中共旌德县委网络安全和信息化委员会文件

旌网信办〔2021〕9号

关于印发《旌德县网络安全事件应急预案》的通知

各镇，县直各单位:

现将《旌德县网络安全事件应急预案》印发给你们，请结合实际认真组织实施。

中共旌德县委网信办

2021年6月23日

旌德县网络安全事件应急预案

为建立健全全县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，维护公共安全和社会秩序，现制订我县网络安全事件应急预案如下:

一、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。

二、事件分级

根据危害程度，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）县内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，对我县安全和稳定构成特别严重威胁。

（3）其他对我县公共安全、社会秩序、经济建设、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）县内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，对我县安全和稳定构成严重威胁。

（3）其他对我县公共安全、社会秩序、经济建设、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）县内重要网络与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，对我县安全和稳定构成较严重威胁。

（3）其他对我县公共安全、社会秩序、经济建设、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，对我县公共安全、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。

三、组织机构与职责

1.领导机构与职责

在县委网信委的领导下，县委网信办统筹协调组织全县

网络安全事件应对工作，建立健全跨部门联动处置机制，县公安局、县数据资源局、县机要局等相关部门按照职责分工负责相应网络安全事件应对工作。必要时成立县网络安全事件应急指挥部，统一领导和协调指挥特别重大网络安全事件的处置工作。

2.办事机构与职责

县网络安全应急办公室（以下简称“县网络安全应急办”）设在县委网信办，负责网络安全应急跨部门、跨地区协调工作和县网络安全事件应急指挥部的事务性工作，组织指导全县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。县公安局、县数据资源局、县机要局等单位相关业务科室负责人为联络员，联络县网络安全应急办工作。

各镇、县直各单位按照职责和权限，负责本单位、本行业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。县委网信办在县委网信委统一领导下，统筹协调组织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。

四、监测与预警

1.预警监测和分级

各镇、县直各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本镇、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。重点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。县委网信办结合实际，统筹组织开展网络和信息系统的安全监测工作。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。

2.预警响应

（1）红色预警响应

①县网络安全应急办组织预警响应工作，联系专家和有关机构，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。遇特别紧急情况，联系、协调市办争取指导支持。

②有关镇和单位网络安全应急机构实行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，重要情况及时报县网络安全应急办。

③县网络安全应急队伍进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等，确保处于良好状态。

（2）橙色预警响应

①有关镇和单位网络安全应急机构启动相应应急预案，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。

②有关镇和单位及时将事态发展情况报县网络安全应急办。县网络安全应急办密切关注事态发展，有关重大事项及时通报。

③县网络安全应急队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

（3）黄色、蓝色预警响应

有关镇和单位网络安全应急机构启动相应应急预案，指导组织开展预警响应。

五、应急处置

1.事件报告

网络安全事件发生后，事发镇和单位应立即启动应急预案，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、重大网络安全事件，立即报告县网络安全应急办。

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。I 级为最高响应级别。

（1）I 级响应

县网络安全应急办会同有关镇和单位，对事件信息进行研判，属特别重大网络安全事件的，及时向县委网信委提出启动 I 级响应的建议，经批准后成立县网络安全事件应急指挥部（以下简称应急指挥部），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。

①启动指挥体系

县网络安全应急办 24 小时值班，负责组织实施。遇到特别紧急情况，经应急指挥部的批准，由县网络安全应急办进驻涉事镇和单位，现场指挥协调。

涉事镇、单位网络安全应急机构进入应急状态，实行 24 小时值班，在应急指挥部的统一领导、协调下，负责本镇本

单位应急处置工作或支援工作，并派员参加县网络安全应急办工作。

②掌握事件动态

跟踪事态发展。事件发生镇或单位及时将事态发展变化情况和处置进展情况报县网络安全应急办。

检查影响范围。有关镇和单位立即全面了解本镇、本单位主管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县网络安全应急办。

及时通报情况。县网络安全应急办负责汇总上述有关情况，重大事项及时报县网络安全事件应急指挥部，并通报有关镇和单位。

③决策部署

县网络安全事件应急指挥部组织有关镇和单位以及专家组、应急队伍及时研究对策意见，对应对工作进行决策部署。

④处置实施

控制事态防止蔓延。有关镇和单位负责组织实施，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。

消除隐患恢复系统。有关镇和单位及时查明事件发生原因，有针对性地采取措施，备份数据、保护设备、排查隐患，恢复受破坏网络和信息系统正常运行。

请求协调。经县网络安全事件应急指挥部批准，报市网络安全应急办，请求指导支持。

（2）II 级响应

①事件发生镇或单位的网络安全应急机构进入应急状态，按照相关应急预案做好应急处置工作。

②事件发生镇或单位及时将事态发展变化情况报县网络安全应急办。县网络安全应急办将有关重大事项及时通报相关镇和单位。

③处置中需要其他有关镇、单位及县网络安全应急队伍配合和支持的，商县网络安全应急办予以协调。相关镇、单位和县网络安全应急队伍应根据各自职责，积极配合、提供支持。

④有关镇和单位根据网络安全应急办的通报，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和损失。

（3）III 级、IV 级响应

事件发生镇和单位按相关预案进行应急响应。

3.应急结束

（1）I 级响应结束

县网络安全应急办提出建议，报县网络安全事件应急指挥部批准后，及时通报有关镇和单位，并报市网络安全应急办。

（2）II 级响应结束

由事件发生镇或单位决定，报县网络安全应急办。县网络安全应急办通报相关镇和单位。

（3）III 级、IV 级响应结束

由事件发生镇或单位决定。

六、调查与评估

特别重大网络安全事件由县网络安全应急办组织有关地镇和单位进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生镇或单位自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报县网络安全应急办。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。

七、预防工作

1.日常管理

各镇、县直各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。

2.宣传培训

各镇各单位应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。将网络安全事件应急知识列为领导干部和有关人员的培训内容，提高防范意识及技能。

3.重要敏感时期的预防措施

在国家、省、市和县重要活动、会议等重要敏感时期，各镇各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。县网络安全应急办统筹协调网络安全保障工作，有关镇和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。

八、保障措施

1.机构和人员

各镇、县直各单位要按照《党委（党组）网络安全工作责任制实施细则》有关要求，落实网络安全应急工作责任制，把责任压实到具体部门、具体岗位和个人，并建立健全应急工作机制。

2.应急队伍

加强网络安全应急队伍建设，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。各镇、县直各单位应配备必要的网络安全专业技术人才，并加强与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。

3.专家队伍

县委网信办、县公安局联合组建全县网络安全专家委员会，遴选县级网络安全应急支撑服务单位，为网络安全事件的预防和处置提供技术咨询和决策建议。各镇、县直各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。

4.物资和经费保障

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。财政部门为网络安全事件应急处置提供必要的资金保障，利用现有政策

和资金渠道，支持网络安全应急队伍建设、专家队伍建设，各镇、县直各单位为网络安全应急工作提供必要的经费保障。

6.责任与奖惩

县委网信办及有关镇和单位对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给予表彰和奖励；对不按照规定制定预案，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，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。

九、附则

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。修订工作由县委网信办负责。各镇、县直各单位要根据本预案制定或修订本镇、本单位网络安全事件应急预案。

2.预案解释

本预案由县委网信办负责解释。

3.实施时间

本预案自印发之日起实施。