贵州省电信领域数据安全事件应急预案
（试行）

1.总则

1.1 编制目的

建立健全贵州省电信领域数据安全事件应急组织体系和工作机制，提高数据安全事件综合应对能力，确保及时有效地控制、减轻和消除数据安全事件造成的危害和损失，保护个人、组织的合法权益，维护国家安全和公共利益，保障经济运行和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规和《国家突发事件总体应急预案》《工业和信息化领域数据安全管理办法（试行）》《工业和信息化领域数据安全事件应急预案（试行）》《贵州省突发事件应急预案管理办法》等相关政策制度。

1.3 适用范围

在贵州省内发生的电信领域数据安全事件应急处置活动，应当遵守相关法律法规、政策制度和本预案的要求。

工业和信息化部、中共贵州省委、贵州省人民政府对重大活动期间数据安全事件应急处置工作另有规定的，从

其规定。

1.4 事件定义

本预案所称数据安全事件，是指数据遭篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

1.5 事件分级

根据数据安全事件对国家安全、企业网络设施和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将数据安全事件分为特别重大、重大、较大和一般四个级别（见附件 1）。

1.6 工作原则

贵州省电信领域数据安全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；坚持“谁管业务、谁管业务数据、谁管数据安全”，落实数据处理者的数据安全主体责任；坚持充分发挥各方面力量，共同做好数据安全事件应急处置工作。

2. 组织体系

2.1 领导机构与职责

在工业和信息化部网络安全和信息化领导小组（以下

简称部网信领导小组）统一领导和工业和信息化领域数据安全工作机制（以下简称部数据安全机制）统筹安排下，贵州省通信管理局成立网络安全工作领导小组（以下简称局网安领导小组）统一负责开展贵州省电信领域数据安全事件应急处置工作。

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

局网安领导小组下设网安应急办公室（以下简称局网安应急办）。

局网安应急办负责牵头开展贵州省电信领域数据安全事件应急处置工作；及时向部数据安全机制报告数据安全事件情况，提出特别重大、重大数据安全事件应对措施建议；负责较大数据安全事件的统一指挥和协调处置；根据需要协调一般数据安全突发事件的应急处置。

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 数据处理者职责

贵州省电信领域数据处理者（以下简称数据处理者）负责本单位数据安全事件预防、监测、应急处置、报告等工作，应当根据应对数据安全事件的需要，制定本单位数据安全事件应急预案。

2.4 应急支撑机构职责

贵州省通信管理局根据需要遴选贵州省数据安全应急支撑机构（以下简称应急支撑机构）。应急支撑机构协助贵州省通信管理局开展数据安全事件预防保护、监测预警、应急处置、攻击溯源等工作。

2.5 协调联动

贵州省通信管理局按照有关法律、行政法规，与有关部门加强协同联动，依法配合有关部门开展数据安全事件应急处置工作。

3.监测预警

3.1 预警监测和报告

贵州省通信管理局、数据处理者、应急支撑机构应当按照《工业和信息化领域数据安全管理办法（试行）》、工业和信息化领域数据安全风险信息报送与共享等要求，加强数据安全风险监测、研判和上报，分析相关风险发生数据安全事件的可能性及其可能造成的影响。

贵州省通信管理局认为可能发生重大及以上数据安全事件的，应当立即上报部数据安全机制。

数据处理者、应急支撑机构认为可能发生较大及以上数据安全事件的，应当立即上报贵州省通信管理局（模板见附件2）。

3.2 预警分级

根据紧急程度、发展态势、数据规模、关联影响和现实危害等，数据安全风险预警等级分为四级：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、较大和一般数据安全事件。

贵州省通信管理局及时汇总分析数据安全风险和预警信息，必要时组织应急支撑机构、专家、相关企业进行会商谈判，明确预警等级。

3.3 预警发布

红色、橙色预警由部数据安全机制统一发布；黄色、蓝色预警由贵州省通信管理局在贵州省电信领域内发布。

发布预警信息时，应当包括预警等级、起始时间、可能的影响范围和造成的危害、警示事项、应采取的防范措施、处置时限要求、发布范围和发布机关等。

3.4 预警响应

发布黄色和蓝色预警后，贵州省通信管理局应当针对即将发生的数据安全事件特点和可能造成的危害，采取下列措施：

（1）要求涉及预警信息的数据处理者及时收集、报告有关信息，加强数据安全风险监测；

（2）组织应急支撑机构加强预警信息分析评估与事态跟踪，密切关注事态发展，提出下步工作措施；

（3）组织专家加强风险研判及原因、影响等分析，提出应急处置方法和整改措施建议。

接到红色和橙色预警后，贵州省通信管理局除采取黄色和蓝色预警响应措施外，还应当针对即将发生的数据安全事件特点和可能造成的危害，采取下列措施：

（1）组织涉及预警信息的数据处理者等相关单位和部门加强值班值守，相关人员保持通信联络畅通；

（2）落实部网信领导小组、部数据安全机制下达的防范措施和应急工作方案。

3.5 预警调整和解除

部数据安全机制、贵州省通信管理局发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布。经研判不可能发生事件或风险已经解除的，应当及时宣布

解除预警，并解除已经采取的有关预警响应措施。

4. 事件响应

4.1 响应分级

数据安全事件应急响应分为四级：一级、二级、三级、四级，分别对应发生特别重大、重大、较大、一般数据安全事件的应急响应。

4.2 事件监测和报告

数据处理者一旦发现数据安全事件，应当立即先行判断，对自判为较大及以上事件的，应当立即向贵州省通信管理局报告，不得迟报、谎报、瞒报、漏报。

应急支撑机构应当通过多种途径监测、收集数据安全事件信息，及时向贵州省通信管理局报告。

贵州省通信管理局初步研判为特别重大、重大数据安全事件的，应当在发现事件后按照“电话 10 分钟、书面 30 分钟”的要求向部数据安全机制报告。

报告事件研判信息时，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。

4.3 先行处置

数据安全事件发生后，数据处理者应当立即启动应急

响应工作，组织本单位应急队伍和工作人员采取应急处置措施，开展数据恢复或追溯工作，尽可能减少对用户和社会的影响，同时保存相关痕迹和证据。

4.4 应急响应

部数据安全机制、贵州省通信管理局视情况组织应急支撑机构、专家等进行研判，确定事件级别和响应等级，启动应急响应。

4.4.1 一级响应

接到部数据安全机制启动应急响应的通知后，贵州省通信管理局立即启动贵州省电信领域数据安全事件应急预案，进入应急状态，加强值班值守，相关人员保持联络畅通，派员参加部数据安全机制工作；加强事件跟踪监测、研判分析和排查处置，全面了解贵州省电信领域相关数据处理者受事件影响情况。

涉事数据处理者立即进入应急状态，数据安全第一责任人（本单位法定代表人或主要负责人）牵头组建事件应对工作专班，组织研究应对措施，统筹开展应急处置工作。数据安全直接责任人（本单位数据安全工作分管领导）对应急处置工作进行具体部署，组织专班加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，

评估影响范围和事件原因，采取有效整改处置措施，并及时汇报工作进展和处置情况。

应急支撑机构进入应急状态，加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

4.4.2 二级响应

接到部数据安全机制启动应急响应的通知后，贵州省通信管理局立即启动贵州省电信领域数据安全事件应急预案，进入应急状态，相关人员保持联络畅通，派员参加部数据安全机制工作；加强事件跟踪监测、研判分析和排查处置，全面了解贵州省电信领域相关企业受事件影响情况。

涉事数据处理者立即进入应急状态，数据安全直接责任人牵头研究应对措施，统筹部署开展应急处置工作，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时汇报工作进展和处置情况。

应急支撑机构进入应急状态，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

4.4.3 三级响应

由贵州省通信管理局按照本预案决定启动，并负责指挥、协调。

贵州省通信管理局组织涉事数据处理者、应急支撑机构等加强事态跟踪研判、开展事件处置，及时将事件进展及重要情况报贵州省通信管理局和部数据安全机制，通知可能受影响的其他区域做好数据安全应急处置工作。

涉事数据处理者持续开展监测分析，跟踪事态发展，评估影响范围和事件原因；加强相关业务系统应用安全加固措施，提升数据安全防护能力，采取有效整改处置措施，并及时汇报工作进展和处置情况。

应急支撑机构持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

4.4.4 四级响应

由涉事数据处理者按照本预案决定启动，并应当按照行业数据安全保护相关政策标准及时采取有效措施处置事件，加强数据安全防护。

4.4.5 响应级别调整

涉事数据处理者可根据事态发展等情况，向贵州省通信管理局申请调整事件响应级别。

贵州省通信管理局根据涉事数据处理者的申请情况或

者事态发展情况等，适时调整事件响应级别，涉及一、二级响应级别调整的应当报部数据安全机制同意。

4.5 舆情监测

贵州省通信管理局组织监测公开信息发布渠道，密切关注数据安全事件舆情信息，跟踪掌握事件影响程度和范围。

4.6 结束响应

事件的影响和危害得到控制或消除后，一级响应应当根据国家数据安全工作协调机制有关决定或经部网信领导小组批准后结束；二级响应由部数据安全机制决定结束，并报部网信领导小组；三级响应由贵州省通信管理局决定结束，并报部数据安全机制；四级响应由相关涉事数据处理者决定结束。

5. 事后总结

5.1 事件总结上报

重大及以上数据安全事件应急工作结束后，涉事数据处理者应当及时调查事件的起因、经过、责任，评估事件造成的影响和损失，总结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，在应急工作结束后5个工作日内形成总结报告（模板见附件3），报送贵州省通

信管理局。贵州省通信管理局汇总审核后，在应急工作结束后10个工作日内形成报告报送部数据安全机制。

5.2 事件警示

贵州省通信管理局在本地区内发布与公众有关的警示信息，引导做好数据安全风险防范。

6. 预防措施

6.1 预防保护

数据处理者应当根据有关法律法规和标准的规定，建立健全数据安全管理制度，建设数据安全应急技术手段。重要数据和核心数据处理者应当每年至少开展一次数据安全风险评估和自查自纠，及时消除风险隐患。

贵州省通信管理局依法开展数据安全监督检查，指导督促相关单位消除风险隐患。

6.2 应急演练

贵州省通信管理局应当定期组织开展数据安全事件应急演练，提高数据安全事件应对能力。

数据处理者要积极参与贵州省通信管理局组织的应急演练，开展本单位数据安全事件应急演练，提高数据安全事件应对能力。重要数据和核心数据处理者应当加强应急演练。

6.3 宣传培训

贵州省通信管理局应当组织开展数据安全事件应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关单位和社会公众的数据安全意识和防护、应急能力。

数据处理者应当面向本单位员工加强数据安全应急宣传教育和培训，鼓励开展各种形式的数据安全应急相关竞赛。

6.4 手段建设

贵州省通信管理局建立贵州省电信领域数据安全监测预警与应急处置能力，组织相关企业开展数据安全风险和事件监测预警工作，及时开展风险和事件应急处置。

数据处理者应当开展数据安全风险和事件监测，积极配合贵州省通信管理局开展数据安全风险监测和技术能力联动等工作，及时排查安全隐患，采取必要的措施防范、处置数据安全风险和事件。

6.5 重大活动期间的预防措施

在国家重大活动期间，贵州省通信管理局组织指导数据处理者、应急支撑机构等加强数据安全风险监测、威胁研判和事件处置，强化风险防范与应对措施。相关重点单位、重点岗位加强值班值守。

7. 保障措施

7.1 落实责任

贵州省通信管理局、电信领域数据处理者、应急支撑机构应当把数据安全应急工作责任落实到单位负责人、具体部门、具体岗位和个人。

7.2 奖惩问责

贵州省通信管理局对数据安全应急事件应对工作中作出突出贡献的先进集体和个人给予表扬。

对未按照相关法律法规、政策制度和本预案的要求开展数据安全事件应急处置工作的，贵州省通信管理局依法依规对数据处理者进行约谈或给予行政处罚。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。

7.3 经费保障

贵州省通信管理局、应急支撑机构等为数据安全应急事件处置工作提供必要的经费保障。

数据处理者应当安排必要的专项资金，支持本单位数据安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

7.4 工作协同

贵州省通信管理局与其他相关部门加强沟通协调，支

持相关企业、科研院所、高等学校开展应急技术攻关、产品服务和能力供给，培养数据安全应急技术人才，形成应急响应工作合力。

7.5 物资保障

贵州省通信管理局和应急支撑机构应当加强对数据安全应急装备、工具的储备，及时调整、升级、优化软件硬件工具，不断增强应急技术支撑能力。

7.6 保密管理

贵州省通信管理局和应急支撑机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

8. 附则

8.1 预案修订

本预案原则上每年评估一次，根据实际情况由贵州省通信管理局适时进行修订。

8.2 排除条款

涉及军事、国家秘密信息、电信领域政务数据等数据安全事件应急响应的，按照国家有关规定执行。

8.3 预案解释

本预案由贵州省通信管理局负责解释。

8.4 实施日期

本预案自印发之日起实施。

附件：1.贵州省电信领域数据安全事件分级

2.数据安全事件上报（模板）

3.数据安全事件应急处置工作总结报告（模板）

4.数据安全事件应急处置流程图

附件 1

贵州省电信领域数据安全事件分级

一、符合下列情形之一的，为特别重大数据安全事件

（一）重要数据、核心数据遭到篡改、破坏、泄露或者非法获取、非法利用，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的；

（二）数据遭到篡改、破坏、泄露或者非法获取、非法利用，导致重要网络设施和信息系统、核心网络设施和信息系统运行中断或严重异常，持续时间 24 小时以上的；

（三）数据遭到篡改、破坏、泄露或者非法获取、非法利用，造成特别重大直接经济损失，损失 10 亿元（含）以上的；

（四）发生特别严重个人信息安全事件，涉及 1 亿人（含）以上个人信息或者 1000 万人（含）以上敏感个人信息的；

（五）其他造成或可能造成特别重大危害或影响的。

二、符合下列情形之一的，为重大数据安全事件

（一）重要数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会秩序、经济建设和公众利益构成严重威胁的；

（二）数据遭到篡改、破坏、泄露或者非法获取、非

法利用，导致重要网络设施和信息系统运行中断或严重异常，持续时间 12 小时以上的；

（三）数据遭到篡改、破坏、泄露或者非法获取、非法利用，造成重大直接经济损失，损失 1 亿元（含）以上 10 亿元以下的；

（四）发生严重个人信息安全事件，涉及 1000 万人（含）以上 1 亿人以下个人信息或者 100 万人（含）以上 1000 万人以 下敏感个人信息的；

（五）其他造成或可能造成重大危害或影响的。

三、符合下列情形之一的，为较大数据安全事件

（一）重要数据或一般数据遭到篡改、破坏、泄露或者非法获取、非法利用，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的；

（二）数据遭到篡改、破坏、泄露或者非法获取、非法利用，导致相关网络设施和信息系统运行中断或严重异常，持续时间 8 小时以上的；

（三）数据遭到篡改、破坏、泄露或者非法获取、非法利用，造成较大直接经济损失，损失 5000 万元（含）以上 1 亿元以下的；

（四）发生较严重个人信息安全事件，涉及 100 万人（含）以上 1000 万人以下个人信息或者 10 万人（含）以上 100 万人以下敏感个人信息的；

（五）其他造成或可能造成较大危害或影响的。

四、符合下列情形之一的，为一般数据安全事件

（一）数据遭到篡改、破坏、泄露或者非法获取、非法利用，对社会秩序、经济建设和公众利益构成较轻威胁的；

（二）数据遭到篡改、破坏、泄露或者非法获取、非法利用，导致相关网络设施、信息系统运行中断或严重异常，持续时间 8 小时以下的；

（三）数据遭到篡改、破坏、泄露或者非法获取、非法利用，造成直接经济损失 5000 万元以下的；

（四）发生个人信息安全事件，涉及 100 万人以下个人信息或者 10 万人以下敏感个人信息的；

（五）其他造成或可能造成一般危害或影响的。

附件 2

数据安全事件上报（模板）

上报单位情况	单位全称	XX
	联系人	XX
	联系方式	XX（手机号）
事件基本情况	发生时间	XX 年 XX 月 XX 日 XX 时 XX 分
	获悉渠道	□自主监测发现 □网上公开发布（URL） □第三方报送（报送单位） □其他 XX
	涉事单位	XX（单位全称）
	事件级别	□一般 □较大 □重大 □特别重大
	涉及系统	XX（系统/平台全称）
		IP/域名/URL：XX
	事件原因	（简要描述事件发生原因）
事件涉及数据情况	类型	□研发 □生产 □管理 □运维 □服务
	级别	□一般 □重要 □核心
	规模	XXGB/XX 条
	个人信息情况	□个人信息 XXGB/XX 条 □敏感个人信息 XXGB/XX 条 □无
事件影响情况	影响主体	XX（单位全称）
	影响范围	XX 地区/行业
事件处置建议	1.XX 2.XX （简要描述事件已采取的措施、拟进一步采取的措施及请求支援事项等。）	

签字（或盖章）：

注：1．涉及系统、影响主体和范围等信息不明确的，可填“尚不明确”。

2．重大及以上数据安全事件需上报人签字或上报单位盖章。

附件 3

数据安全事件应急处置工作总结报告（模板）

填 报 单 位：_____（加盖公章）

填 报 日 期：_____年_____月_____日

填 写 说 明

1.报告材料应客观、真实，不得弄虚作假，不涉及国家秘

密，填报单位对所提交材料的真实性负责。

2.本报告除表格外,其他各项填报要求:A4 幅面编辑，正文应采用仿宋_GB2312 三号字，单倍行间距，两端对齐，一级标题三号黑体，二级标题为三号楷体_GB2312 加粗。

3.需在报告首页加盖公章。

4.本报告未经允许不得公开。

一、事件基本情况

（包括数据安全事件的起因、经过、真实性、责任落实等
情况，评估事件造成的影响和损失等）

二、已采取的处置措施

（包括数据处理者在管理制度、技术保护、人员管理等方
面采取的处置措施，以及针对本次数据安全事件可能造成的危害已采取的应急手段、用户合法权益保护告知情况等）

三、后续提升改进计划

（包括针对相关数据安全事件情况，进一步提升数据安全
保护能力的相关措施）

四、工作经验总结

（针对此类数据安全事件，总结分析事件防范和应急处置
工作的经验教训等）

五、其他事项

（其他需补充说明的事项）

注：请随附数据安全事件应急处置相关证明材料

附件 4

数据安全事件应急处置流程图