# 绥化市人民政府办公室文件

绥政办发〔2021〕14号

## 绥化市人民政府办公室<br>关于印发绥化市网络安全事件<br>应急预案的通知

各县（市、区）人民政府，绥化经济技术开发区管委会，市政府各有关直属单位：

经市政府同意，现将《绥化市网络安全事件应急预案》印发给你们，请认真贯彻执行。

绥化市人民政府办公室

2021年8月4日

# 绥化市网络安全事件应急预案

## 目　录

## 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，特制定本预案。

### 1.2 编制依据

《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》《国家网络安全事件应急预案》《黑龙江省网络安全事件应急预案》《黑龙江省人民政府突发公共事件总体应急预案》《信息安全技术信息安全事件分类分级指南》（GB/Z20986-2007）等相关规定。

### 1.3 适用范围

本预案适用于本市发生的网络安全事件，以及发生在其他省（区、市）影响本市网络安全事件的预防、监测、报告和处置工作。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，分为有害程序事件、网络攻击事件、信息破坏事件、设施设备故障、灾害性事件和其他网络安全事件。

### 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，为较大网络安全事件：

①关键信息基础设施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

在市委网络安全和信息化委员会的领导下，市网络安全应急指挥部统一领导、组织和指挥网络安全事件应急处置工作。市网络安全应急指挥部指挥长由市政府分管副市长担任，副指挥长由协助分管副市长工作的市政府副秘书长和市委网

信办主要负责人担任。市委网信委委员单位和市委保密和机要局、市通信管理办公室、国网绥化供电公司、中国联通绥化分公司、中国移动绥化分公司、中国电信绥化分公司等有关部门为市网络安全应急指挥部成员单位。

市网络安全应急指挥部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，建立健全预防和应对网络安全事件的各项应急机制，密切配合，形成应对和处置网络安全事件工作合力。

2.2 办事机构与职责

市网络安全应急指挥部办公室设在市委网络安全和信息化委员会办公室（市互联网信息办公室，以下简称市委网信办），具体工作由市委网信办承担。市网络安全应急指挥部办公室主任由市委网信办主要负责人担任。主要职责是统筹协调组织本市网络安全事件应对工作，建立健全跨部门应急联动机制，承担网络安全应急跨部门、跨县（市、区）协调工作和指挥部的事务性工作，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。市网络安全应急指挥部成员单位相关业务科室主要负责人为市网络安全应急指挥部办公室联络员。

2.3 各部门职责

中省市直各部门按照职责和权限，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；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，并向市网络安全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 各县（市、区）职责

各县（市、区）网信部门在本级党委网络安全和信息化委员会的统一领导下，统筹协调组织本地区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

网络运营者及网络产品、服务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。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；在发生危害网络安全事件时，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。网络产品、服务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，分别对应发生或者可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“属地管理、分级负责”“谁主管谁负责、谁运行谁负责”的原则，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。各县（市、区）网信部门结合本地实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各县（市、区）、各部门要将重要监测信息报市委网信办，市委网信办组织开展跨县（市、区）、跨部门网络安全信息共享。

3.3 预警研判和发布

各县（市、区）、各部门组织对本地、本部门、本行业网络安全监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生较大以上网络安全事件的信息及时向市网络安全应急指挥部办公室报告。各县（市、区）、各部门可根据监测研判情况，发布本地、本行业蓝色预警。

市网络安全应急指挥部办公室组织研判，确定和发布黄色及以下预警和涉及多县（市、区）、多部门、多行业预警。橙色预警报请省委网信办发布。红色预警逐级上报省委网信

办，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 预警响应

3.4.1 红色预警响应

（1）红色预警响应报请中央网信办统一组织实施，省网络安全应急指挥部配合国家统一行动，并做好本省预警响应工作，市网络安全应急指挥部配合省统一行动，并做好本市预警响应工作。

（2）市网络安全应急指挥部按照市委网络安全和信息化委员会和省委网信办要求，组织预警响应工作，联系专家和有关机构，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各项准备工作。

（3）市网络安全应急指挥部办公室、有关县（市、区）和部门网络安全应急指挥机构实行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或准备、风险评估和控制工作，按照规定及时向市网络安全应急指挥部办公室报送事件信息。

（4）市网络安全应急技术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）橙色预警响应报请省委网信办统一组织实施，市网络安全应急指挥部配合省统一行动，并做好本市预警响应工作。

（2）市网络安全应急指挥部办公室按照市网络安全应急指挥部部署，组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定预防措施和应急工作方案，协调组织资源调度和部门联动各项准备工作。

（3）市网络安全应急指挥部办公室、有关县（市、区）和部门网络安全事件应急指挥机构实行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或准备、风险评估和控制工作，按照规定及时向市网络安全应急指挥部办公室报送事件信息。

（4）市网络安全应急技术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。

（5）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服务合同要求做好应急准备工作。

3.4.3 黄色预警响应

（1）黄色预警响应由市网络安全应急指挥部统一组织实施，各县（市、区）网络安全应急指挥部配合市统一行动，并做好本县（市、区）预警响应工作。

（2）有关县（市、区）、部门网络安全事件应急指挥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工作。

（3）有关县（市、区）、部门及时将事件事态发展情况报市网络安全应急指挥部办公室。市网络安全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县（市、区）和部门。

（4）有关县（市、区）、部门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。

3.4.4 蓝色预警响应

有关县（市、区）、部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

3.5 预警解除

预警发布部门根据实际情况，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本单位网络安全事件应急预案，实施处置并按照规定及时报送信息。各有关县（市、区）、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息报送工作。

各级、各部门要建立健全网络安全事件信息报告机制。确认为一般（IV 级）或较大（Ⅲ级）网络安全事件发生后，各县（市、区）网信部门要在事件发生后4小时内，向市网络安全应急指挥部办公室报告有关情况，市网络安全应急指挥部办公室向省网络安全应急指挥部办公室报告有关情况。对于初判为特别重大（Ⅰ级）、重大（Ⅱ级）网络安全事件的，应立即报告本级网络安全和信息化委员会及市网络安全应急指挥部办公室。市网络安全应急指挥部办公室按有关要求上报省委网信办，省网络安全应急指挥部办公室按有关要求上报中央网信办。同时上述信息按有关要求报送市政府。

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

4.2.1 I级和II级响应

市网络安全应急指挥部办公室组织对事件信息进行研判，属特别重大网络安全事件和重大网络安全事件的，及时向市委网络安全和信息化委员会提出启动I级或II级响应的建议，经批准后，启动应急指挥体系。属于I级、II级网络安全事件的，市委网络安全和信息化委员会需向省委网络安全和信息化委员会提出启动I级、II级响应建议。属于I级网络安全事件的，还需报请省委网络安全和信息化委员会向中央网络安

全和信息化委员会提出启动I级响应建议。市网络安全应急指挥部配合国家、省I级、II级响应，并做好本市I级、II级响应工作。

（1）启动指挥体系。

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

②有关各县（市、区）、部门应急指挥机构进入应急状态，在市网络安全应急指挥部统一领导、指挥、协调下，负责本县（市、区）、本部门应急处置工作或支援保障工作，相关工作人员24小时值班，并派员参加市网络安全应急指挥部办公室工作。

（2）掌握事件动态。

①跟踪事态发展。事件发生县（市、区）或部门及时将事态发展变化情况和处置进展情况报市网络安全应急指挥部办公室。

②检查影响范围。有关县（市、区）和部门立即全面了解本地区、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网络安全应急指挥部办公室。

③及时通报情况。市网络安全应急指挥部办公室负责汇总上述有关情况，重大事项及时报省委网信办和市网络安全

应急指挥部，并通报有关县（市、区）和部门。

（3）决策部署。

市网络安全应急指挥部组织有关县（市、区）、部门以及专家组、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）处置实施。

①控制事态防止蔓延。市网络安全应急指挥部组织有关县（市、区）和部门尽快控制事态，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。有关县（市、区）和部门根据事件发生原因，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、网络产品和服务提供者依法为网络安全事件调查取证工作提供技术支持和协助。

④省、市际协调。有关部门根据国家有关规定，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。

⑤协调配合网络安全事件引发的其他突发事件应急处置。对于引发或可能引发其他特别重大和重大安全事件的，市网络安全应急指挥部办公室应及时按照程序上报。在相关部门应急处置中，市网络安全应急指挥部办公室做好协调配合工作。

4.2.2 III 级响应

网络安全事件的 III 级响应，由市网络安全应急指挥部根据事件的性质和情况确定，并将有关情况报省网络安全应急指挥部办公室。

（1）事件发生县（市、区）或部门应急指挥机构进入应急状态，按照相关预案做好应急处置工作。

（2）事件发生县（市、区）或部门及时将事态发展变化情况报市网络安全应急指挥部办公室。市网络安全应急指挥部办公室将有关重大事项及时通报相关县（市、区）和部门。

（3）处置中需要其他县（市、区）、部门和本市网络安全应急技术支撑队伍配合和支持的，由市网络安全应急指挥部办公室予以协调。相关县（市、区）、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。

（4）有关县（市、区）或部门根据市网络安全应急指挥部办公室通报，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。

4.2.3 IV 级响应

事件发生县（市、区）或部门按照相关预案进行应急响应。

4.3 应急结束

4.3.1 I 级响应结束

按照国家统一部署结束I级响应。市网络安全应急指挥部办公室及时通报有关县（市、区）和部门。特别重大网络安全事件应急处置涉及我市的相关工作按照国家要求时限完成。

4.3.2 II 级响应结束

按照省统一部署结束 II 级响应。市网络安全应急指挥部办公室及时通报有关县（市、区）和部门。重大网络安全事件应急处置要在 7 个工作日内完成，如网络安全事件性质严重、影响范围广、处置难度大，可根据实际情况调整。

4.3.3 III 级和 IV 级响应结束

III级响应结束由市网络安全应急指挥部办公室提出建议，经市网络安全应急指挥部同意后，报市委网络安全和信息化委员会批准后及时通报有关县（市、区）和部门。IV 级响应结束由事件发生县（市、区）或部门决定，报市网络安全应急指挥部办公室。III 级网络安全事件应急处置要在72小时内完成，IV级网络安全事件应急处置要在48小时内完成。

**5 调查与评估**

特别重大、重大网络安全事件由市委网信办协调有关县（市、区）和部门配合国家、省调查评估，并按程序上报。较大网络安全事件由市委网信办组织县（市、区）和有关部门进行调查处理和总结评估，并按程序上报。一般网络安全事

件由事件发生县（市、区）或部门自行组织调查处理和总结评估，其中：一般网络安全事件相关总结调查报告报市委网信办。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

各县（市、区）、各部门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发生及危害，提高应对网络安全事件能力。

### 6.2 演练

市委网信办按省有关要求，协调有关部门定期组织演练，检验和完善预案，提高实战能力。各县（市、区）、各部门、各单位定期组织应急演练，并将演练情况于每年的12月之前报送市委网信办。

### 6.3 宣传

各级、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强网络安全有关法律法规和政策宣传，开展网络安全基本知识和技能宣传活动。

6.4 培训

各级、各部门要将网络安全事件应急知识列为领导干部和有关人员培训内容，加强网络安全特别是网络安全应急预案培训，提高防范意识和技能。

6.5 重要活动期间预防措施

在国家和本省、市重要活动、会议期间，各县（市、区）、各部门要加强网络安全事件防范和应急响应，确保网络安全。市委网信办统筹协调网络安全保障工作，根据实际要求有关县（市、区）、部门启动红色、橙色或黄色预警响应。有关县（市、区）、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。

**7 保障措施**

7.1 机构和人员

各级、各部门、各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。

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，市网络安全和舆情应急指挥中心做

好市内重大网络安全事件监测预警、风险控制、应急处置和技术支撑工作。各县（市、区）、各部门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。

7.3 专家队伍

建立市网络安全应急专家组，职责是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。各级、各部门加强各自专家队伍建设，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、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，提高应对特别重大、重大、较大网络安全事件能力。

7.5 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。各县（市、区）、各部门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。

7.6 网络安全风险信息

各级网信部门协调有关职能部门、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。

7.7 技术研发和产业促进

各有关部门要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。

7.8 省、市际合作

各有关部门要建立省、市际合作渠道，签订合作协定，必要时通过省、市际合作共同应对网络安全事件。

7.9 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。

7.10 经费保障

各级、各部门为网络安全事件应急处置提供必要的资金保障。各有关部门利用现有政策和资金渠道，支持网络安全应急技术队伍建设、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、物资保障等工作开展。

7.11 责任追究

网络安全事件应急管理工作实行责任追究制。对不按照规定制定应急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；涉嫌犯罪的，依法移送司法机关。

**8 附则**

8.1 预案管理

本预案原则上每年评估一次，根据实际情况按规定适时修订。修订具体工作由市委网信办负责。

各县（市、区）、各部门要根据本预案制定或修订本地区、本部门、本行业、本领域、本单位网络安全事件应急预案，各预案要做好与本预案的衔接，并报市委网信办备案。

8.2 预案施行时间

本预案自印发之日起施行。《绥化市人民政府办公室关于印发绥化市网络安全事件应急预案的通知》（绥政办发〔2018〕15号）同时废止。

附件：1．名词术语

2．网络和信息系统损失程度划分说明

附件1

# 名词术语

## 一、网络安全事件及其分类

（一）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。

（二）网络安全事件分类。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。

**二、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”。

**三、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。

**四、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：

（一）损害国防、国际关系；

（二）损害国家财产、公共利益以及个人财产和人身安全；

（三）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；

（四）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；

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

（六）危害国家关键基础设施、政府信息系统安全；

（七）影响市场秩序，造成不公平竞争，破坏市场规律；

（八）可推论出国家秘密事项；

（九）侵犯个人隐私、企业商业秘密和知识产权；

（十）损害国家、企业、个人的其他利益和声誉。

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；

**四、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。

抄送：市委各单位，中省直驻绥各单位。
市人大办，市检察院，市中级人民法院。

绥化市人民政府办公室　　2021年8月4日印发