贵州省公共互联网网络安全突发事件应急预案

贵州省通信管理局

2024 年 11 月

目 录

1. 总则

1.1 编制目的

建立健全贵州省公共互联网网络安全突发事件应急组织体系和工作机制，提高本省公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除公共互联网网络安全突发事件造成的社会危害和损失，保证本省公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行安全和社会秩序稳定。

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》《中华人民共和国电信条例》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《公共互联网网络安全突发事件应急预案》《贵州省突发事件应急预案管理办法》等相关规定，制定本预案。

1.3 适用范围

本预案适用于贵州省面向社会提供服务的基础电信企业、域名注册管理和服务机构（以下简称域名机构）、互联网企业（含工业互联网平台企业、标识解析企业）发生网络安全突发事件的应对工作。

本预案所称网络安全突发事件，是指突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社

会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、病毒传播等事件。

本预案所称电信主管部门包括工业和信息化部及贵州省通信管理局。

工业和信息化部、中共贵州省委、贵州省人民政府对国家和本省重大活动期间网络安全突发事件应对工作另有规定的，从其规定。

1.4 工作原则

贵州省公共互联网网络安全突发事件应急工作坚持统一领导、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；落实基础电信企业、域名机构、互联网服务提供者的主体责任；充分发挥网络安全技术支撑单位、网络安全企业和专家学者等各方面力量的作用。

2. 组织体系

2.1 领导机构与职责

在工业和信息化部、中共贵州省委、贵州省人民政府的领导下，贵州省通信管理局网络安全工作领导小组（以下简称局网安领导小组）统一组织领导本省公共互联网网络安全突发事件应急管理工作，负责本省公共互联网网络安全突发事件的统一指挥和协调。

局网安领导小组组长由贵州省通信管理局局长担任，副组长由贵州省通信管理局分管领导担任，成员由省内基础电信企业、域名机构、互联网企业主要负责人担任。

2.2 办事机构与职责

在工业和信息化部网络安全应急办公室（以下简称部应急办）和局网安领导小组领导下，贵州省通信管理局网安应急办公室（以下简称局网安应急办）负责贯彻执行部应急办和局网安领导小组相关指示和部署，负责本省网络安全应急管理事务性工作，及时向部应急办和局网安领导小组报告突发事件的情况，提出特别重大、重大网络安全突发事件应对措施建议；负责较大、一般网络安全突发事件的统一指挥和协调。

局网安应急办主任由贵州省通信管理局分管领导兼任，具体工作由贵州省通信管理局网络安全管理处承担，有关单位应明确负责人和联络员，参与局网安应急办工作。

2.3 其他相关单位职责

省内基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持，并及时向局网安应急办上报事件处置进展情况。

网络安全技术支撑单位受贵州省通信管理局委托，协助监测、报告贵州省公共互联网网络安全突发事件和预警信息，为应急工作提供决策支持和技术支撑。

鼓励省内网络安全企业参与支撑公共互联网网络安全突发事件应急工作。

3.事件分级

根据社会影响范围和危害程度，公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。

3.1 特别重大事件

符合下列情形之一的，为特别重大网络安全事件：

（1）全国范围大量互联网用户无法正常上网；

（2）.CN 国家顶级域名系统解析效率大幅下降；

（3）1 亿以上互联网用户信息泄露；

（4）网络病毒在全国范围大面积爆发；

（5）其他造成或可能造成特别重大危害或影响的网络安全事件。

3.2 重大事件

符合下列情形之一的，为重大网络安全事件：

（1）多个省大量互联网用户无法正常上网；

（2）在全国范围有影响力的网站或平台访问出现严重异常；

（3）大型域名解析系统访问出现严重异常；

（4）1 千万以上互联网用户信息泄露；

（5）网络病毒在多个省范围内大面积爆发；

（6）其他造成或可能造成重大危害或影响的网络安全事件。

3.3 较大事件

符合下列情形之一的，为较大网络安全事件：

（1）省内大量互联网用户无法正常上网；

（2）省内有影响力的网站或平台访问出现严重异常；

（3）100 万以上互联网用户信息泄露；

（4）网络病毒在省内大面积爆发；

（5）其他造成或可能造成较大危害或影响的网络安全事件。

3.4 一般事件

符合下列情形之一的，为一般网络安全事件：

（1）1 个地市大量互联网用户无法正常上网；

（2）10 万以上互联网用户信息泄露；

（3）其他造成或可能造成一般危害或影响的网络安全事件。

4. 监测预警

4.1 事件监测

省内基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的

网络安全突发事件，应当立即向局网安应急办报告，不得迟报、谎报、瞒报、漏报。

网络安全技术支撑单位、网络安全企业应当通过多种途径监测、收集已经发生的公共互联网网络安全突发事件信息，并及时向局网安应急办报告。

报告突发事件信息时，应按《贵州省公共互联网网络安全突发事件报送表》（附件）进行填报，并电话确认报送结果。如遇特殊情况，在第一时间通过其他快速便捷方式报送事件信息，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议，《贵州省公共互联网网络安全突发事件报送表》应在事发当日进行补报。

4.2 预警监测

省内基础电信企业、域名机构、互联网企业、网络安全技术支撑单位、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估；认为可能发生网络安全突发事件的，应当立即向局网安应急办报告。

4.3 预警分级

建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全

突发事件。

4.4 预警发布

局网安应急办应当及时汇总分析突发事件隐患和预警信息，必要时组织相关单位、专业技术人员、专家学者进行会商研判。

对于国家网络安全应急办公室发布的红色预警和部应急办发布的橙色预警，局网安应急办应当立即向局网安领导小组报告，并及时通告省内相关单位及互联网用户。

认为需要发布黄色、蓝色预警的，由局网安应急办报请局网安领导小组同意后，可在本省内发布，并报部应急办，同时通报省应急管理相关部门。对于达不到预警级别但又需要发布警示信息的，局网安应急办可以在本省发布风险提示信息。

发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。面向社会发布预警信息可通过网站、短信、微信等多种形式。

4.5 预警响应

4.5.1 红色、橙色预警响应

接到发布的红色、橙色预警后，局网安应急办应立即向局网安领导小组报告，除采取黄色、蓝色预警响应措施外，还应在部应急办和局网安领导小组的领导下，针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

（1）要求各相关单位实行24小时值班，相关人员保持通信联络畅通；

（2）组织研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备工作，重要情况报部应急办和局网安领导小组；

（3）组织有关单位加强对重要网络、系统的网络安全防护；

（4）要求省内网络安全技术支撑单位、网络安全企业及专家进入待命状态，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。

4.5.2 黄色、蓝色预警响应

发布黄色、蓝色预警后，局网安应急办应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

（1）要求有关单位、机构和人员及时收集、报告有关信息，加强网络安全风险的监测；

（2）组织有关单位、机构和人员加强事态跟踪分析评估，密切关注事态发展，重要情况报部应急办和局网安领导小组；

（3）及时宣传避免、减轻危害的措施，公布咨询电话，并对相关信息的报道工作进行正确引导。

4.6 预警解除

红色、橙色预警调整及解除应当按照部应急办统一安排在本省内执行，同时上报局网安领导小组。

针对黄色、蓝色预警，局网安应急办应当根据事态发展，及时向局网安领导小组报告，经批准后适时调整预警级别并按

照权限重新发布；经研判不可能发生突发事件或风险已经解除的，应当报请局网安领导小组同意后宣布解除预警，并解除已经采取的有关措施，并及时上报部应急办，同时通报省应急管理相关部门。

5. 应急处置

5.1 响应分级

公共互联网网络安全突发事件应急响应分为四级：I 级、II 级、III 级、IV 级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

5.2 先行处置

本省发生公共互联网网络安全突发事件发生后，事发单位在按照本预案规定立即向局网安应急办报告的同时，应当立即启动本单位应急预案，组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。

事发单位在先期处置时根据需要可向局网安应急办请求支援，局网安应急办可安排贵州省通信管理局网络安全专家组成员提供技术支援，各单位接到调派指令后，应积极响应并提供必要的协助和配合。

5.3 启动响应

I 级响应根据国家有关决定或经部领导小组批准后启动，由部领导小组统一指挥、协调。

II 级响应由部应急办决定启动，由部应急办统一指挥、协调。

III 级、IV 级响应经局网安领导小组批准后启动，由局网安应急办负责指挥、协调。

启动 I 级、II 级响应后，局网安应急办及其他相关单位在部应急办统一指挥协调下，组织开展相关应急工作。

启动 III 级、IV 级响应后，局网安应急办和相关单位进入应急状态，省内基础电信企业、域名机构、互联网企业、网络安全技术支撑单位等相关单位及时向局网安应急办报送情况，报送内容应包含已采取的应急处置措施、处置时间、达到的效果、下一步处置计划和有关建议；相关人员保持 24 小时联络畅通；局网安应急办视情设立应急恢复、攻击溯源、影响评估、信息发布、跨部门协调等工作组，并及时将相关情况报部应急办和局网安领导小组。

5.4 事态跟踪

启动 I 级、II 级响应后，在部应急办的统一指挥、协调下，局网安应急办应立即了解本省受影响情况，并报部应急办和局网安领导小组。

启动 III 级、IV 级响应后，事发单位、网络安全技术支撑单位和网络安全企业应当持续加强监测，跟踪事态发展，检查

影响范围，密切关注舆情，及时将事态发展变化、处置进展情况、相关舆情报局网安应急办。局网安应急办及时全面了解全省受影响情况，并报部应急办和局网安领导小组。

5.5 决策部署

启动Ⅰ级、II级响应后，在部应急办的统一指挥协调下，局网安应急办立即组织开展相关应急处置工作，并及时将处置情况报部应急办和局网安领导小组。

启动III级、IV级响应后，局网安应急办组织相关单位开展应急处置工作，针对突发事件的类型、特点和原因，要求相关单位采取以下措施：带宽紧急扩容、控制攻击源、过滤攻击流量、修补漏洞、查杀病毒、关闭端口、启用备份数据、暂时关闭相关系统等；对省内大规模用户信息泄露事件，要求事发单位及时告知受影响的用户，并告知用户减轻危害的措施；防止发生次生、衍生事件的必要措施；其他可以控制和减轻危害的措施。必要时报部应急办协调其他区域提供配合与支持。

做好信息报送。省内相关单位应及时向局网安应急办等报告突发事件处置进展情况，局网安应急办视情况向省内相关职能部门、相关行业主管部门通报突发事件有关情况，必要时向部应急办和相关部门请求提供支援。

注重信息发布。省内相关单位应及时向社会公众通告突发事件情况，宣传避免或减轻危害的措施，公布咨询电话，引导社会舆论。未经局网安应急办同意，各相关单位不得擅自向社会发布突发事件相关信息。

5.6 结束响应

突发事件的影响和危害得到控制或消除后，I 级、II 级响应根据部应急办相关规定结束，III、IV 级响应由局网安应急办报请局网安领导小组批准后决定结束，并报部应急办，同时通报省应急管理相关部门。

6. 事后总结

6.1 调查评估

公共互联网网络安全突发事件应急响应结束后，事发单位要及时调查突发事件的起因（包括直接原因和间接原因）、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后 10 个工作日内形成总结报告，报局网安应急办。局网安应急办应在应急响应结束后 20 个工作日内形成报告，报部应急办和局网安领导小组。

6.2 奖惩问责

贵州省通信管理局对本省网络安全突发事件应对工作中作出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由贵州省通信管理局给予约谈、通报或依法、依规给予问责。省内基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

7. 预防与应急准备

7.1 预防保护

省内基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。电信主管部门依法开展网络安全监督检查，指导督促相关单位消除安全隐患。

7.2 应急演练

贵州省通信管理局应当组织开展贵州省公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。省内基础电信企业、互联网企业、域名机构要积极参与贵州省通信管理局组织的应急演练，并应每年组织开展至少一次本单位网络安全应急演练，应急演练情况要向贵州省通信管理局报告。

7.3 宣传培训

贵州省通信管理局组织开展网络安全相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关企业和社会公众

的网络安全意识和防护、应急能力，各相关企业应积极参加。省内基础电信企业、域名机构、互联网企业要面向本单位员工加强网络安全应急宣传教育和培训，建立健全本单位应急工作培训制度，对本单位员工进行培训，使其熟悉应急预案规则和流程，学习网络安全突发事件应急技术，提高应急工作技能，确保应急预案的有效实施。鼓励开展各种形式的网络安全竞赛。

7.4 手段建设

贵州省通信管理局指导省内基础电信企业、大型互联网企业、域名机构等单位规划建设本单位突发事件信息系统，并与贵州省网络安全威胁联动应急处置平台实现互联互通。

7.5 工具配备

省内基础电信企业、域名机构、互联网企业和网络安全技术支撑单位应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的储备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。

8. 保障措施

8.1 落实责任

省内基础电信企业、域名机构、互联网企业、网络安全技术支撑单位要落实网络安全应急工作责任制，把责任落实到单位领导、具体部门、具体岗位和个人，建立健全本单位网络安全应急工作体制机制。

8.2 经费保障

省内基础电信企业、域名机构、大型互联网企业为开展公共互联网网络安全突发事件应对工作提供必要的经费保障，支持本单位网络安全应急队伍建设、手段建设、应急演练、应急培训等工作的开展。

8.3 队伍建设

省内基础电信企业、域名机构、大型互联网企业要建立专门的网络安全应急队伍，提升本单位网络安全应急能力。支持网络安全企业提升应急支撑能力，促进网络安全应急产业发展。

8.4 社会力量

建立贵州省通信管理局网络安全专家组，充分发挥专家在应急处置工作中的作用。从通信企业、网络安全技术支撑单位、网络安全企业、科研院所、高等学校中选拔网络安全技术人才，形成网络安全技术人才库。

8.5 对外合作

贵州省通信管理局加强同省内外网络安全应急管理机构的工作交流。鼓励省内基础电信企业、互联网企业、网络安全技术支撑单位、网络安全企业开展网络安全跨区域交流与合作。

9. 附则

9.1 预案管理

本预案根据实际情况由贵州省通信管理局适时进行修订。

基础电信企业、域名机构、互联网企业要制定本单位公共互联网网络安全突发事件应急预案。基础电信企业、域名机构、大型互联网企业的应急预案要向贵州省通信管理局备案。

9.2 预案解释

本预案由贵州省通信管理局负责解释。

9.3 预案实施时间

本预案自印发之日起实施。2019 年 1 月 21 日印发的《贵州省公众互联网网络安全应急预案》同时废止。

附件

贵州省公共互联网网络安全事件报送表

填表人：　　填报时间：　年　月　日　时

<table>
<tr><td rowspan="3">单位基本情况</td><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>单位所属类型</td><td colspan="6">☐基础电信企业　☐域名机构　☐互联网企业
☐网络安全技术支撑单位　☐网络安全企业　☐其它：</td></tr>
<tr><td>联系人姓名</td><td></td><td>电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td rowspan="4">安全事件基本情况</td><td>涉事网络单元名称</td><td colspan="6"></td></tr>
<tr><td>涉事网络单位地址</td><td colspan="6"></td></tr>
<tr><td>事件简要描述</td><td colspan="6"></td></tr>
<tr><td>事件发生时间</td><td colspan="2"></td><td>发现时间</td><td colspan="3"></td></tr>
<tr><td rowspan="7">事件情况初判</td><td>事件类型</td><td colspan="6">☐互联网用户无法正常上网　☐域名解析系统异常
☐重要网站平台访问异常　☐互联网用户信息泄露
☐网络病毒爆发 ☐其它：</td></tr>
<tr><td rowspan="5">当前影响和破坏情况</td><td colspan="6">互联网用户无法正常上网：☐全国范围　☐若干省
☐全省范围　☐若干区县　☐区县</td></tr>
<tr><td colspan="6">域名解析系统严重异常：☐完全无法访问　☐效率下降导致延迟时间为毫秒</td></tr>
<tr><td colspan="6">重要网站平台访问异常：☐在全国范围有影响力
☐在省内有影响力
是否为关键信息基础设施　☐是　☐否</td></tr>
<tr><td colspan="6">互联网用户信息泄露：
☐一亿条以上　☐一千万条以上　☐一百万条以上
☐十万条以上　☐十万条以下</td></tr>
<tr><td colspan="6">网络病毒爆发：☐全国范围　☐若干省　☐全省范围
☐ 若干区县　☐区县</td></tr>
<tr><td>建议事件级别</td><td colspan="6">☐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　☐其它：</td></tr>
<tr><td rowspan="3">已启用应急措施及有关建议</td><td>已启动应急预案名称</td><td colspan="6"></td></tr>
<tr><td>已启动本单位应急响应级别</td><td colspan="6">☐I 级　☐II 级　☐III 级　☐IV 级</td></tr>
<tr><td>已采取应急措施</td><td colspan="6"></td></tr>
</table>

	建议采取工作措施	
技术支持	是否需要技术支持	□是 □否
	需要技术支持类型	□专家咨询 □应急队伍 □技术设备 □其它：