巫山司发〔2022〕17号

巫山县司法局

关于印发网络与信息安全应急预案的通知

各基层司法所，机关各科室，社区矫正帮教服务中心、法律援助中心：

 现将《网络与信息安全应急预案》印发给你们。请遵照执行。

（此件公开发布）

巫山县司法局

2022年1月1日

网络与信息安全应急预案

1 总则

　　1.1编制目的

　　加强我局网络运行安全和信息安全防范能力，做好应对网络与信息安全突发公共事件的应急处置工作，提高预防和控制网络突发公共事件的能力和水平，减轻或消除网络突发公共事件的危害和影响，做好网上舆论管理和信息安全保障工作，确保网络运行安全与信息安全。

　　1.2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》《计算机病毒防治管理办法》等有关规定，制定本预案。

　　1.3工作原则

**1.3.1积极防御，综合防范。**立足安全防护，加强预警，抓好预防、监控、应急处理、应急保障等环节，在管理、技术、人才等方面采取各种措施，充分发挥各方作用，共同构筑我局网络与信息安全保障体系。

　**1.3.2明确责任，分级负责。**按照“谁主管谁负责，谁使用谁负责”的原则，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。

**1.3.3科学决策，快速反应。**加强技术储备，规范应急处置措施和操作流程，网络与信息安全突发事件发生时，要快速反应，及时获取准确信息，跟踪研判，及时报告，果断决策，迅速处理，最大限度地减少危害和影响。

1.4适用范围

本预案适用于我局发生的网络与信息安全突发事件和可能导致网络与信息安全突发事件的处置工作。

2 组织体系

　　2.1 成立网络与信息安全领导小组。组长由局长黄裕萍担任，副组长由政治处主任唐志恒担任，成员由办公室和相关科室的主要负责人组成。领导小组下设办公室，设在局办公室，由李劲松兼任办公室主任。

　　2.2领导小组的主要职责：统一领导网络与信息安全的应急工作，全面负责信息网络可能出现的各种突发事件处置工作。发生网络与信息安全突发事件时，启动本预案，领导小组办公室牵头组成应急工作小组，开展应急处置。

3 预防预警

　　3.1 安全监测与报告

　　3.1.1进一步完善网络与信息安全突发事件监测、预测和预警制度。落实工作责任制，按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引起突发事件的有关信息的收集、分析、判断和持续监测，同时定期递交网络与信息安全报告。当发现有网络与信息安全突发事件发生时，立即在第一时间向领导小组办公室报告，做到秒级响应。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建议等。

　　3.1.2发现下列情况应及时向领导小组办公室报告：利用网络从事违法犯罪活动；网络或信息系统通信和资源使用异常；网络或信息系统瘫痪，应用服务中断或数据篡改、丢失；网络恐怖活动的嫌疑和预警信息；其他影响网络与信息安全的情况。

　　3.2 预警处理与发布

　　3.2.1对可能发生或已经发生的网络与信息安全突发事件，立即采取措施，制止事件的延续、蔓延，并在1小时内进行风险评估，必要时启动相应预案，同时向领导小组办公室报告。

　　3.2.2领导小组办公室接到报告后，对可能发生或已经发生的网络与信息安全突发事件，迅速召开领导小组会议，启动本预案，研究确定处置意见。

　　3.2.3对需要向上级相关部门通报的，要及时通报，并争取支援。

4 应急响应

　　4.1 先期处置

　　当发现我局网络或信息系统（设备）受到不明攻击或恶意入侵时，值班人员应在第一时间联系服务器运营商，告知我局IP地址，运营商会根据IP地址进行断网处理。同时告知网络维护商进行修复，再向领导小组办公室报告。领导小组办公室接到报告后，应加强与有关方面的联系，掌握最新发展动态。对发生重大和有可能演变为重大的网络与信息安全突发事件，要立即报告领导小组，并做好启动本预案的各项准备工作；领导小组组长在接到报告后，要根据网络与信息安全突发事件发展情况，视情况决定是否赶赴现场指挥，组织派遣应急支援力量。

　　4.2 应急指挥

　　本预案启动后，领导小组办公室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。根据事件性质组建各类应急工作小组，开展应急处置工作，必要时，向相关部门申请应急支援。

　　4.3 信息处理

　　应急工作小组应对事件进行动态监测、评估，不得隐瞒、缓报、谎报。要做好信息分析、报告和发布工作，及时提供事件动态信息给领导小组办公室研究决策。应组织专家和有关技术人员研判各类信息，研究提出处置措施，完善应急处置计划方案。

5 后期处置

　　5.1 善后处理

　　在应急处置工作结束后，应急工作小组要迅速采取措施，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。处理后，应对系统进行查病毒、查木马等安全排查，检测是否受到攻击，梳理安全事件发生原因。做好数据统工作，对事件造成的损失和影响以及恢复重建所需的时间、费用等进行分析评估，认真制定恢复重建计划，并迅速组织实施。最后，要将善后处置的有关情况报领导小组办公室。

　　5.2 调查评估

　　应急处置工作结束后，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损失情况，总结经验教训，写出调查评估报告，报网络与信息安全领导小组。

6 保障措施

　　6.1 技术保障

　　提升网络日常防护级别，网络维护公司对服务器进行自动实时监控，每日进行人工检查，出现异常及时断网修复。每周对服务器进行漏洞扫描，及时查补漏洞。每日凌晨进行异机数据备份。聘请专业网络安全技术公司进行日常维护和全天候防护，一旦发生突发事件时，在技术上实现自动同步响应，采取断网措施。定期邀请县公安网监部门对我局网络进行检测。

　　6.2 应急装备保障

　　对于重要网络与信息系统，在系统建设时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全突发公共事件发生时，报领导小组同意后，由应急工作小组负责统一调用。

　　6.3 数据保障

　　重要信息系统均应建立容灾备份系统和相关工作机制，保证重要数据在遭到破坏后，可紧急恢复。各容灾备份系统应具有一定的兼容性，在特殊情况下各系统间可互为备份。

7 监督管理

　　7.1要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。

　　7.2建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

　　7.3调动和利用好社会力量参与我局网络和信息安全建设，对在网络与信息安全突发公共事件应急处置中作出突出贡献的集体和个人，给予表彰奖励。

8 附则

　　8.1 预案管理与更新

　　本预案由办公室负责制订、修订，报局领导审核后实施。结合信息网络发展情况和我局工作实际情况，配合相关法律法规的制定、修改和完善，适时修订本预案。

　　8.2 实施时间

　　本预案自印发之日起实施。

巫山县司法局办公室 2022年1月1日