垫江县卫生健康委员会电子公文

垫卫发〔2022〕89号

垫江县卫生健康委员会
关于印发《垫江县卫生健康委员会网络安全事件应急预案》的通知

各委属单位，委机关各科室：

根据中共垫江县委网络安全和信息化委员会办公室《关于印发<垫江县网络安全事件应急预案>（修订版）的通知》，结合实际，制定《垫江县卫生健康委员会网络安全事件应急预案》，请各委属单位认真组织实施。

垫江县卫生健康委员会

2022年5月24日

垫江县卫生健康委员会
网络安全事件应急预案
目录

8.附则

8.1 预案管理

8.2 预案解释

8.3 预案实施时间

1.总则

1.1 编制目的

响应《国家网络安全事件应急预案》《重庆市网络安全事件应急预案》和《垫江县网络安全事件应急预案》（修订版），建立健全垫江县卫生健康委员会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，保护公众利益，维护信息安全和社会稳定。

1.2 编制依据

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》《党委（党组）网络安全工作责任制实施办法》《重庆市突发事件应对条例》《重庆市突发事件总体预案》《重庆市网络安全事件应急预案》《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）和《垫江县网络安全事件应急预案》（修订版）等相关规定，制定本预案。

1.3 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，对社会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。

本预案适用于垫江县卫生健康委员会网络安全事件的应对工作。其中，有关垫江县卫生健康委员会信息内容安全事件的应对，另行制定专项预案。

1.4 事件等级

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。

（1）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，造成系统大面积瘫痪，丧失业务处理能力。

②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。

③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。

（2）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。

③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。

（3）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较大的系统损失，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较严重威胁。

③其他对国家安全、社会秩序、经济建设和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。

（4）除上述情形外，对国家安全、社会秩序、经济建设和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。

1.5 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”和属地管理的原则，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。

2.组织机构与职责

2.1 领导机构与职责

在县委网络安全和信息化委员会（以下简称“县委网信委”）的领导下，在县委网络安全和信息化委员会办公室（以下简称“县

委网信办”）指导下，成立垫江县卫生健康委员会网络安全事件应急工作领导小组（以下简称“领导小组”），接受县网络安全事件应急指挥部（以下简称“县指挥部”）的指挥和协调，负责本委一般和较大网络安全事件处置的组织指挥和协调，组长由垫江县卫生健康委员会党委书记、主任担任，副组长由垫江县卫生健康委员会副主任担任，成员由各委属单位和垫江县卫生和计划生育信息中心主要负责同志担任。

2.2 办事机构与职责

垫江县卫生健康委员会网络安全事件应急工作领导小组下设委网络安全应急办公室，设在委信息统计科，负责统筹协调组织全委网络安全事件的预防、监测、报告和应急处置工作，建立健全本部门跨机构联动处置机制。负责全系统网络安全应急跨单位协调工作和领导小组的事务性工作，组织指导全系统网络安全应急技术支撑队伍做好应急处置的技术支撑工作。办公室主任由委信息统计科负责人担任，副主任由垫江县卫生和计划生育信息中心科室负责人担任，成员由各科室负责人担任。

2.3 各委属单位职责

各委属单位根据《党委（党组）网络安全工作责任制实施办法》《网络安全工作责任制落实工作指标》等相关规定，建立健全网络安全工作责任制，成立本单位网络安全工作领导小组，明确负责网络安全工作的相关科室、机构职责、机构岗位、岗位职

责、岗位人员等，制定或修订网络安全应急预案，按照职责和权限，负责本单位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。

3.监测与预警

3.1 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。

3.2 预警监测

各委属单位按照“谁主管谁负责、谁运行谁负责”和属地管理原则，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。行业主管或监管部门组织指导做好本行业网络安全监测工作。委网络安全应急办公室统筹组织开展对县卫生健康系统内网络和信息系统的安全预警监测工作。各委属单位将重要监测信息报委网络安全应急办公室，委网络安全应急办公室组织开展跨单位的网络安全信息共享。

3.3 预警研判和发布

各委属单位组织对监测信息进行初判，认为需要立即采取防范措施的，应当及时通知有关单位做好防范，对可能发生一般及以上网络安全事件的信息按照网络安全事件报告模板格式，及时向委网络安全应急办公室报告。领导小组根据监测和报告情况组

织研判，确定和发布蓝色预警、黄色预警以及涉及多单位的预警。红色预警、橙色预警由上级网络安全应急办公室确定或发布，领导小组根据上级要求统筹抓好响应工作。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、发布机关等。

3.4 预警响应

3.4.1 红色预警响应

（1）领导小组按照县网络安全应急办公室的统一安排，组织响应市网络安全应急办公室红色预警。

（2）委网络安全应急办公室、有关单位实行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，组织指导委网络安全应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报县网络安全应急办公室和县指挥部。

（3）委网络安全应急办公室联系专家和有关单位，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工作方案，协调组织资源调度和单位联动的各项准备工作。

（4）委网络安全应急支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

（1）领导小组组织响应县网络应急办公室橙色预警。

（2）委网络安全应急办公室联系专家和有关机构，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工作方案，协调组织资源调度和单位联动的各项准备工作。及时将事态发展情况报告县网络安全应急办公室。

（3）委网络安全应急办公室、有关单位实行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，组织指导委网络安全应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报告县网络安全应急办公室和领导小组。

（4）委网络安全应急支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.3 黄色预警响应

（1）领导小组启动相应应急预案，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。

（2）委网络安全应急支撑队伍联系专家和有关机构，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工作方案，协调组织资源调度和单位联动的各项准备工作。及时将事态发展情况报告县网络安全应急办公室。

（3）委网络安全应急办公室、有关单位实行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，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报告县网络安全应急办公室和领导小组。

（4）委网络安全应急支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件等，确保处于良好状态。

3.4.4 蓝色预警响应

（1）委网络安全应急办公室在领导小组批准和统一指挥下启动相应应急预案，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。

（2）委网络安全应急办公室联系专家和有关单位，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工作方案，协调组织资源调度和单位联动的各项准备工作。及时将事态发展情况报告县网络安全应急办公室。

（3）委网络安全应急办公室，有关单位实行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，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报告县网络安全应急办公室和领导小组。

（4）委网络安全应急支撑队伍进入待命状态，针对预警信

息研究制定应对方案，检查应急车辆、设备、软件等，确保处于良好状态。

（5）有关单位根据委网络安全应急办公室发布的蓝色预警指令，组织响应相应应急预案，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。

3.5 预警解除

预警发布单位根据实际情况，确定是否解除预警，及时发布预警解除信息。

4.应急处置

4.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。有关单位立即组织先期处置，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。对网络安全事件进行初判，并立即向委网络安全应急办公室报告。

4.2 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，即分别对应红色预警、橙色预警、黄色预警和蓝色预警。I级为最高响应级别。

4.2.1 Ⅰ、Ⅱ级响应

委网络安全应急办公室组织对事件信息进行研判，属特别重

大、重大网络安全事件的，及时向领导小组报告，由领导小组向县委网信委、县指挥部安全应急办公室报告。

（1）进入应急状态

在县指挥部的统一领导、指挥、协调下，领导小组负责全系统应急处置工作或支援保障工作，领导小组成员保持24小时联络畅通，委网络安全应急办公室、各委属单位实行24小时值班，并派员参与县网络安全应急办公室相关应急工作。

（2）了解事情动态

委网络安全应急办公室立即全面了解全系统范围内的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报告县网络安全应急办公室。

（3）处置实施

①控制事态防止蔓延。在县网络安全应急办公室的统一指挥下，领导小组负责组织实施，尽快控制事态；组织、督促相关运行单位有针对性地加强防范，防止事态蔓延。

②消防隐患恢复系统。委网络安全应急办公室根据事件发生原因，有针对性的采取措施，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。必要时可依法征用单位和个人的设备和资源，并按规定给予补偿。

4.2.2 Ⅲ级响应

委网络安全应急办公室组织对事件信息进行研判，属较大网

络安全事件的，及时向领导小组报告，由领导小组向县委网信委、县指挥部提出启动Ⅲ级响应的建议，各委属单位根据领导小组发布的响应指令进入应急响应状态。

（1）启动指挥体系

①领导小组进入应急状态，履行应急处置工作的统一领导、指挥、协调职责。领导小组成员保持24小时联络畅通。委网络安全应急办公室实行24小时值班。

②有关单位进入应急状态，在领导小组的统一领导、指挥、协调下，负责本单位应急处置工作或支援保障工作，各委属单位实行24小时值班，并派员参与委网络安全应急办公室相关应急工作。

（2）掌握事件动态

①跟踪事态发展。事件发生单位及时将事态发展变化情况和处置进展情况报告委网络安全应急办公室。

②检查影响范围。有关单位立即全面了解本单位的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报告委网络安全应急办公室。

③及时通报情况。委网络安全应急办公室负责汇总上述有关情况，重大事项及时报领导小组，并通报有关单位。

（3）决策部署

领导小组组织有关单位、专家组和应急技术支撑队伍及时研

究对策意见，就应对工作进行决策部署。

（4）处置实施

①控制事态防止蔓延。委网络安全应急办公室负责组织实施，尽快控制事态；组织、督促相关运行单位有针对性地加强防范，防止事态蔓延。

②消除隐患恢复系统。委网络安全应急办公室根据事件发生原因，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的正常运行。必要时可依法征用单位或个人的设备和资源，并按照规定给予补偿。

③工作协调。各委属单位根据统一要求，按照各自渠道和工作规定，开展与上级部门或有关单位之间的协调。

④协调配合引发的其他突发事件的应急处置。对于引发或可能引发其他较大安全事件的，委网络安全应急办公室应及时按程序上报。在相关单位应急处置中，委网络安全应急办公室做好协调配合工作。

4.2.3 Ⅳ级响应

委网络安全应急办公室组织对事件信息进行研判，属一般网络安全事件的，及时向领导小组和县委网信办报告，由领导小组和县委网信办向县委网信委、县指挥部提出启动Ⅳ级响应的建议，各委属单位根据委网络安全应急办公室发布的响应指令进入应急响应状态。

（1）事件发生单位进入应急状态，按照相关应急预案做好应急处置工作。

（2）事件发生单位及时将事态发展变化情况报告委网络安全应急办公室。委网络安全应急办公室将有关重大事项及时通报相关部门。

（3）处置中需要其他部门、单位和委网络安全应急技术支撑队伍配合和支持的，委网络安全应急办公室予以协调。相关单位和委网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

（4）有关单位根据委网络安全应急办公室的通报，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的损失。

4.3 应急结束

4.3.1 Ⅰ、Ⅱ级响应结束

由预警发布单位决定，委网络安全应急办公室按照县网络安全应急办公室要求，及时通报事发单位结束应急响应状态。事发单位将事件梳理成报告，报委网络安全应急办公室。

4.3.2 Ⅲ及响应结束

由县指挥部决定结束应急响应状态，报市网络安全应急办公室。事发单位将事件梳理成报告，报委网络安全应急办公室。

4.3.3 Ⅳ级响应结束

由领导小组报告县指挥部批准后结束应急响应状态。事发单

位将事件梳理成报告，报委网络安全应急办公室。

5.调查与评估

特别重大网络安全事件由国家网络安全应急办公室组织有关部门和省（区、市）进行调查处理和总结评估。重大网络安全事件由市网络安全应急办公室组织有关部门和县进行调查处理和总结评估。较大网络安全事件由县网络安全应急办公室组织有关单位或县级部门进行调查处理和总结评估，并按照程序上报市网络安全应急办公室。一般网络安全事件由事件发生单位或垫江县卫生健康委员会自行组织调查处理和总结评估，并按程序上报县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。

6.预防工作

6.1 日常管理

各委属单位按职责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。

6.2 演练

委网络安全应急办公室协调有关单位，每年至少组织一次预案演练，检验和完善预案，提高实战能力。有重要网络和信息系统的单位原则上每年至少组织一次预案演练，并将演练情况报告委网络安全应急办公室；其余单位原则上两年至少组织一次预案演练，并将演练情况报告委网络安全应急办公室。

6.3 宣传

各委属单位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。

6.4 培训

各委属单位要将网络安全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，提高防范意识及技能。

6.5 重要敏感时期的预防措施

在国家、全市和全县重要活动、会议等重要敏感时期，各委属单位要加强网络安全事件的防范和应急响应，确保网络安全。委网络安全应急办公室统筹协调全系统网络安全保障工作，根据需要要求有关单位启动预警响应。有关单位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，重点单位、重点岗位保持24小时值班，及时发现和处置网络安全事件隐患。

7.保障措施

7.1 机构和人员

各委属单位要落实网络安全工作责任制，把责任落实到具体科室、具体岗位和人员，并建立健全应急工作机制。

7.2 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。支持网络安全企业提升应急处置能力，提供应急技术支援。按照相关规定组织评估和认定委网络安全应急技术支撑队伍。各委属单位根据本单位网络安全形势和发展态势，配备必要的网络安全专业技术人才，成立网络安全人才库，并在委网络安全应急办公室的指导支持下，加强与县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。

7.3 专家队伍

建立委网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各委属单位加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

从教育科研机构、企事业单位、社会组织中选拔网络安全人才，加强与高等院校、科研单位的合作，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对网络安全事件的能力。

7.5 基础平台

委网络安全应急办公室统筹全系统网络安全预警和能力建设，充分运用县委网信办网络安全协调指挥和态势感知平台，做到早发现、早预警、早响应，提高应急处置能力。

7.6 情报力量

县人民医院、县中医院等重点单位要加强网络安全有关情况收集能力建设，完善情报共享机制，为全系统的网络安全应急工作提供情报支撑。

7.7 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。

7.8 经费保障

各委属单位要为网络安全事件应急处置提供必要的资金保障。充分利用现有政策和资金渠道，支持本单位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、情报力量建设、技术研发、预案演练、物资保障等工作开展。

7.9 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

领导小组和县网信办对在网络安全事件应急管理工作中作出突出贡献的先进集体和个人，报县网信委研究决定后，给予表彰和奖励。

按照《网络安全法》《党委（党组）网络安全工作责任制实施办法》等有关规定，领导小组会同县委网信办对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。网络安全建设与绩效纳入审计范围。

8.附则

8.1 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。修订工作由委网络安全应急办公室负责，并报县委网信办备案。

各委属单位要根据本预案制定或修订本单位网络安全事件应急预案，做好与本预案的衔接，并委网络安全应急办公室备案。

若各委属单位负责网络安全应急处置工作的分管领导和联络人员发生变动，应及时告知委网络安全应急办公室。

8.2 预案解释

本预案由委网络安全应急办公室解释。

8.3 预案实施时间

本预案自印发之日起实施。