领导小组具体工作由信息技术处承担。主要职责：做好本单位网络和信息系统安全监测；管理培训网络安全应急技术支撑队伍和网络安全事件应急处置的技术支撑工作；与上级网络安全管理部门沟通协调。

三、监测与预警

（一）预警监测

信息技术处组织对本单位建设运行的网络和信息系统开展网络安全监测工作，及时将网络安全隐患报局（馆）网络安全事件应急处置领导小组。

（二）预警研判

局（馆）网络安全事件应急处置领导小组组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时处置，对可能发生较大及以上网络安全事件的信息及时向市网络安全应急办公室报告。

（三）预警响应

1．红色预警响应

在市网络安全应急办公室组织指导下响应国家网络安全应急办公室红色预警，开展应急处置或准备、风险评估和控制工作。

2．橙色预警响应

响应市网络安全应急办公室橙色预警，局（馆）应急指挥组实行24小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急处置力量开展应急处置或准备、风险评估和控制工作，重要情况报市网络安全应急办公室。

3．黄色预警响应

局（馆）应急指挥组启动应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作,及时将事态发展情况报市网络安全应急办公室。

4．蓝色预警响应

局（馆）应急指挥组启动应急预案，组织开展预警响应工作。

四、应急处置

（一）事件报告

网络安全事件发生后，应立即启动应急预案，实施处置并及时报送信息。局（馆）网络安全事件应急处置领导小组立即组织先期处置，控制事态，消除隐患，同时组织研判，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、较大网络安全事件的，立即报告市网络安全应急办公室。

（二）应急响应

1．Ⅰ级响应

由市网络安全应急办公室组织实施。

2．Ⅱ级响应

（1）局（馆）应急指挥组进入应急状态，24小时值班，在市指挥部的统一领导、指挥、协调下，负责本部门应急处置工作或支援保障工作。

（2）全面了解本单位主管范围的网络和信息系统是否受到事件的波及或影响，并及时将事态发展变化情况和处置情况报市网络安全应急办公室。

（3）根据事件发生原因，有针对性地采取措施，备份数据、保护设备、排查隐患，恢复受破坏的网络和信息系统正常运行。

（4）协调配合引发的其他突发事件的应急处置。

3．Ⅲ级响应

（1）局（馆）应急指挥组进入应急状态，按照相关应急预案做好应急处置工作。

（2）及时将事态发展变化情况报市网络安全应急办公室。

（3）处置中需要其他区县（自治县）、部门和市网络安全应急技术支撑队伍配合和支持的，商市网络安全应急办公室予以协调。

4．Ⅳ级响应

按相关预案处置实施。

5．响应结束

按相关规定执行。

（三）调查与评估

较大及以下网络安全事件由本单位组织调查处理和总结评估，其中较大网络安全事件相关总结调查报告报市网络安全应急办公室。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。

五、预防工作

（一）应急处置领导小组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，依法发布有关消息和警报。全面组织本单位各项网络安全防御、处理工作，每年至少组织一次预案演练，并将演练情况报市委网信办。将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识和技能。

（二）信息技术处牵头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和危害，提高应对网络安全事件的能力。

（三）相关处室加强对局（馆）网内计算机设备的管理，加强对局(馆)网络的使用者的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

（四）加强各类值班值勤，保持通讯畅通，及时掌握局(馆)情况，全力维护正常工作秩序。

（五）按预案落实各项物资准备。

六、网络攻击事件应急处理

（一）网站事故处理预案

1．网站值守人员及网络管理员一旦发现局（馆）网站上出现重大不良信息（或者被黑客攻击修改了网页），立刻关闭网站。

2．备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。

3．打印不良信息页面留存。

4．完全隔离出现不良信息的目录，使其不能再被访问。

5．不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行。

6．修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐

患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接。

7．全面查对HTTP日志，防火墙网络连接日志，确定该不良信息的源IP地址，如果来自局(馆)外，则立刻全面升级此次事件为最高紧急事件，向处置小组副组长汇报，视情节严重程度领导小组可决定是否向市网络安全应急办公室及公安机关报告。

8．从事故发生到处理事件的整个过程，必须保持向应急处置领导小组副组长、组长汇报、报告此次事故的发生情况、发生原因、处理过程。

（二）网络恶意攻击事故处理预案

1．出现网络恶意攻击，立刻确定该攻击来自单位内还是单位外；受攻击的设备有哪些；影响范围有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断服务器及外网的网络连接，以保护重要数据及信息。

2．如果攻击来自局（馆）外，立刻从防火墙中查出对方IP地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

3．如果攻击来自局（馆）内，立刻确定攻击源，关闭该计算机网络连接，并查找分析原因，做出相应处理。

4．从事故发生到处理事件的整个过程，必须保持向应急处置领导小组副组长、组长汇报、解释此次事故的发生情况、发生原因、处理过程。

七、责任与奖惩

网络安全事件应急处置工作实行责任追究制。相关处室及人员不按照相关规定加强网络安全预防和管理，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，视情节轻重依照《中华人民共和国公务员法》和《行政机关公务员处分条例》对相应责任人给予处分；构成犯罪的，依法追究刑事责任。