第一章　总　则

第一条　为建立健全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，依据国家网络安全事件应急的有关规定，制定本预案。

第二条　本预案所指网络安全事件是指由于人为、软硬件缺陷或故障、自然灾害等原因，对我局网络和信息系统或者其中数据造成危害，对社会造成不良影响的事件。

第三条　坚持统一指挥、密切协同、快速反应、科学处置；坚持以预防为主，预防与应急相结合；坚持“谁主管谁负责、谁运营谁负责、谁使用谁负责”等原则，充分调动各方力量，共同做好市审计局网络安全事件的预防与处置工作。

第四条　本预案适用于市审计局网络安全事件的应对工作，各区县审计局可参照本预案制定本单位网络安全事件应急预案。

第二章　管理机构及职责

第五条　市审计局成立网络安全应急办公室，在局网络安全和信息化领导小组（以下简称领导小组）的领导下开展网络安全应急工作。网络安全应急办公室设在电子数据审计处，电子数据审计处处长为网络安全应急办公室主任。

第六条　网络安全应急办公室主要职责：

（一）贯彻落实局党组决策部署，落实领导小组工作安排;

（二）向领导小组报告网络安全事件应对工作相关情况，重大事项向局党组报告；

（三）制定（完善）局网络安全事件应急预案；

（四）组织技术力量开展网络安全应急事件处置工作；

（五）开展网络安全风险评估控制、隐患排查和整改；

（六）开展网络安全事件应急预案演练。

第三章　事件分级

第七条　网络安全事件分为四级：由高到低划分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）4个级别，其中特别重大（Ⅰ级）、重大（Ⅱ级）遵循《国家网络安全事件应急预案》分级标准进行分级，较大（Ⅲ级）、一般（Ⅳ级）分级标准由我局按照严重程度、可控性和影响范围等因素确定。

第八条　符合下列情形之一的，为特别重大网络安全事件：

（一）重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力；

（二）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁；

（三）其他对国家安全、社会秩序、经济建设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。

第九条　符合下列情形之一的，为重大网络安全事件：

（一）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；

（二）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁；

（三）其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

第十条　符合下列情形之一的，为较大网络安全事件：

（一）机房、网络配线间火灾或面临火灾威胁；

（二）因中心节点断电、水害、故障失灵等，导致网络中断且5个工作日以内不能恢复正常使用；

（三）因数据丢失或系统故障，主要信息系统5个工作日以内不能恢复正常使用；

（四）局门户网站内容被恶意篡改；

（五）病毒或木马入侵导致网络30%以上的服务器、计算机感染。

第十一条　符合下列情形之一的，为一般网络安全事件：

（一）因中心节点断电、水害、故障失灵等，导致网络中断且1个工作日以内不能恢复正常使用；

（二）因数据丢失或系统故障，主要信息系统1个工作日以内不能恢复正常使用；

（三）局门户网站被攻击导致1个工作日以上不能正常发布内容；

（四）病毒或木马入侵导致网络10%以上的服务器、计算机感染。

第四章　监测与预警

第十二条　建立网络安全事件信息监测机制，通过以下途径获取预报信息：

（一）主管部门告知的预报信息；

（二）国家通过新闻媒体公开发布的网络安全事件预警信息；

（三）各区县局上报的网络安全事件预警信息；

（四）网络与信息安全通报机制渠道接收的网络安全预警信息、事件信息；

（五）经风险评估得出的可能发生的网络安全事件；

（六）国家信息安全漏洞共享平台日常更新漏洞列表。

第十三条　按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，电子数据审计处负责局机关网络安全监测工作,办公室负责局门户网站监测工作。

第十四条　网络安全事件预警等级遵循《国家网络安全事件应急预案》的分级标准，由高

到低依次为：红色预警、橙色预警、黄色预警和蓝色预警，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。

第十五条　网络安全应急办公室通过对监测信息进行研判，对需要立即采取防范措施的，立即向领导小组报告，同时组织实施相应预防工作，并结合具体情况发布黄色及以下预警。

对可能发生重大及以上网络安全事件的信息，在报经领导小组同意后，及时向市委网信办报告。

第十六条　加强网络安全事件应急响应工作。

对网络安全主管部门发布的红色预警，应及时转发并指定专人24小时值班，应急工作全部人员保持通信联络畅通，同时组织开展应急处置或准备、风险评估和控制工作。

对网络安全主管部门发布的橙色预警，应及时转发并组织开展应急响应工作，结合实际情况及时开展风险评估、应急准备和风险控制工作。

对黄色、蓝色预警，应根据需要转发并对事态的发展进行跟踪研判，同时制定防范措施，协调开展应急处置。

上述工作的有关情况应及时报告领导小组，发现重要情况经领导小组同意后，及时向市委网信办报告。

第十七条　网络安全应急办公室应根据实际情况，报请领导小组审核后，确定是否解除经网络安全应急办公室发布的黄色、蓝色预警。

第五章　应急处置

第十八条　网络安全事件应急处置工作在网络安全应急办公室统一调度下开展。

发生较大或一般网络安全事件时，相关人员必须在1小时内向网络安全应急办公室主任报告，应急办公室主任在知晓情况后，4小时内向领导小组报告，同时组织开展应急处置工作，必要时组织外部技术专家参与。

第十九条　根据不同网络安全事件，采取针对性紧急处置措施。

（一）设备设施故障应急处置

1．机房供电中断。

（1）供电中断后，值班人员应立即告知电力维修人员，同时记录相关信息，开展原因排查；

（2）如因内部故障（线路、设备等故障），应迅速抢修恢复；

（3）如因外部原因，立即与供电单位联系，迅速恢复供电；如告知需长时间停电，应作如下安排：预计停电2小时以内，由UPS供电；预计停电2-4小时，关掉非关键设备；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。

2．服务器故障。

（1）系统管理员应立即记录相关信息，并对故障原因进行排查，如有备用服务器应立即启用；

（2）如属于软件故障，应先备份好数据，再对系统进行修复或重新安装；

（3）如属于硬件故障不能恢复的，应注意保存磁盘数据，避免反复重启，并立即与相关厂商联系维修；

（4）如设备不能及时修复，应公告各使用单位。

3．内部局域网中断。

（1）网络管理员应立即记录相关信息，迅速判断故障节点，并对故障原因进行排查；

（2）如属线路故障，应更换故障线路并调试通畅；

（3）如属路由器、交换机等网络设备故障，应立即启用备用设备，并调试通畅，然后视情况联系设备厂商报修或购买新设备；

（4）如属路由器、交换机配置文件损坏，应迅速重新配置，并调试通畅。

4．电信运营线路中断。

（1）网络管理员应立即联系电信运营商迅速排查故障节点，查明故障原因；

（2）督促电信运营商尽快恢复通信；

（3）如预计恢复时间超过两小时，应告知各使用单位暂停使用网络直到网络恢复正常。

5．机房空调非正常停机。

（1）排查停机原因，尝试再次重启空调；

（2）如空调重启无效，可先开窗、开门降温，借用普通风扇、小型柜机空调机等设备降温，在尽量保持网络畅通的情况下关闭非关键设备，同时联系厂家维修空调；

（3）空调正常运行后，开启关闭的设备和服务器，并监视房间温度达到正常要求。

（二）网络攻击、木马、病毒等应急处置

1．网络攻击事件。

（1）保护好现场，记录好相关信息，保存好系统日志等；

（2）立即通过技术手段阻止网络攻击的进一步升级，必要时可切断网络，将被攻击的服务器等设备从网络中隔离出来。若相关系统遭破坏时，停止系统运行；

（3）追查非法网络攻击来源，必要时可请信息安全机构参与分析研究。查明情况后，经领导小组同意，向市委网信办报告或向市公安部门报警；

（4）针对发现的安全问题，采取相应的安全技术进行防护，避免再次被攻击，及时恢复或重建被攻击或被破坏的系统。

2．重要系统被植入木马或间谍程序。

（1）抓取能证明被植入木马或间谍程序的界面，注意保存好相关系统日志；

（2）必要时可切断网络，将被植入木马或间谍程序的服务器等设备从网络中隔离出来；

（3）及时清除木马或间谍程序，并追查来源，必要时可请信息安全机构参与分析研究。查

明情况后，经领导小组同意，向市委网信办报告或向市公安部门报警；

（4）针对发现的安全问题，采取相应的安全技术进行防护，防止再次被植入木马或间谍程序。

3．危害系统运行的病毒暴发。

（1）将染毒计算机、服务器从网络上隔离，启用反病毒软件杀毒；

（2）当认为查杀病毒可能对服务器数据造成损害时，应对服务器数据进行备份；

（3）启用反病毒软件杀毒无效时，立即升级最新版本后查杀，仍无效时，通知反病毒软件公司或相关技术专家，提供病毒样本，寻求支持解决；

（4）确认反病毒软件有效时，应发布公告，组织全网计算机统一清查杀毒。

（三）重要信息系统安全事件紧急处置

1．局门户网站内容被恶意篡改。

（1）立即切断网站服务器与互联网的联接；

（2）抓取保存被恶意篡改内容的全部网页页面，并保存好系统日志；

（3）查找系统安全漏洞，采取进一步的安全防范措施；

（4）清除非法信息，重新加载正确信息，经检查发布无误后，联通互联网，恢复网站访问；

（5）分析追查非法信息来源，必要时可请信息安全机构参与分析研究。查明情况后，经领导小组同意，向市委网信办报告或向市公安部门报警。

2．审计管理系统故障。

（1）通过查看系统服务运行状况、分析系统运行日志等开展系统故障排查工作；

（2）如属系统配置的问题，保存好系统日志，重新配置，调试至系统正常运行；

（3）如属系统服务停止运行，根据具体情况重启数据库、中间件、应用系统等服务。同时根据日志等信息分析原因，做好系统修复；

（4）不能判断故障原因时，联系应用软件开发集成商、系统软件开发商，提出解决方案。

（四）灾害性事件紧急处置

1．机房发生火灾。

（1）火灾刚发生时，机房值班人员或身置起火现场的人员使用灭火器等扑救初期火灾，呼喊提醒同事协助，设法电话联系物业值班室（67518489）或门卫（67519108）一同处置；

（2）火灾不能及时扑灭，火势蔓延迅速，全部人员迅速撤出火灾现场，关闭机房房门，机房值班人员迅速启用机房消防联动系统实施灭火；

（3）火势已无法控制，立即拨打119报警电话，通过专业消防实施扑救。疏散周围人员迅速离开，同时关闭好办公楼其他房间门窗，以减少火灾殃及其他区域的可能性；

（4）火灾扑灭后，协助专业消防部门保护现场，配合调查起火原因，清理现场，尽可能保全设备资产和信息资源；

（5）研讨尽快恢复系统设备正常运行的最佳解决方案，做好系统恢复。

2．机房发生水害。

（1）立即清扫去除积水，加强通风，必要时应当先切断电源再行处置；

（2）需要系统停止运行再行处置的，执行相应的操作；

（3）属于空调排水系统故障造成水害，应立即维修或更换排水系统，必要时联系厂家；

（4）属于自来水造成的水害，应立即通知物业值班室（67518489）或门卫（67519108）关闭水源；

（5）确认水害消除，机房干燥后，恢复供电或恢复系统运行。

第六章　调查与评估

第二十条　网络安全事件处置完毕后，网络安全应急办公室应向领导小组报告处置情况，对发现的重要情况经领导小组同意后，向市委网信办报告。

第二十一条　网络安全事件处置完毕后，网络安全应急办公室应对应急响应工作进行分析和回顾，总结经验并部署采取适当的后续措施。

第七章　预防工作

第二十二条　国家重要活动、会议、节假日等敏感时期，网络安全应急办公室应加强排查网络安全隐患，加强网络安全值守。

第二十三条　网络安全应急办公室应定期或不定期安排应急演练，及时发现应急工作存在的问题，不断完善应急预案，提高应急处置能力。

局门户网站作为局关键信息基础设施，每年应至少开展一次网络安全应急演练，演练方案见附件。

第八章　附　则

第二十四条　本预案由电子数据审计处负责解释。

第二十五条　本预案自印发之日起执行。