阳城县人民政府办公室文件

阳政办发〔2025〕23号

阳城县人民政府办公室
关于印发阳城县网络与信息安全事件
应急预案的通知

各乡(镇)人民政府,开发区管委会,县直及驻阳各有关单位,各有关企业:

《阳城县网络与信息安全事件应急预案》已经县政府同意,现印发给你们,请结合工作实际,认真抓好贯彻落实。

阳城县人民政府办公室

2025年4月14日

(此件公开发布)

阳城县网络与信息安全事件应急预案

1 总则

1.1 编制目的

建立健全网络与信息安全事件应急响应机制,提高我县应对网络与信息安全事件能力,预防和减少网络与信息安全事件造成的损失和危害,维护国家安全和社会稳定,结合我县实际,特制定本预案。

1.2 工作原则

信息化系统建设、管理与使用工作实行“谁主管谁负责,谁运营谁负责,谁使用谁负责,谁保管谁负责”。坚持统一领导,协同配合;分级负责,职责明确;防范为主,加强监控;依法管理,规范有序;快速反应,有效应对的原则。

1.3 编制依据

《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国安全生产法》《中华人民共和国突发事件应对法》《中华人民共和国计算机信息系统安全保护条例》《网络安全等级保护条例》《山西省突发事件应对条例》《晋城市网络与信息安全突发事件应急预案》《阳城县突发事件总体应急预案》《信息安全技术网络安全事件分

类分级指南》等。

1.4 适用范围

本预案适用于本县行政区域内网络与信息安全事件的预防和应对工作。另有规定的，依照其规定执行。

1.5 事件分类分级

参照《信息安全技术网络安全事件分类分级指南》(GB/T 20986—2023)，网络安全事件分为：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等10类。事件分类详情见附录8.3。

参照《信息安全技术网络安全事件分类分级指南》(GB/T 20986-2023)，网络安全事件分为4个级别：特别重大事件、重大事件、较大事件和一般事件，由高到低分别为一级、二级、三级和四级。事件分级详情见附录8.4。

2 组织体系与职责

2.1 县网络与信息安全事件应急指挥部及职责

县人民政府设立阳城县网络与信息安全事件应急指挥部(以下简称县指挥部)。

指 挥 长：县人民政府分管网络与信息工作的副县长

副指挥长：县政府办分管网络与信息工作的副主任、县委宣传部分管网络与信息工作的副部长、县数据中心主任、县应急局局长、县公安局常务副局长。

成员单位：县委办公室（县委机要保密室）、县委政法委、县委宣传部（县委网信办、县政府新闻办公室）、县政府外事办公室、县发展和改革局、县教育局、县科学技术局、县工业和信息化局、县公安局、县财政局、县交通运输局、县文化和旅游局、县应急管理局、县市场监督管理局、县数据中心、国网山西省电力公司阳城县供电公司（以下简称阳城县供电公司）、中国移动通信集团山西有限公司阳城县分公司（以下简称移动阳城分公司）、中国联合网络通信有限公司阳城县分公司（以下简称联通阳城分公司）、中国电信股份有限公司阳城分公司（以下简称电信阳城分公司）、中国铁塔晋城市分公司阳城县办事处（以下简称铁塔阳城办事处）。各成员单位分管负责人为指挥部成员。根据网信突发事件实际情况，指挥长可随时增加县直有关单位为指挥部成员单位。

主要职责：统一领导、指挥、协调全县网络与信息安全事件的应急处置工作；负责对网络与信息安全事件、预防和预警工作进行及时报告和建议；决定启动与结束网络与信息安全事件应急响应；指导全县开展网络与信息安全事件应急处置工作；批准县指挥部办公室提请审议的重要事项；负责突发事件的信息发布；分析网络与信息安全事件发生原因；组织协调网络与信息安全培训演练、总结评估、督导检查等工作。

2.2 县指挥部办公室及职责

县指挥部办公室设在县委宣传部（县委网信办）。办公室主任由县委宣传部分管网络与信息工作的副部长兼任。

主要职责：落实县指挥部指示和部署，承担县指挥部日常工作；监测汇总上报网络与信息安全事件预防和应对工作进展情况，分析研判网络与信息安全形势，做好舆情监管和引导工作，提出具体应急处置方案和措施建议；指导协调县网络与信息安全应急技术支撑队伍工作；负责协调数据安全保障体系建设，组织实施数据安全审查和监管工作；负责统筹协调全县政务大数据云平台系统及安全保障体系建设，承担安全等级保护、应急协调等相关工作；办理县指挥部交办的其他事项。

2.3 县指挥部成员单位及职责

县指挥部成员单位根据相关法律法规和各自职责，做好网络与信息安全事件日常监管和预防预警工作。事件发生时，根据职责分工承担相应的工作任务，详情见附录8.5。

本预案未列出的部门和单位，根据县指挥部指令，按照本部门、本单位职责，依法做好网络与信息安全应急相关工作。

2.4 应急工作组组成及职责

县指挥部下设综合协调组、现场抢修组、技术专家组、后勤保障组、新闻宣传组5个应急工作组，各组的设立、成员单位可根据实际情况进行调整。各应急工作组组成及职责见附录8.6。

2.5 各乡（镇）指挥部

各乡（镇）人民政府设立相应的网络与信息安全事件应急指挥部，组织和指挥本地区网络与信息安全事件的预防、监测、报告和应急处置工作。

3 预防和预警

3.1 预防

各乡(镇)人民政府、开发区管委会、县直各部门应按照“谁主管谁负责,谁运行谁负责”的要求,做好网络与信息安全事件的风险评估和隐患排查工作,加强信息安全风险评估和等级保护工作,提高信息系统自身防护能力。落实涉密防范措施,提高涉密信息和系统的监管水平。加强网络监管,提高舆情驾驭能力。制订完善相关应急管理制度,及时采取有效措施,避免和减少网络与信息安全事件的发生及其危害。

3.2 预警

3.2.1 预警分级

根据预警信息分析结果,对可能发生的网络与信息安全事件进行预警。按照事件可能造成的危害、紧急程度和发展态势,预警级别分为四级:Ⅰ级(特别严重)、Ⅱ级(严重)、Ⅲ级(较重)、Ⅳ级(一般),依次用红色、橙色、黄色和蓝色表示。

3.2.2 监测与发布

县委宣传部(网信办)、县数据中心、县公安局、县委办公室(县委机要保密室)以及各重要信息系统主管部门,各乡(镇)人民政府、开发区管委会共同承担全县网络与信息安全预警监测工作。信息系统运营单位及其主管部门要建立健全网络与信息安全事件监测、预测、预警制度,及时对网络与信息安全事件和可能引发网络与信息安全事件有关信息进行收集、分析和持续监测。

事发单位对于可能发生的网络与信息安全突发事件，应立即采取措施控制事态，及时进行风险评估并报告县指挥部。根据各级各部门监测发现的及上级有关部门通报的有关网络与信息安全预警信息，县指挥部办公室及时组织成员单位、技术支撑队伍及有关单位进行分析研判，根据问题的性质、危害程度，提出预警等级建议，明确预警的响应范围和公开程度（或保密要求），经县指挥部批准后发布预警信息并报县委县政府。

3.2.3 预警行动

根据预警信息，相关单位要对本部门网络与信息系统安全状况的监测，做好应急队伍、装备等应急处置准备工作，随时向县指挥部报告事态进展情况，县指挥部办公室及有关部门要及时跟踪了解情况。

3.2.4 预警解除

县指挥部办公室根据事件发展情况，组织有关部门、技术支撑队伍进行研判，认为网络安全隐患已消除且网络与信息系统已恢复正常运行后，提出预警解除建议，按照规定的权限和程序，经批准同意后，发布预警解除信息，并报县委县政府和上级有关部门。

4 应急响应

4.1 信息安全报告

网络与信息安全事件发生后，事发单位和监测单位立即向上级单位和事发地人民政府报告，并报送县指挥部办公室。对较大和暂时无法判明等级的突发事件，事发后30分钟内报告县人民

政府。对特别重大、重大突发事件，事发地人民政府或有关部门在获知事件发生后立即报告县委县政府和上级有关部门。

突发事件报告内容应包括时间、地点、单位名称、信息来源、事件类别、经济损失的初步评估、影响范围、事件发展态势及处置情况等。

4.2 分级响应

根据突发事件危害程度、影响范围等实际情况，应急响应分为Ⅰ级、Ⅱ级、Ⅲ级，一级为最高级别。

4.2.1 Ⅰ级响应

4.2.1.1 启动条件

当符合以下情形之一时，启动Ⅰ级应急响应：

（1）发生或暂时情况不明有可能发生较大以上网络与信息安全事件时。

（2）超出县指挥部应对能力，需上级指挥部予以协调应对的。

（3）县指挥部根据事发当时情形，经过分析研判，认为需要启动Ⅰ级应急响应的。

4.2.1.2 启动程序

事件发生后，县指挥部办公室经评估，向县指挥部提出建议，由县指挥部指挥长决定启动Ⅰ级响应。

4.2.1.3 响应措施

县指挥部组织有关力量对突发事件进行先期处置，控制事态发展。同时上报上级指挥部请求支援，开展应急处置工作。主要

处置措施如下：

(1)启动指挥体系

县指挥部进入应急状态，履行全县应急处置工作的统一领导、指挥、协调职责。县指挥部成员单位24小时值班，保持联络畅通；组织专家、技术人才研究对策，提出处置方案建议，为领导决策提供支撑。

(2)掌握事件动态

事件影响单位将事态发展变化情况和处置进展情况及时上报县指挥部办公室，县指挥部组织有关成员单位全面了解本县行政区域内的基础网络和信息系统受到事件波及或影响情况，及时汇总并上报县人民政府和上级指挥部，并通报县指挥部各成员单位。

(3)决策部署

待上级指挥部明确接管权限时，立即移交指挥权，接受上级指挥部的统一指挥，县指挥部成员单位、技术支撑队伍，积极配合开展应急救援。

(4)处置实施

控制事态，防止蔓延。县指挥部根据上级指挥部的部署或指导意见，组织事发单位及应急队伍，采取各种技术措施、管控手段，最大限度地阻止和控制事态发展；县指挥部全面启动应急机制，及时督促、指挥本县网络与信息系统运营使用管理单位有针对性地加强防范，防止事件进一步蔓延。

迅速处置，消除隐患。组织专家、应急技术力量、事发单位尽

快分析事件发生原因、特点、发展趋势，快速制定具体的解决方案，组织实施处置，对受破坏网络与信息系统及时组织恢复。

及时开展调查取证。事发单位在应急恢复过程中应尽量保留相关证据，对于人为破坏活动，公安等部门按职责分工负责组织侦查和调查工作，并及时向县指挥部办公室报告有关情况。

4.2.2 Ⅱ级响应

4.2.2.1 启动条件

当符合以下情形之一时，启动Ⅱ级应急响应：

（1）发生或暂时情况不明有可能发生一般网络与信息安全事件时。

（2）超出县直单位或各乡（镇）指挥部应急处置能力，需县指挥部协调处置的。

（3）县指挥部根据事发当时情形，经分析研判，认为应当启动Ⅱ级应急响应的。

4.2.2.2 启动程序

县指挥部办公室会同成员单位、技术支撑队伍对事件信息进行研判，及时向县指挥部提出启动Ⅱ级响应建议，县指挥部指挥长或副指挥长批准后，决定启动Ⅱ级响应状态。

4.2.2.3 响应措施

（1）启动指挥体系

县指挥部进入应急状态，履行全县应急处置工作的统一领导、指挥、协调职责。县指挥部成员单位保持24小时联络畅通。

县指挥部办公室24小时值班。

各乡(镇)指挥部和县指挥部成员单位进入应急状态,在县指挥部统一指挥、协调下,负责本地区、本部门应急处置工作或支援保障工作,明确联络员参与县指挥部办公室工作。

(2)掌握事件动态

跟踪事态发展。事件发生地乡(镇)人民政府及有关部门及时将事件发展变化情况和处置进展情况报县指挥部办公室。

检查影响范围。网络与信息系统主管部门立即全面了解本部门主管范围内的网络与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指挥部办公室。

及时通报情况。县指挥部办公室负责汇总上述有关情况,重大事项及时报县人民政府及上级有关部门,并通报县指挥部成员单位。

(3)决策部署

县指挥部统一指导,组织成员单位、技术支撑队伍,及时开展应急救援工作。

(4)处置实施

控制事态、防止蔓延。有关部门和单位要负责组织实施,安排网络与信息安全应急技术支撑队伍采取技术措施,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,防止事件蔓延至其他网络与信息系统。对于信息内容安全事件要及时采取必要的管控措施,防止有害信息传播扩散。

迅速处置、消除隐患。有关部门和单位要根据事件发生原因,有针对性地采取措施,恢复受破坏网络与信息系统正常运行。

及时开展调查取证。事发单位在应急恢复过程中应尽量保留相关证据,对于人为破坏活动,公安等部门按职责分工负责组织侦查和调查工作,并及时上报县指挥部办公室。

根据实际需要,县指挥部及有关成员单位、技术支撑单位及时向上级有关部门或技术支撑队伍申请援助。

4.2.3 Ⅲ级响应

4.2.3.1 启动条件

当符合以下情形之一时,启动Ⅲ级应急响应:

(1)发生或暂时情况不明有可能发生一般以下网络与信息安全事件,且依靠事发单位或事发地乡(镇)指挥部可以应对的。

(2)县指挥部根据事发当时情形,经分析研判,认为需要启动Ⅲ级应急响应的。

4.2.3.2 启动程序

县指挥部办公室对事件信息进行分析研判,及时向县指挥部提出启动Ⅲ级响应建议,由县指挥部办公室主任启动Ⅲ级响应。

4.2.3.3 响应措施

(1)县指挥部办公室密切关注事态发展,视情派出应急工作组到事发地进行协调指导。

(2)各网络与信息安全应急技术支撑队伍根据各自职责,积极提供配合和支持。

(3)将事件处理进展情况及时报告县政府及相关部门。

4.3 社会力量动员与参与

依托社会优秀互联网网络安全企业,充分发挥社会力量和人才在网络与信息安全中的积极作用,合理动员、组织其参与网络与信息安全事件应急响应工作。

4.4 信息发布

新闻主管部门按照指挥部意见,组织做好对外信息发布工作,对受影响的公众进行解释、疏导。未经批准,其他部门和单位一律不得发布相关信息。

4.5 应急结束

应急处置完成后,经分析评估认为网络与信息安全风险隐患已消除,网络及业务系统恢复正常。经县指挥部批准后,由县指挥部办公室宣布应急响应结束,必要时向社会公布。

5 后期处置

5.1 事件总结

特别重大、重大、较大网络与信息安全事件由县指挥部组织有关部门和地区配合上级应急指挥机构进行调查处理和总结评估。

一般网络与信息安全事件由县人民政府或部门组织调查处理和总结评估,对事件的起因、性质、影响、责任等进行调查,提出处理意见和改进措施。相关总结调查报告上报市指挥部办公室。

5.2 善后处置

县指挥部、事发地区乡(镇)政府、事件责任单位要积极稳妥、

深入细致地搞好善后处置。对参与处置的工作人员，以及紧急调集、征用有关单位、个人的物资，要按照规定给予补助或补偿。

5.3 恢复重建

恢复重建工作由事发单位负责。事发单位和相关职能部门在对可利用的资源进行评估后，制订重建和恢复计划，迅速采取各种有效措施，恢复网络与信息系统的正常运行。

6 应急保障

6.1 技术支撑队伍

相关部门应加强网络与信息安全应急技术支撑队伍建设，完善技术支撑队伍检查监测装备、培养和引进人才，开展网络与信息安全防范技术研究，做好网络与信息安全事件的应急技术支援工作。密切与市网络与信息安全应急技术支撑队伍的联系，及时取得技术外援支持，提高应对突发网络与信息安全事件的能力。

6.2 专家队伍

县指挥部办公室设立网络与信息安全咨询工作组，为网络与信息安全事件的预防和处置提供技术咨询，充分发挥专家在科学决策中的作用。

6.3 通信信息

指挥部和成员单位按照职责分工，加强应急通信装备准备，确保应急响应启动后，指挥系统通信与信息传达联络畅通。

6.4 基础平台

预留重要信息系统应急硬件，备份重要系统软件和基础数据

库，确保在网络与系统遭到破坏或毁损后，及时有效处置突发事件，恢复系统基本功能，提高应急处置能力。

6.5 情报力量

县公安局等部门加强网络与信息安全有关情报搜集能力建设，为网络与信息安全应急工作提供情报支持。

6.6 经费保障

乡（镇）政府、开发区及其有关部门应根据网络与信息安全事件应急救援需要，统筹安排应急救援专项资金和应急培训、演练所需经费，财政部门要纳入财政预算。

6.7 宣传教育和培训演练

指挥部和成员单位应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络与信息安全事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣传活动。

指挥部和成员单位要将网络与信息安全事件的应急知识等列为行政管理干部和有关人员的培训内容，加强网络与信息安全特别是网络与信息安全应急预案的培训，提高防范意识及技能。

县指挥部办公室会同有关部门、技术支撑队伍每年至少组织一次应急演练，模拟处置重大网络与信息安全事件，提高实战能力，检验和完善预案。

7 附则

7.1 预案管理与更新

本预案根据网络和信息安全发展形势以及相关法律法规的变更，三年评估一次，根据评估情况适时进行修订。评估及修订工作由县委宣传部（网信办）负责。本预案由县指挥部办公室统一管理，各成员单位根据本预案要求，按照各自职责分工，制定简单实用、操作性强的网络安全应急处置和保障行动方案，报指挥部办公室备案，建立健全预防和应对网络安全事件各项应急机制，同时密切配合，形成应对和处置网络安全事件工作合力。

7.2 表彰和惩处

对在网络与信息安全应急工作中表现突出的单位和个人给予表彰；对保障不力、瞒报漏报网络与信息安全事件，给国家和社会造成严重损失的单位和个人按照相关规定进行惩处。

7.3 预案解释部门

本预案由县委宣传部（网信办）制定并负责解释。

7.4 预案实施时间

本预案自印发之日起实施。

8 附录

8.1 阳城县网络与信息安全事件应急组织机构图

8.2 阳城县网络与信息安全事件应急工作流程图

8.3 网络安全事件分类

8.4 网络安全事件分级

8.5 阳城县网络与信息安全事件指挥部成员单位职责

8.6 阳城县网络与信息安全事件应急工作组组成及职责

8.7 阳城县网络与信息安全事件上报表

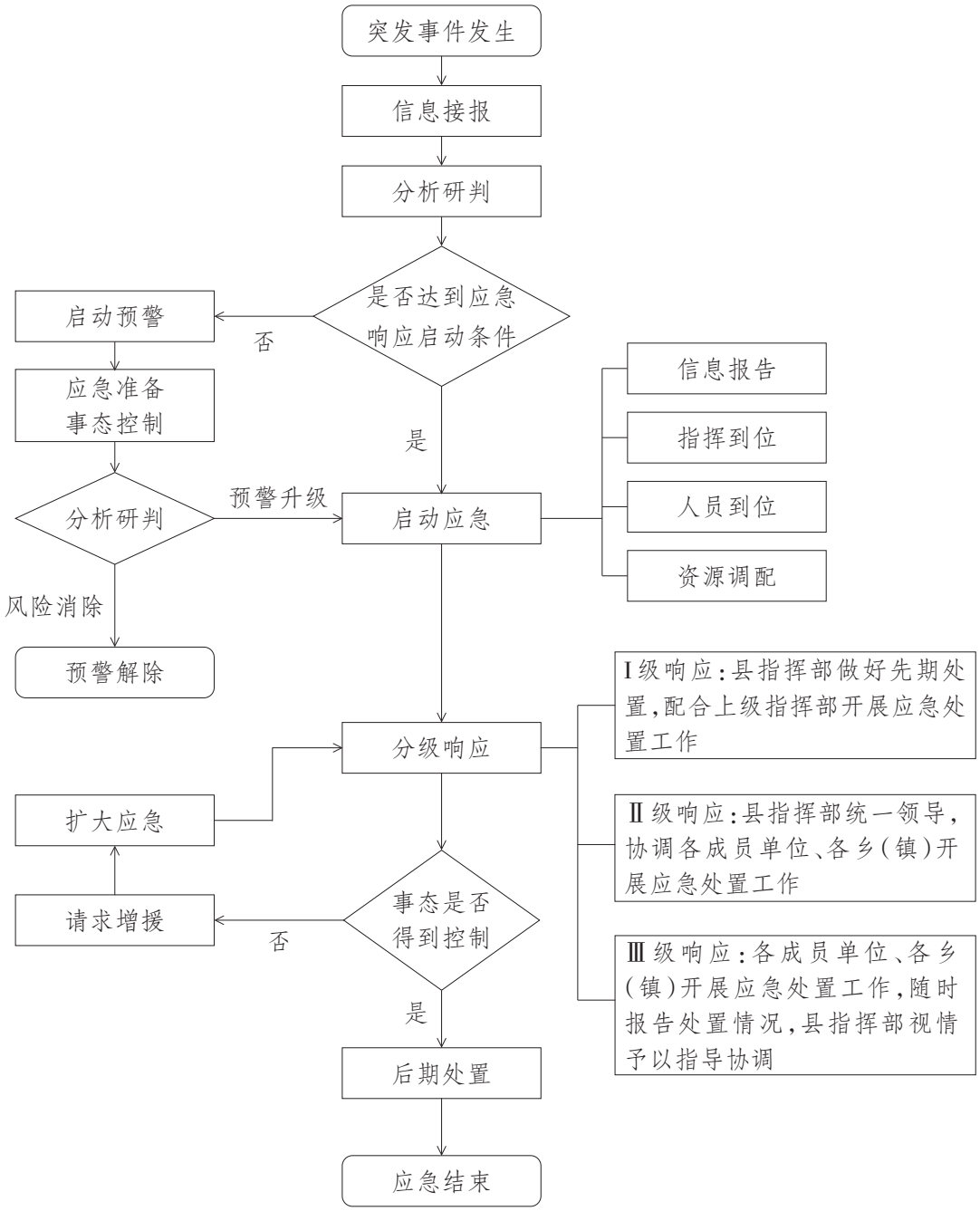
8.8 阳城县网络与信息安全事件应急联络表

附录8.1

阳城县网络与信息安全事件应急组织机构图

附录8.2

阳城县网络与信息安全事件应急工作流程图



附录8.3

网络安全事件分类

序号	类　别	定　　义	子　　项
1	恶意程序事　　件	在网络蓄意制造或传播恶意程序而导致业务损失或造成社会危害的网络安全事件。	包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、恶意代码内嵌网页事件、恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件、混合攻击程序事件和其他恶意程序事件等。
2	网络攻击事　　件	通过技术手段对网络实施攻击而导致业务损失或造成社会危害的网络安全事件。	包括网络扫描探测事件、网络钓鱼事件、漏洞利用事件、后门利用事件、后门植入事件、凭据攻击事件、信号干扰事件、拒绝服务事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、DNS污染事件、WLAN劫持事件、流量劫持事件、BGP劫持攻击事件、广播欺诈事件、失陷主机事件、供应链攻击事件、APT事件和其他网络攻击事件等。
3	数据安全事　　件	通过技术或其他手段对数据实施篡改、假冒、泄露、窃取等导致业务损失或造成社会危害的网络安全事件。	包括数据篡改事件、数据假冒事件、数据泄露事件、社会工程事件、数据窃取事件、数据拦截事件、位置检测事件、数据投毒事件、数据滥用事件、隐私侵犯事件、数据损失事件和其他数据安全事件等。
4	信息内容安全事件	通过网络传播危害国家安全、社会稳定、公共安全和利益的有害信息导致业务损失或造成社会危害的网络安全事件。	包括反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、权益侵害事件、信息滥发事件、网络欺诈事件和其他信息内容安全事件等。

序号	类　别	定　　义	子　　项
5	设备设施故障事件	由于网络自身出现故障或设备设施受到破坏或干扰而导致业务损失或造成社会危害的网络安全事件。	包括技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件和其他设备设施故障事件等。
6	违规操作事　　件	人为故意或意外地损害网络功能而导致业务损失或造成社会危害的网络安全事件。	包括权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件、人员可用性破坏事件、资源未授权使用事件、版权违反事件和其他违规操作事件等。
7	安全隐患事　　件	网络中出现能被攻击者利用的漏洞或隐患，一旦被利用可能对网络造成破坏，进而导致业务损失或造成社会危害的网络安全事件。提前发现这些漏洞或隐患能防范由此引起的其他网络安全事件。	包括网络漏洞事件、网络配置合规缺陷事件、其他安全隐患事件等。
8	异常行为事　　件	网络本身稳定性不足或违规访问网络造成访问、流量等异常行为，进而导致业务损失或造成社会危害的网络安全事件。	包括访问异常事件、流量异常事件和其他异常行为事件等。
9	不可抗力事　　件	因突发事件损害网络的可用性而导致业务损失或造成社会危害的网络安全事件。	包括自然灾害事件、事故灾难事件、公共卫生事件、社会安全事件和其他不可抗力事件等。
10	其他事件	未归为上述分类的网络安全事件。	

附录8.4

网络安全事件分级

事件级别	网络安全事件分级
特别重大事件（一级）	①重要网络和信息系统遭受特别严重的业务损失，造成网络大面积瘫痪，丧失业务处理能力。 ②重要数据或敏感个人信息遭到严重破坏，恢复业务正常运行和消除安全事件负面影响所需付出的代价十分巨大，对事发组织是不可承受的。 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，造成极其恶劣负面影响的网络安全事件。
重大事件（二级）	①重要网络和信息系统遭受严重的业务损失，造成网络长时间中断或局部业务瘫痪，业务处理能力受到极大影响。 ②重要数据或敏感个人信息遭到破坏，恢复业务正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的。 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，造成恶劣负面影响的网络安全事件。
较大事件（三级）	①重要网络和信息系统遭受严重或较大的业务损失，造成网络中断，导致业务处理能力受到较大影响。 ②数据或敏感个人信息受到损坏，恢复业务正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的。 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，或对相关公民、法人或其他组织的利益造成严重损害或特别严重损害的网络安全事件。
一般事件（四级）	①网络和信息系统遭受到攻击，造成网络短暂中断或较小的业务损失，导致业务处理能力受到一定影响。 ②数据或敏感个人信息受到影响，恢复业务正常运行和消除安全事件负面影响所需付出的代价较小。 ③其他不影响国家安全、社会秩序、经济建设和公众利益，但是对相关公民、法人或其他组织的利益造成一般损害的网络安全事件。

附录8.5　阳城县网络与信息安全事件指挥部成员单位职责

序号	成员单位	职责
1	县委办(县委机要保密室)	组织查处网络与信息安全突发事件中泄露国家秘密行为,对泄露国家秘密有关材料提请上级保密行政管理部门进行鉴定;负责网上失泄密事件的应急处置工作;负责党委重要信息系统密码保障和安全认证监督管理;协调发生突发事件时非机要部门使用的普通密码和商用密码、密码设备的配置及密码设备安全处置工作。
2	县委政法委	负责协调指导各相关部门做好网络安全领域反邪教工作,协调处理重大突发事件等。
3	县委宣传部 (县委网信办、 县政府新闻办公室)	负责网络与信息安全事件舆论引导和管理工作;通知相关部门或网站及时删除危害国家安全和社会稳定的有害信息;指导重点新闻网站开展网络安全事件的预防、监测和应急处置工作;负责统筹协调全县网络安全保障体系建设和全县信息安全防护工作,指导推进全县政府部门、重点行业网络安全保障工作;负责指导和协调突发事件信息发布工作;负责媒体记者的组织、管理和引导。
4	县政府外事办公室	负责网络与信息安全突发事件中涉外、涉台港澳的指导、协调。
5	县发展和改革局	将网络与信息安全应急基础设施建设纳入阳城县国民经济和社会发展“十五五”规划;根据县应急管理局的指令,负责应急状态下所需应急救灾物资的保障工作。
6	县教育局	负责全县学校的应急宣传教育工作;负责教育城域网和校园网络信息安全应急协调工作。
7	县科学技术局	负责科研等非经营性网络突发事件应急协调工作。
8	县工业和信息化局	指导电信管理部门做好基础信息网络的安全防范工作;组织协调电信行业开展处置恢复工作。
9	县公安局	负责监督、指导和检查社会领域各网络与信息系统运营单位开展网络与信息安全突发事件的预防和应对工作;开展网络安全监测,发现并通报网络攻击、病毒木马传播、地下黑产等网络安全事件,发布预警信息;依法打击网络与信息安全事件中的违法犯罪行为;依法打击邪教组织的违法犯罪活动等。

序号	成员单位	职责
10	县财政局	负责县级网络与信息安全突发事件应急处置经费的保障工作。
11	县交通运输局	负责网络与信息安全应急处置人员、物资车辆公路运输保障。
12	县文化和旅游局	负责组织监测、发现影响或可能影响全县广播电视传输网络正常运行的事件，并负责开展处置恢复工作；配合无线电管理部门监测、发现无线电干扰广播电视信号事件，配合有关部门开展处置恢复；组织监测、发现卫星干扰广播电视信号事件，并进行处置；组织监测、发现网上有害和敏感视听节目，并会同有关部门进行处置和管控。
13	县应急管理局	负责做好网络与信息安全应急县级地方标准制(修)订的指导工作。
14	县市场监督管理局	
15	县数据中心	负责全县大数据基础设施统筹规划、协调建设、管理运维；负责组织全县电子政务外网规划和建设、运维管理；协调基础电信运营企业为信息系统的正常运行提供基础网络保障，确保网络与信息安全应急指挥系统通信的联络畅通；配合有关部门监测发现网络与信息安全事件，并按有关规定具体实施管控措施。
16	阳城县供电公司	负责电力行业网络与信息安全突发事件的预防、监测、报告和应急处置工作；负责为网络与信息安全应急提供电力保障。
17	移动阳城分公司	负责组织通信、信息网络安全等事故的应急救援工作，做好应急救援通信保障工作。
18	联通阳城分公司	
19	电信阳城分公司	
20	铁塔阳城办事处	

附录8.6　阳城县网络与信息安全事件应急工作组组成及职责

序号	应急工作组	组　　成	职　　责
1	综合协调组	牵头部门:县委宣传部(县委网信办) 组成部门:县委办公室(县委机要保密室)、县发展和改革局、县教育局、县科学技术局、县工业和信息化局、县公安局、县应急管理局、县市场监督管理局、县数据中心、事发地乡(镇)人民政府等	负责做好网络与信息安全事件的组织协调工作;在县指挥部的领导下,负责收集汇总相关数据、进行初步分析及技术研判,评估事件影响;组织、协调成员单位参与网络与信息安全事件的应急救援与处置工作;及时向县指挥部报告突发事件发生和发展情况;协调处理相关善后工作;承办县指挥部交办的其他事项。
2	现场抢修组	牵头部门:县委宣传部(县委网信办) 组成部门:县委办公室(县委机要保密室)、县委政法委、县政府外事办公室、县工业和信息化局、县公安局、县文化和旅游局、县数据中心、移动阳城分公司、联通阳城分公司、电信阳城分公司、铁塔阳城办事处、事发地乡(镇)人民政府等	控制事态、防止蔓延。安排网络与信息安全应急技术支撑队伍采取技术措施,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,防止事件蔓延至其他网络与信息系统。对于信息内容安全事件要及时采取必要的管控措施,防止有害信息传播扩散;迅速处置、消除隐患。根据事件发生原因,有针对性地采取措施,恢复受破坏网络与信息系统正常运行。

序号	应急工作组	组　　成	职　　责
3	技术专家组	牵头部门:县数据中心 组成部门:县委宣传部(县委网信办)、县科学技术局、县工业和信息化局、移动阳城分公司、联通阳城分公司、电信阳城分公司、铁塔阳城办事处等。	分析、研判事件,对网络与信息安全事件的发展趋势、抢修方案等提供技术支持和决策咨询,并对事件可能造成的危害进行预测、评估。
4	后勤保障组	牵头部门:县发展和改革局 组成部门:县财政局、县交通运输局、县科学技术局、县工业和信息化局、县文化和旅游局、县应急管理局、阳城供电公司、移动阳城分公司、联通阳城分公司、电信阳城分公司、铁塔阳城办事处等。	负责提供网络与信息安全事件应急所需的人员、车辆、物资、装备、经费、通讯、电力等保障。
5	新闻宣传组	牵头部门:县委宣传部(县政府新闻办公室) 组成部门:县委宣传部(县委网信办)、县文化和旅游局、县融媒体中心等。	对网络与信息安全事件相关信息进行管理,包括信息发布、新闻报道、舆论引导、舆情监测和网络舆情调控等。

附录8.7

阳城县网络与信息安全事件上报表

报告单位		报告时间	
事发单位		事件起始时间	
填 报 人		审 核 人	
事件分类	□恶意程序类事件 □网络攻击类事件 □数据安全类事件 □信息内容安全类事件 □设备设施故障类事件 □违规操作类事件 □安全隐患类事件 □异常行为类事件 □不可抗力类事件 □其他事件		
事件级别	□特别重大事件 □重大事件 □较大事件 □一般事件		
危害表象	□网络中断 □系统瘫痪 □数据毁坏 □数据泄密 □其他危害		
事件描述(包括突发事件发生的原因、性质,初步原因和危害程度判断):			
处置措施(突发事件发生单位已采取的控制措施及其他应对措施):			
事件后果的初步估计:			
有关意见和建议:			

附录8.8

阳城县网络与信息安全事件应急联络表

单　　位	值班电话	单　　位	值班电话
省委办公室	0351-4045001	阳城供电公司	2166214
省政府办公室	0351-3046789	电信阳城分公司	6921273
市委办公室	2062298	联通阳城分公司	4223547
市政府办公室	2198345	移动阳城分公司	3291656
市委网信办	2566200	铁塔阳城办事处	18635617707
县委办公室	4223770	润城镇人民政府	4814501
县政府办公室	4222726	寺头乡人民政府	4970002
县委政法委	4222186	西河乡人民政府	4834102
县委宣传部（县委网信办、县政府新闻办公室）	4239360	董封乡人民政府	4900002
县政府外事办公室	4227599	河北镇人民政府	4920099
县发展和改革局	4238298	白桑镇人民政府	4879000
县教育局	4223192	东冶镇人民政府	4860016
县科学技术局	4222171	凤城镇人民政府	4222788
县工业和信息化局	4222029	北留镇人民政府	4851226
县公安局	4233414	町店镇人民政府	3200360
县财政局	4222727	芹池镇人民政府	4980098
县交通运输局	4222269	演礼镇人民政府	4841001
县文化和旅游局	4232366	次营镇人民政府	4930399
县应急管理局	4220426	横河镇人民政府	4939018
县市场监督管理局	4239265	蟒河镇人民政府	4870016
县数据中心	4220369		

（此页无正文）

（此页无正文）

抄送：县委办，县人大办，县政协办，县法院，县检察院，各人民团体，各新闻单位。

阳城县人民政府办公室　　2025年4月14日印发