虎林市人民政府文件

虎政办规〔2025〕1号

虎林市人民政府办公室关于印发虎林市网络安全事件应急预案的通知

各乡（镇）人民政府，市政府各直属单位:

《虎林市网络安全事件应急预案》业经2月27日市政府七届44次常务会议讨论通过，现予印发，请认真贯彻执行。

虎林市人民政府办公室

2025年3月5日

虎林市网络安全事件应急预案

1. 总则

1.1 编制目的

为科学应对网络安全事件，建立健全本市网络安全应急工作体制机制，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，制定本预案。

1.2 编制依据

依据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《中华人民共和国突发事件应对法》《信息安全技术信息安全事件分类分级指南》（GB/Z20986-2007）《鸡西市突发事件应急预案管理办法》等法律法规，并与《黑龙江省网络安全事件应急预案》《鸡西市人民政府突发公共事件总体应急预案》《鸡西市网络安全事件应急预案》相衔接。结合我市网络安全实际情况，制定本预案。

1.3 适用范围

本预案适用于本市发生的网络安全事件，影响本市的网络安全事件的预防、监测、报告和处置工作。

1.4 事件分级

网络安全事件分为四级：特别重大网络安全事件（I 级）、重大网络安全事件（II级）、较大网络安全事件（III 级）、一般网络安全事件（Ⅳ级）。

（1）符合下列情形之一的，为特别重大网络安全事件：

①关键信息基础设施以及其他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泄露、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关键信息基础设施以及其他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，为较大重大网络安全事件:

①关键信息基础设施以及其他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、密切协同；坚持统一指挥、快速反应、科学应对；坚持底线思维、突出重点、预防为主；坚持属地管理、谁主管谁负责、谁运行谁负责；坚持政府主导、军地结合、社会协同。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. 组织指挥体系与职责

2.1 领导机构与职责

在市委网络安全和信息化委员会的领导下，成立虎林市网络安全事件应急指挥部（以下简称市应急指挥部），作为非常设机构，统一领导、组织和指挥网络安全事件应急处置工作。市应急指挥部总指挥由市政府常务副市长担任，副总指挥由市委网信办主任担任。市委保密和机要局、市委宣传部、市委网信办、市委政法委、市委编办、市委统战部、市政府办（金融服务局）、市信访局、市发改局、市教育局、市住建局、市卫生健康局、市工信局、市公安局、市国家安全局、市外事办、市财政局、市文体广电和旅游局、市应急管理局、市营商环境建设监督局、电业局等有关部门为市应急指挥部成员单位。

根据应急工作实际需要，成员单位可随时调整。市应急指挥部职责:

（1）贯彻落实国家、省、鸡西市关于网络安全事件应急工作的决定事项，及时报告重要情况、提出建议。

（2）研究确定处置网络安全事件的决策和指导意见。

（3）负责本预案的启动，对网络安全事件发生地提供技术支持和支援。

2.2 办事机构与职责

市应急指挥部下设办公室，办公地点设在市委网信办。主任由市委网信办主任兼任。市应急指挥部成员单位相关业务处室主要负责人为市应急指挥部办公室联络员。

市应急指挥部办公室职责:

（1）统筹协调组织本市网络安全事件应对工作。

（2）建立健全跨部门应急联动机制。

（3）组织编制修订本预案，并组织成员单位开展预案应急演练工作。

（4）负责网络安全事件信息的收集、研判、综合和对上报告工作。

（5）承担网络安全应急跨部门、跨区域协调工作和市应急指挥部的事务性工作，通报相关情况。

（6）组织指导本市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。

（7）完成市应急指挥部交办的其他工作。

2.3 成员单位职责

（1）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。

（2）建立健全预防和应对网络安全事件的各项应急机制，同时密切配合，形成应对和处置网络安全事件工作的合力。

（3）按照职责和权限，负责本部门、本行业、本领域网络和

信息系统网络安全事件的预防、监测、报告和应急处置工作。

（4）建立健全网络安全责任制，明确网络安全第一责任人、直接责任人，内设的网络安全职能部门、技术机构、网络产品和服务提供者、网络安全合作单位等相关责任主体和责任人，并向市应急指挥部办公室备案；备案信息发生变更的，应及时更新备案信息。

2.4 市委网信办职责

市委网信办在市委网络安全和信息化委员会的统一领导下，统筹协调组织本地网络安全事件的预防、监测、报告和应急处置工作。

2.5 网络运营者及网络产品、服务提供者职责

（1）网络运营者及网络产品、服务的提供者要严格落实国家法律法规和本市有关网络安全管理制度。

（2）网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

（3）在发生危害网络安全的事件时，立即启动应急预案，采取相应补救措施，并按照规定向有关主管部门报告。

（4）网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

3. 监测与预警

3.1 预防监测与报送

3.1.1 日常预防

市应急指挥部各成员单位按照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、网络安全监测及预警管控、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。

3.1.2 重要活动期间的预防

在国家、省、鸡西市重要活动、会议期间，全市各部门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。市委网信办统筹协调网络安全保障工作，根据实际要求市应急指挥部成员单位启动预警响应。有关部门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。

3.1.3 安全监测与信息报送

市应急指挥部各成员单位按照“属地管理、分级负责”“谁主管谁负责、谁运行谁负责”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，负责关键信息基础设施安全保护工作的部门分别做好本行业、本领域网络安全监测工作。

市委网信办结合本地实际，统筹组织开展对本市网络和信息系统的安全监测工作。市应急指挥部各成员单位将重要监测信息报市委网信办。

市应急指挥部各成员单位要对监测预测工作中获取疑似网络安全事件信息进行综合预判，加强统计信息报送工作，保证信息报送渠道畅通，按照有关要求，如实、规范、及时报送信息。

报告内容:

（1）辖区内所发现的网络安全事件或已发生的情况，包括发

生时间、区域范围、可能造成的危害等。

（2）辖区内发生的网络安全事件的风险或已发生的原因、趋势、影响和社会反映。

（3）相关措施建议。

3.2 预警分级

网络安全事件预警等级分为四级：由高到低划分为特别重大（Ⅰ级）、重大（Ⅰ级）、较大（Ⅲ级）和一般（Ⅳ级），依次用红色、橙色、黄色和蓝色表示，预警分级与网络安全事件分级相对应。根据事态发展情况和采取措施的效果，预警级别可以升级、降级或者解除。

3.3 预警研判和发布

3.3.1 预警研判

（1）市应急指挥部成员单位组织对本部门、本行业网络安全监测信息，对照本预案及自行制定的预案开展研判工作，认为需要立即采取防范措施的，应当及时通知相关部门、单位及网络用户，对可能发生网络安全事件的信息及时向市应急指挥部和鸡西市网络安全应急指挥部办公室报告。

（2）市应急指挥部办公室、市应急指挥部相关成员单位要会同专业技术人员适时对预警的网络安全事件信息进行分析评估，当引发网络安全事件因素基本消除或已得到有效控制时，应及时向市应急指挥部报告。市应急指挥部根据鸡西市网络安全应急指挥部发布预警解除信息要求，终止各项预警行动和措施，恢复日常基本监测监控状态。

3.3.2 预警发布与解除

一般级别（蓝色）和较大级别（黄色）预警发布与解除，由鸡西市应急指挥部办公室向鸡西市应急指挥部提出一般（Ⅳ级）、较大（Ⅲ级）网络安全事件或涉及多部门、多行业的一般（Ⅳ级）、较大（Ⅲ级）网络安全事件蓝色或黄色预警发布或解除预警建议，经鸡西市网络安全应急指挥部副总指挥审定，通过鸡西市应急管理局应急指挥中心通过鸡西市突发事件预警信息发布平台统一对外发布，并上报省网络安全应急指挥部办公室备案。

重大（Ⅱ级）级别的橙色预警发布与解除，由省网络安全应急指挥部办公室发布。特别重大（Ⅰ级）级别的红色预警发布与解除，由省网络安全应急指挥部报请中央网信办发布。

预警信息包括事件类别、预警级别、起始时间、可能影响范围、警示事项、应采取措施和时限要求、发布机关等。

3.4 预警分级响应

3.4.1 红色和橙色预警响应

红色预警响应由中央网信办统一组织实施，橙色预警响应由省网络安全应急指挥部统一组织实施，市应急指挥部按照鸡西市网络安全应急指挥部、市委网络安全和信息化委员会的要求，配合国家和省统一行动，在采取黄色预警响应措施基础上，加强组织领导做好本市预警响应工作。

3.4.2 蓝色和黄色预警响应

（1）蓝色和黄色预警响应由市应急指挥部统一组织实施，市应急指挥部按程序启动本预案，组织开展预警响应工作。

（2）市应急指挥部办公室组织相关市应急指挥部成员单位做好本行业、本领域预警响应行动，组织专家和有关机构对事态发

展情况进行跟踪研判，研究制定预防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。

（3）相关市应急指挥部成员单位启动本级、本系统、本部门网络安全事件应急预案，按照职责分工落实预防措施和各项准备工作。

（4）市应急指挥部办公室、相关市应急指挥部成员单位应急指挥机构实行 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，组织指导应急支撑队伍、相关运行单位开展应急处置准备、风险评估和控制工作。

（5）市网络安全应急技术支撑队伍进入待命状态，针对鸡西市网络安全应急指挥部发布的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。

（6）有关市应急指挥部成员单位要及时将事件的事态发展情况报市应急指挥部办公室。市应急指挥部办公室密切关注事态发展，有关重大事项及时通报相关部门，并按照规定及时向鸡西市网络安全应急指挥部办公室报送事件的事态发展情况。

（7）有关网络运营者、网络产品和服务提供者按照国家法律法规以及与我市用户的服务合同要求做好应急准备工作。

4. 应急处置

4.1 信息报告

全市各部门各单位要建立健全网络安全事件信息报告机制。网络安全事件发生后，事发单位要按照有关规定第一时间向市委网信办或市政府报告信息，最迟不得超过事发后 1 小时。

确认为一般或较大突发事件的，市委网信办在接到事件信息

报告后经核实，应立即向市委、市政府及鸡西市网络安全应急指挥部办公室报告，市委办公室于20分钟内向鸡西市委办公室（信息科）电话报告，市政府于20分钟内向鸡西市政府办公室（市政府总值班室）电话报告，并于1小时内书面报告。

确认为重大和特别重大事件的，市委网信办在接到事件信息报告后经核实，应立即向市委、市政府及鸡西市网络安全应急指挥部办公室报告，市委办公室于20分钟内向鸡西市委办公室（信息科）电话报告，市政府于20分钟内向鸡西市政府办公室（市政府总值班室）电话报告，必要时可直接向省政府总值班室报告。

报告内容包括事件所涉机构名称、地点、时间；事发原因、性质、等级、危害程度、影响范围、社会稳定情况；事态发展趋势、可能造成的损失、采取的应对措施；其他与事件相关内容。

4.2 先期处置

网络安全事件发生后，市应急指挥部及相关成员单位要立即启动本级预案，迅速进入应急状态，协调公安机关等成员单位采取措施控制事态发展，并立即将事件相关情况向鸡西市应急指挥部办公室、鸡西市委办公室和鸡西市政府办公室（市政府总值班室）报告。

4.3 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（I级）、重大（II级）、较大（III级）和一般（IV级）网络安全事件。级别为最高响应级别。

4.3.1 I级和II级应急响应

省网络安全应急指挥部办公室组织对事件信息进行研判，属

特别重大网络安全事件和重大网络安全事件的，由中央网络安全和信息化委员会、省委网络安全和信息化委员会启动Ⅰ级或Ⅱ级响应。市应急指挥部收到Ⅰ级或Ⅱ级通报后，在市委网络安全和信息化委员会统一领导、指挥协调下，配合省市网络安全应急指挥部组织做好本市应急响应工作。

4.3.2 Ⅲ级和Ⅳ级应急响应

鸡西市网络安全应急指挥部办公室组织对事件信息进行研判，属较大或一般网络安全事件或涉及多部门、多行业的较大或一般网络安全事件的，由鸡西市网络安全应急指挥部提出启动Ⅲ级或Ⅳ级应急响应。市应急指挥部办公室根据鸡西市网络安全应急指挥部启动应急响应的要求，经副总指挥审定，报市政府分管副市长批准同意后，及时通报市应急指挥部各成员单位，在市委网络安全和信息化委员会统一领导、指挥协调下，配合鸡西市网络安全应急指挥部组织的Ⅲ级或Ⅳ级应急响应工作。

（1）启动指挥体系

①市应急指挥部进入应急状态，履行网络安全事件应急工作的统一领导、指挥、协调职责。市应急指挥部成员保持 24 小时联络畅通。市应急指挥部办公室 24 小时值班。

②有关市应急指挥部成员单位应急指挥机构进入应急状态，在市应急指挥部统一领导、指挥协调下，负责本行业领域应急处置工作或支援保障工作，相关工作人员 24 小时值班，并派员参加市应急指挥部办公室工作。

（2）掌握事件动态

①跟踪事态发展。市应急指挥部有关成员单位及时将事态发

展变化情况和处置进展情况报市应急指挥部办公室，市应急指挥部办公室及时将事态发展变化情况和处置进展情况报鸡西市网络安全应急指挥部办公室。

②检查影响范围。市应急指挥部有关成员单位立即全面了解本部门主管范围内网络和信息系统是否受到事件波及或影响，并将有关情况及时报市应急指挥部办公室，市应急指挥部办公室及时将有关情况报鸡西市网络安全应急指挥部办公室。

③及时通报情况。市应急指挥部办公室负责汇总上述有关情况，及时报鸡西市网络应急指挥部办公室和市应急指挥部，并通报有关市应急指挥部成员单位。

（3）决策部署

市应急指挥部组织有关市应急指挥部成员单位以及专家组、网络安全应急技术支撑队伍、有关企事业单位等方面及时研究对策意见，对应对工作进行决策部署。

（4）处置措施

①控制事态防止蔓延。市应急指挥部组织有关市应急指挥部成员单位尽快控制事态，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。

②消除隐患恢复系统。有关市应急指挥部成员单位根据事件发生原因，有针对性采取措施，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。网络运营者及网络产品、服务提供者应立即采取相应补救措施，及时处置各类网络安全风险及事件。必要时可依法征用单位和个人设备等财产，并依法给予补偿。

③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，市委网信办、市公安局、市国家安全局、市委保密和机要局按照职责分工负责组织开展调查取证工作。有关网络运营者及网络产品、服务提供者依法为网络安全事件的调查取证工作提供技术支持和协助。

④加强协调。市应急指挥部有关成员单位根据国家有关规定，按照各自渠道和有关合作框架，开展与其他地区和社会组织的协调合作。

⑤协调配合网络安全事件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安全事件的，市应急指挥部办公室应及时按照程序上报。

⑥在市应急指挥部成员单位应急处置中需要其他部门和本市网络安全应急技术支撑队伍配合和支持的，市应急指挥部办公室做好协调配合工作。其他部门和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。

⑦其他部门根据市应急指挥部办公室的通报，结合各自实际有针对地加强防范，防止造成更大范围影响和损失。

4.4 响应终止

4.4.1 I 级和 II 级应急响应结束

按照省网络安全应急指挥部办公室通报要求结束国家统一部署的 I 级应急响应、省统一部署的 II 级应急响应。市应急指挥部办公室根据鸡西市网络安全应急指挥部办公室的通报，在市委网络安全和信息化委员会统一领导、指挥协调下，配合省市网络安全应急指挥部组织的 I 级或 II 级应急响应结束工作。

特别重大（I级）网络安全事件应急处置涉及我市的相关工作按照省市要求的时限完成。重大（II级）网络安全事件应急处置要在7个工作日内完成，如网络安全事件的性质严重、影响范围广、处置难度大，可根据实际情况调整。

4.4.2 III 级和 IV 级响应结束

市应急指挥部办公室根据鸡西市应急指挥部办公室提出的结束III级或IV级应急响应行动要求，经市应急指挥部副总指挥审定，报总指挥批准同意后，及时通报市应急指挥部相关成员单位，配合鸡西市网络安全应急指挥部组织的III级或IV级应急响应结束工作。

较大（III级）网络安全事件应急处置要在72小时内完成，一般（IV级）网络安全事件应急处置要在48小时内完成。

5. 后期处置

5.1 善后处置

（1）网络安全事件处置结束后，要依据各自职责，依法依规对市应急指挥部各成员单位开展相关责任追究、损失补偿等工作，尽最大可能维护受害人合法权益。

（2）市应急指挥部办公室组织市应急指挥部成员单位对网络安全事件处置工作进行总结评估，总结经验教训，并形成专门报告上报市应急指挥部办公室。

（3）针对处置过程中暴露出的问题，市应急指挥部办公室和参与事件处置的市应急指挥部成员单位要提出整改措施，修改完善各自应急预案，视情况提出修订完善监管措施和风险预警机制相关建议，并协调、指导有关部门加强善后处置，防止出现类似

事件。

5.2 调查与评估

网络安全事件由市委网信办协调有关部门配合国家、省、鸡西市委网信办组织的调查和评估。总结调查报告应对事件起因、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. 应急保障

6.1 机构和人员

市应急指挥部各成员单位要落实网络安全工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制，定时组织开展培训和演练，提高应急队伍实战能力。

6.2 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。鼓励和引导各类网络安全技术机构和企业参与本市网络安全应急技术支持和保障工作。市委网信办按照国家标准，组织评估和认定本市网络安全应急技术支撑队伍。市应急指挥部各成员单位应配备必要的网络安全专业技术人才，并加强与各级各类网络安全技术机构和企业的沟通、合作，建立健全网络安全信息共享机制。

6.3 专家队伍

建立市网络安全应急专家组，为网络安全事件预防和处置提供技术咨询、决策建议，并参与事件应急处置工作。全市各部门各单位要加强网络专家队伍建设，充分发挥网络专家在应急

处置工作中的作用。

6.4 社会资源

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

6.5 基础平台

市委网信办统筹本市网络安全基础设施建设，统一规划建设网络安全应急基础平台和网络安全相关信息系统。市应急指挥部各成员单位加强网络安全应急相关信息系统建设，有条件的应与市级平台互联互通，资源共享。做到早发现、早预警、早响应，提高应急处置能力。

6.6 网络安全风险信息

市委网信办协调有关职能部门、网络安全社会组织、网络安全企事业单位加强网络安全风险信息搜集，完善信息共享机制，为网络安全应急工作提供信息支撑。

6.7 科技支撑

市应急指挥部各成员单位加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预警防护、处置救援、应急服务等方向，提升网络安全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。

6.8 加强合作

市应急指挥部有关成员单位建立市际合作渠道，签订合作协定，必要时通过市际合作共同应对网络安全事件，必要时通过县

（市）区合作共同应对网络安全事件。

6.9 应急物资

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。

6.10 应急经费

市应急指挥部各成员单位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，支持开展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、网络安全信息共享平台建设、技术研发、预案演练、物资保障等工作。

6.11 责任追究

对迟报、谎报、瞒报、漏报有关突发事故的信息，或者通报、报送、公布虚假信息的，造成后果的，构成玩忽职守不履行法定职责等行为的，依法予以处理；涉嫌犯罪的，依法移送司法机关。

7. 监督管理

7.1 应急预案演练

市委网信办按照省鸡西市有关要求，组织协调市应急指挥部成员单位定期开展综合性应急演练，检验和完善应急预案，提高实战能力。市应急指挥部各成员单位定期组织本系统应急演练，并将演练情况于每年12月前报送市委网信办，由市委网信办统一报送鸡西市委网信办。

7.2 宣教培训

市应急指挥部各成员单位应充分利用各种传播媒介及其他有效宣传形式，加强网络安全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。

市应急指挥部各成员单位要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，加强网络安全特别是网络安全应急预案的培训，提高防范意识和技能。

7.3 预案编制与更新

本预案由市委网信办牵头组织制定，报市政府批准后实施。本预案原则上每年评估一次，市委网信办根据实际情况按规定适时组织修订，并报鸡西市委网信办备案。

市应急指挥部各成员单位要根据本预案制定或修订本部门、本行业领域网络安全事件应急预案，要做好与本预案的衔接，并报市委网信办备案。

7.4 预案解释

本预案由市委网信办负责解释。

7.5 生效时间

本预案自印发之日起施行。

8. 附则

8.1 名词术语

8.1.1 网络安全事件及其分类

（1）网络安全事件

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。

（2）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、设施设备故障、灾害性事件和其他网

络安全事件等。

①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。

②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。

③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。

④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。

⑤设施设备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。

⑥灾害性事件是指由自然灾害等突发事件导致的网络安全事件。

⑦其他事件是指不能归为以上分类的网络安全事件。

8.1.2 关键信息基础设施

《中华人民共和国网络安全法》规定："国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定"。

8.1.3 重要网络与信息系统

重要网络与信息系统是指所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

8.1.4 重要敏感信息

重要敏感信息是指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公众利益密切相关的信息。这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果:

（1）损害国防、国际关系。

（2）损害国家财产、公共利益以及个人财产和人身安全。

（3）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等。

（4）影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为。

（5）干扰政府部门依法公正开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责。

（6）危害国家关键基础设施、政府信息系统安全。

（7）影响市场秩序，造成不公平竞争，破坏市场规律。

（8）可推论出国家秘密事项。

（9）侵犯个人隐私、企业商业秘密和知识产权。

（10）损害国家、企业、个人的其他利益和声誉。

8.2 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：

（1）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。

（2）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。

（3）较大的系统损失：造成系统中断，明显影响系统使用效率，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，但对于事发组织是可承受的。

（4）较小的系统损失：造成系统短暂中断，影响系统使用效率，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、可用性受到影响，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。

抄送：市委办公室。
市人大常委会办公室，市政协办公室，市法院，市检察院。

虎林市人民政府办公室　　2025年3月5日印发

共印70份。