广 西 壮 族 自 治 区

通信管理局文件

桂通管网〔2025〕6号

广西通信管理局关于印发《广西电信领域数据安全事件应急预案（试行）》的通知

各基础电信运营企业、各车联网平台企业、各增值电信企业：

为进一步健全我区公共互联网数据安全突发事件应急机制，提升应对能力，根据《工业和信息化领域数据安全时间应急预案（试行）》，结合我区实际，制定《广西电信领域数据安全事件应急预案（试行）》。现印发你们，请遵照执行。

附件：1.广西电信领域数据安全事件应急预案（试行）

1.1 广西电信领域数据安全事件分级

1.2 数据安全事件上报（模版）

1.3 数据安全事件应急处置工作总结报告（模版）

1.4 广西电信领域数据安全事件应急处置流程图

2.电信企业和车联网平台企业清单

广西壮族自治区通信管理局

2025 年 3 月 28 日

（联系电话：0771-2618632）

（此件主动公开）

附件 1

广西电信领域数据安全事件应急预案
（试行）

广西通信管理局

2025 年 3 月

目录

1. 总则

1.1. 编制目的

建立健全广西电信领域数据安全事件应急组织体系和工作机制，提高本区电信领域数据安全事件应对能力，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，保障广西经济稳定运行和社会稳定，维护国家安全和公共利益。

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》《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》《工业和信息化领域数据安全事件应急预案（试行）》《公共互联网网络安全突发事件应急预案》等相关规定。

1.3. 适用范围

在广西区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、行政法规和预案的要求。

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，将数据安全分为特别重大、重大、较大和一般四个级别（见附件1.1）。

1.6. 工作原则

数据安全事件应急工作应当坚持统一领导，分级负责。坚持统一指挥、密切协同、快速反应、科学处置。坚持“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. 领导机构和职责

在工业和信息化部的统一领导和在自治区数据安全工作协调机制办公室协调下，广西通信管理局组织成立以局党组书记、局长担任组长，分管副局长担任副组长，网络安全管理处负责人为成员的网络与信息安全工作领导小组（以下简称局网信领导小组），统一负责广西电信领域数据安全事件应急管理工作，负责数据安全事件的统一指挥和协调。

2.2. 办事机构与职责

在局网信领导小组领导下，组织成立广西数据安全应急办

公室，负责贯彻执行局网信领导小组相关指示和部署，负责广西电信领域数据安全应急管理事务性工作，负责广西电信领域数据安全数据安全事件预防、监测、应急处置、报告等工作；负责及时向工业和信息化部及局网信领导小组报告数据安全事件情况，并按工业和信息化部及局网信领导小组的指导，对特别重大、重大数据安全事件处置进行指挥和协调；负责较大数据安全突发事件的统一指挥和协调；根据需要协调一般数据安全突发事件应急处置工作。

广西数据安全应急办公室主任由广西通信管理局网络安全管理处负责人担任，成员由广西通信管理局网络安全管理处工作人员组成。日常工作由广西通信管理局网络安全管理处承担。

2.3. 应急支撑机构与职责

广西数据安全应急办公室根据需要遴选属地专业数据安全应急支撑机构，负责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，为应急工作提供决策支持和技术支撑。

3. 监测与预警

3.1. 预警监测和报告

数据处理者、数据安全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。

数据处理者、数据安全应急支撑机构认为可能发生较大及以上数据安全事件的，应当立即向广西数据安全应急办公室报告（模版见附件 1.2）。

广西数据安全应急办公室认为可能发生重大及以上数据安全事件的，应当立即上报工业和信息化部。

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，将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。

广西数据安全应急办公室及时汇总分析数据安全风险和预警信息，必要时组织数据安全应急支撑机构、专家、相关企业进行会商谈判，明确预警等级。

3.3. 预警发布

认为需要发布红色、橙色预警的，由广西数据安全应急办公室报工业和信息化部统一发布，并同步向自治区数据安全工作协调机制办公室报送相关信息；认为需要发布黄色和蓝色预警的，由广西数据安全应急办公室在本区域发布。

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，相关单位应当针对即将发生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、报告相关信息，加强数据安全风险监测;

（2）组织数据安全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。

工业和信息化部发布红色和橙色预警后，相关单位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）涉及预警信息的数据处理者等相关单位部门加强值班值守，相关人员保持通信联络畅通;

（2）数据安全应急支撑机构进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等使用情况，确保处于良好状态。

3.5. 预警调整和解除

红色和橙色预警由工业和信息化部统一负责调整和解除，相关信息由广西数据安全应急办公室同步报局网信领导小组和自治区数据安全工作协调机制办公室。

黄色和蓝色预警由广西数据安全应急办公室发布预警后，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：Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ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，对自判断为较大事件的，应当立即按照“电话 20 分钟、书面 40 分钟”的要求向广西数据安全应急办公室报告，对自判断为特别重大、重大事件的，应当立即按照“电话 10 分钟、书面 30 分钟”的要求向广西数据安全应急办公室报告，不得迟报、谎报、瞒报、漏报。

数据安全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，及时向广西数据安全应急办公室报告。

报告事件研判信息时，应当说明事件发生事件、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

广西数据安全应急办公室视情况组织数据安全应急支撑机构、专家等进行研判，判定事件级别和响应等级，启动应急响应。

4.4.1. Ⅰ级响应

由工业和信息化部启动，并统一指挥和协调。

广西数据安全应急办公室在发现事件后按照“电话 10 分钟、书面 30 分钟”的要求将事件情况报工业和信息化部、自治区数据安全工作协调机制办公室和局网信安领导小组；进入应急状态，加强值班值守，全面了解数据处理者受事件影响情况，组织涉事数据处理者、数据安全应急支撑机构等加强事态跟踪研判、开展事件处置，加强事件跟踪监测配合做好应急响应工作，通知可能受影响的其他区域做好数据安全应急处置工作。

涉事数据处理者立即启动本单位数据安全事件应急预案，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。数据安全直接负责人（本单位数据安全工作分管领导）对应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。

数据安全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。

组织专家加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议。

4.4.2. Ⅱ级响应

由工业和信息化部启动，并统一指挥和协调。

广西数据安全应急办公室在发现事件后按照“电话 10 分钟、书面 30 分钟”的要求将事件情况报工业和信息化部、自治区数据安全工作协调机制办公室和局网信安领导小组；进入应急状态，全面了解数据处理者受事件影响情况，组织涉事数据处理者、数据安全应急支撑机构等加强事态跟踪研判、开展事件处置，加强事件跟踪监测配合做好应急响应工作，通知可能受影响的其他区域做好数据安全应急处置工作。

涉事数据处理者立即启动本单位数据安全事件预案，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，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。

数据安全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。

组织专家加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议。

4.4.3. Ⅲ级响应

根据自治区数据安全工作协调机制办公室决定或经由局网信领导小组批准启动。

广西数据安全应急办公室在发现事件后按照“电话 20 分钟、书面 40 分钟”的要求将事件情况报工业和信息化部、自治区数据安全工作协调机制办公室和局网信安领导小组；进入应急状态，负责统一指挥协调，全面了解相关企业受事件影响情况，组织涉事数据处理者、数据安全应急支撑机构等加强事态跟踪研判、开展事件处置，通知可能受影响的其他区域做好数据安全应急处置工作。

涉事数据处理者立即启动本单位数据安全事件应急预案，进入应急状态，保持联络畅通；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。

相关数据安全应急支撑机构加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

4.4.4. Ⅳ级响应

涉事数据处理者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，向广西数据安全应急办公室申请调整事件响应级别。

广西数据安全应急办公室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Ⅰ、Ⅱ级响应级别调整的应当报工业和信息化部同意。

4.5. 舆情监测

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，Ⅰ级、Ⅱ级响应由工业和信息化部决定结束；Ⅲ级响应由广西数据安全应急办公室报局网信领导小组批准同意结束，并报工业和信息化部和自治区数据安全工作协调机制办公室；Ⅳ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（模版详见附件1.3），报广西数据安全应急办公室。广西数据安全应急办公室汇总审核后，在应急工作结束后10个工作日内形成报告报送工业和信息化部。

5.2. 事件警示

广西数据安全应急办公室在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。

广西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

数据处理者应当积极参与广西通信管理局组织开展数据安全事件应急演练，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

数据处理者应当面向本单位员工围绕数据安全事件应急相关法律法规、应急预案和基本知识开展宣传教育和培训，提高数据安全意识和防护、应急能力，鼓励开展和参加各种形式的数据安全应急相关竞赛。

6.4. 手段建设

数据处理者和相关单位应当开展数据安全风险和事件监测，积极配合广西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，广西通信管理局组织指导数据处理者、数据安全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

数据处理者、数据安全应急支撑机构应当建立健全数据安全应急工作机制，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

广西通信管理局对数据安全事件应急处置工作中作出突

出贡献的集体和个人给予表扬。

对未按照本预案开展数据安全事件应急处置工作的，广西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。

7.3. 经费保障

数据安全应急支撑机构为数据安全事件应急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

广西通信管理局支持区内企业、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

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

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，根据实际情况广西通信管理

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

本预案由广西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 2

电信企业和车联网平台企业清单

电信企业：中国电信广西公司、中国移动广西公司、中国联通广西分公司、广西广电网络公司、中国铁塔广西分公司。

车联网平台企业：上汽通用五菱汽车股份有限公司、东风柳州汽车有限公司、广西汽车集团有限公司、柳州市东科智慧城市投资开发有限公司。

抄送：工业和信息化部网络安全管理局，自治区数据安全工作协调机制办公室。

广西壮族自治区通信管理局办公室　　2025 年 3 月 28 日印发