苍溪县网络安全事件应急预案（试行）

1 总则

1.1 编制目的

建立健全我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，维护国家安全、公共安全和社会秩序。

1.2 编制依据

根据《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》《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》《关键信息基础设施安全保护条例》《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》《信息安全技术信息安全事件分类分级指南》《四川省网络安全事件应急预案（试行）》《苍溪县突发事件总体应急预案（试行）》等法律法规和相关规定，结合苍溪实际，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，对我县网络和信息系统或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、灾害性事件和其他网络安全事件。

本预案适用于苍溪县域内网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

1.4 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，平战结合，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。

1.5 事件分级

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：

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。

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。

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：

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。

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。

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:

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。

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。

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。

2 苍溪网络安全事件应急组织

2.1 组织指挥体系

建立跨部门联动处置机制，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，县委网信办统筹协调组织全县网络安全事件应对工作。县委宣传部、县委保密机要局、县委国安办、县经信局、县公安局、县互联网信息中心等相关部门（单位）按照职责分工负责网络安全事件应对工作。县委网信办下设县网络安全应急办公室（以下简称“县网安应急办”），

负责日常工作。

发生特别重大、重大网络安全事件以及涉及面广、危害性大或处置不当可能造成严重后果的较大、一般网络安全事件时，成立县网络安全事件应急指挥部（以下简称“县指挥部”），负责应急处置的组织指挥和协调，指挥长由分管网信工作的县领导担任，成员由跨部门联动处置机制有关单位负责同志担任。根据工作需要指挥部可对成员进行调整。

2.2 办事机构与职责

县网安应急办负责全县网络安全日常工作及指挥部成立后的事务性工作，开展网络安全信息的汇集、分析、研判和通报工作，协调县网络安全应急技术支撑队伍、专家和装备、物资等参与网络安全事件处置，管控网络安全事件相关网络舆情，及时上报网络安全事件处置情况。

2.3 各单位职责

县委宣传部（县政府新闻办）：负责网络安全事件的应急新闻工作，开展新闻发布和舆论引导工作。

县委保密机要局：负责涉及国家秘密的网络安全监测预警、威胁治理、信息通报和应急处置等工作。

县委国安办：负责危害国家安全的网络监测预警、威胁治理、信息通报和应急处置工作，防范、制止和打击各种网络渗透、窃密行为。

县经信局：负责电信和工业领域网络安全监测预警工作，指

导县级有关部门、重点行业的重要信息系统与信息网络应急保障工作，参与处置相关网络安全事件。

县公安局：负责关键信息基础设施网络安全监测预警、威胁治理、信息通报和应急处置工作，对关键信息基础设施的安全风险进行抽查检测，开展网络安全执法检查，依法侦查打击针对和利用网络实施的违法犯罪活动。

县互联网信息中心：负责互联网行业网络安全监测预警、威胁治理、信息通报和应急处置等工作，配合打击网络犯罪和处理网络有害信息。

县级有关部门（单位）按照职责和权限，负责本部门（单位）、本行业网络安全事件的预防、监测、报告和应急处置工作。

跨部门联动处置机制有关部门（单位）的业务股室主要负责人为县网安应急办联络员。应急响应期间，根据工作需要和职能职责，派员参与县网安应急办联合值班值守。

3 监测与预警

3.1 预警分级

网络安全事件预警等级由高到低分为四级：一级、二级、三级、四级，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

按照“谁主管谁负责、谁运行谁负责”要求，各网络和信息系统运行单位对本单位建设运行的网络和信息系统开展网络安

全监测。行业主管部门（单位）指导做好本行业网络安全监测工作。重要监测信息按程序报县网安应急办。

3.3 预警研判和发布

按照《国家网络安全事件应急预案》《四川省网络安全应急预案（试行）》《广元市网络安全应急预案（试行）》规定，红色预警由国家网络安全应急办公室（以下简称“国家网安应急办”）发布，橙色预警由省网安应急办发布，黄色预警和涉及多县（区）、多部门（单位）、多行业的蓝色预警由市网安应急办发布。

县网安应急办对监测信息进行研判，发布本地的网络安全事件蓝色预警。需要立即采取防范措施的，应及时通知可能受网络安全事件影响的部门（单位）。对可能发生的较大及以上网络安全事件，及时向市网安应急办报告有关信息。

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）县网安应急办根据国家网安应急办发布的红色预警和涉及多省（区、市）、多部门（单位）、多行业的预警，积极组织开展预警响应工作。县网安应急办、有关乡镇和县级有关部门（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信息搜集报送工作，组织指导应急技术支撑

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，重要情况按程序报送市网安应急办。

（2）县网络安全应急技术支撑队伍进入待命状态，积极与市网络安全应急技术支撑队伍对接，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，做好参与现场处置的准备工作。

3.4.2 橙色预警响应

（1）县网安应急办组织开展预警响应工作，联系专家和有关机构，跟踪研判事态发展情况，研究制定防范措施和应急工作方案，协调做好资源调度和部门联动的各项准备工作，及时将事态发展情况报送市网安应急办。

（2）有关乡镇、县级有关部门（单位）启动相应应急预案，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信息搜集报送工作，组织指导应急技术支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，及时将事态发展情况报送县网安应急办。县网安应急办密切关注事态发展，有关重大事项及时通报相关乡镇和县级有关部门（单位）。

（3）县网络安全应急技术支撑队伍保持联络畅通，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、蓝色预警响应

（1）市网安应急办发布的黄色、蓝色预警，县网安应急办发布的蓝色预警，由县网安应急办统筹协调，各乡镇、县级有关

部门（单位）启动相应应急预案，组织指导应急技术支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报送市网安应急办。

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 先期处置及事件报告

网络安全事件发生后，事发单位应立即开展处置并及时报送信息，并组织先期处置，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。

各级各部门(单位)应建立健全网络安全事件信息报告机制。对于初判为一般或较大网络安全事件的，涉事乡镇或县级有关部门（单位）应在事件发生后 2 小时内报告县网安应急办，县网安应急办在接到报送后 1 小时内报告市网安应急办。对于初判为特别重大、重大网络安全事件的，应立即报告县委网信委及县网安应急办，县网安应急办按有关要求报告市网安应急办。

4.2 应急响应

县级层面应急响应由高到低分为三级：一级、二级、三级。一级对应特别重大网络安全事件，二级对应重大网络安全事件，三级对应较大和一般网络安全事件。

4.2.1 一级响应

特别重大网络安全事件由省网安应急办启动一级响应。经县委网信委批准后，成立县指挥部。

（1）启动指挥体系

县指挥部进入应急状态，保持与市网安应急办密切衔接，在市指挥部的统一指挥、指导、协调下，开展应急处置或支援保障工作。县指挥部成员保持24小时通信联络畅通。县网安应急办24小时值班。

相关乡镇、县级有关部门（单位）进入应急状态，在县指挥部的统一领导、指挥、协调下，负责本辖区、本部门（单位）应急处置或支援保障工作，24小时值班，并派员参加县网安应急办工作。

（2）掌握事件动态

跟踪事态发展。涉事乡镇或县级有关部门（单位）及时将事态发展变化情况和处置进展情况报县网安应急办。

检查影响范围。相关乡镇、县级有关部门（单位）立即全面了解本辖区或本部门（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，及时将有关情况报送县网安应急办。

及时通报情况。县网安应急办负责汇总上述有关情况，重大事项及时报告县指挥部和市网安应急办，并通报相关乡镇、县级有关部门（单位）。

（3）决策部署

县指挥部落实上级指挥部要求，组织有关乡镇、县级有关部

门（单位）以及专家组、应急技术支撑队伍和有关方面及时研究对策意见，安排部署处置工作。

（4）处置实施

控制事态防止蔓延。县网安应急办和相关乡镇、县级有关部门（单位）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。相关乡镇、县级有关部门（单位）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，恢复受破坏网络和信息系统的正常运行。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。

调查取证。事发单位在应急恢复过程中应保留相关证据。对于人为破坏活动，县委保密机要局、县公安局、县委国安办在上级相关部门指导下，按职责分工组织开展调查取证工作。

信息发布。县委宣传部（县政府新闻办）在市委宣传部（市政府新闻办）指导下，开展新闻发布和舆论引导工作。未经批准，其他部门（单位）不得擅自发布相关信息。

4.2.2 二级响应

重大网络安全事件由市网安应急办启动二级响应，经县委网信委批准后，成立县指挥部。

（1）启动指挥体系

县指挥部成员保持24小时通信联络畅通。县网安应急办进入应急状态，需要其他县（区）、市级部门（单位）和市网络安

全应急技术支撑队伍配合和支持的，报请市网安应急办予以协调。

涉事单位进入应急状态，按照相关应急预案做好应急处置工作。有关乡镇、县级有关部门（单位）和县网络安全应急技术支撑队伍根据各自职责，积极配合、提供支持。

（2）掌握事件动态

跟踪事态发展。涉事单位及时将事态发展变化情况和处置进展情况报送县网安应急办。

检查影响范围。县网安应急办立即了解全县范围内的网络安全和信息系统受波及和影响情况。有关乡镇和县级有关部门（单位）立即全面了解本辖区、本部门（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送县网安应急办。

及时通报情况。县网安应急办负责汇总上述有关情况，重大事项及时报告县指挥部和市网安应急办，并通报有关乡镇和县级有关部门（单位）。

（3）决策部署

县指挥部组织有关乡镇、县级有关部门（单位）以及专家组、应急技术支撑队伍和有关企业、单位等方面及时研究对策意见，安排部署处置工作。

（4）处置实施

控制事态防止蔓延。县网安应急办和相关乡镇、县级有关部

门（单位）负责组织开展处置工作，尽快控制事态；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。相关乡镇、县级有关部门（单位）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，恢复受破坏网络和信息系统的正常运行。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。

调查取证。事发单位在应急恢复过程中应保留相关证据。对于人为破坏活动，县委保密机要局、县公安局、县委国安办在上级相关部门指导下，按职责分工组织开展调查取证工作。

信息发布。县委宣传部（县政府新闻办）在市委宣传部（市政府新闻办）指导下，开展新闻发布和舆论引导工作。未经批准，其他部门（单位）不得擅自发布相关信息。

4.2.3 三级响应

较大、一般网络安全事件由县网安应急办根据事件的性质和发展情况向县委网信委提出启动三级应急响应的建议，县委网信委批准后，启动三级响应，成立县指挥部。根据事态发展变化情况及时向市网安应急办报告。对涉及面广、危害性大或处置不当可能造成严重后果的较大、一般网络安全事件，根据工作需要，可由县网安应急办研判提出，报请县委网信委同意后，上报市网安应急办请求启动市级层面三级响应，并按照二级响应流程组织应对处置。

4.3 响应终止

网络安全事件应急响应终止应符合以下条件：应急处置工作结束、网络安全事件造成的影响减弱并逐步消失、网络安全风险得到有效控制。

一级响应的终止，由县网安应急办根据上级网安应急办通报实施，并报县指挥部指挥长和县委网信委主要负责同志。

二级响应的终止，由县网安应急办根据市网安应急办通报实施，并报县委网信委主要负责同志和县网安应急办。

三级响应的终止，由县网安应急办根据市网安应急办通报实施，并报县指挥部指挥长和县委网信委主要负责同志；或由县网安办研判提出，报县指挥部指挥长批准后实施，并报县委网信委主要负责同志和市网安应急办。

5 调查与评估

特别重大网络安全事件按照省网安应急办要求，由县网安应急办配合市网安应急办开展调查处理和总结评估。重大网络安全事件按照市网安应急办要求，由县网安应急办配合市网安应急办开展调查处理和总结评估。较大及一般网络安全事件由县网安应急办组织有关乡镇和县级有关部门（单位）调查处理和总结评估，报县委网信委和市网安应急办。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

各乡镇、县级各部门（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

县委网信办协调有关部门(单位)每年至少组织1次预案演练，检验和完善预案，提高实战能力，并将演练情况报市委网信办。

各乡镇、县级各部门（单位）每年至少组织1次预案演练，并将演练情况报县委网信办。

6.3 宣传

各乡镇、县级各部门（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

各乡镇、县级各部门（单位）应将网络安全事件的应急处置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

在国家和省市县重要活动、会议期间，各乡镇、县级各部门

（单位）应在常规工作基础上进一步强化预警措施，加强网络安全事件的防范，确保网络安全。县网安应急办统筹协调网络安全保障工作，如国家、省、市网安应急办启动有关预警，县网安应急办和有关乡镇、县级有关部门（单位）根据上级要求或需要启动相应级别预警响应。有关乡镇、县级有关部门（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，重点部门、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

各乡镇、县级各部门（单位）应落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，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。根据中央网信办制定的评估认定标准，县委网信办报请市委网信办对我县网络安全应急技术支撑队伍进行评估和认定。各乡镇、县级各部门（单位）应配备必要的网络安全专业技术人才，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

县网安应急办组织建立县网络安全应急专家队伍，为网络安全事件的预防和处置提供技术咨询和决策建议。县应急指挥机构逐步加强专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

鼓励从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对较大以上网络安全事件的能力。

7.5 基础平台

在市网络安全战略预警和决策指挥能力建设基础上，各乡镇、县级各部门（单位）加强网络安全应急基础平台和管理平台建设，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

县公安局、县委国安办等部门加强网络安全信息获取与情报分析能力建设，完善信息情报共享机制，为网络安全应急工作提供情报支撑。

7.7 产业促进

有关部门（单位）加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务、灾难备份等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.8 物资保障

各乡镇、县级各部门（单位）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。

7.9 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。各乡镇、县级各部门（单位）利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、基础平台建设、预案演练、物资保障等工作开展。各乡镇、县级各部门（单位）为网络安全应急工作提供必要的经费保障。

8 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

县委网信办、有关乡镇和县级有关部门（单位）可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给予奖励。

县委网信办和县级有关部门（单位）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。

9 附则

9.1 预案管理

本预案原则上每年评估 1 次，根据实际情况适时修订。修订工作由县委网信办负责。

各乡镇、县级各部门（单位）应根据本预案制定或修订本辖区、本部门、本行业网络安全事件应急预案。各预案应与本预案相衔接，并抄送网信、应急部门和上级主管部门。

9.2 预案解释

本预案由县委网信办负责解释。

9.3 预案实施时间

本预案自印发之日起实施。

附件：1. 网络安全事件分类

2. 网络和信息系统损失程度划分说明

附件 1

网络安全事件分类

网络安全事件分为有害程序事件、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、灾害性事件和其他网络安全事件等。

一、有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

二、网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

三、信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

四、信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

五、设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

六、灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

七、其他事件是指不能归为以上分类的网络安全事件。

附件 2

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

一、特别严重的系统损失。造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统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，对于事发组织是不可承受的。

二、严重的系统损失。造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统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。

三、较大的系统损失。造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统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。

四、较小的系统损失。造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。