广西壮族自治区

数据安全事件报告和调查处理办法

#  总 则

第一条 为建立健全广西壮族自治区数据安全事件管理工作机制，提高应对数据安全事件的能力，预防和减少数据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，根据《广西壮族自治区大数据发展条例》《广西壮族自治区数据安全管理办法》等相关文件要求，结合我区实际，制定本办法。

第二条 本办法适用于广西区域范围内的数据安全事件的报告、处理、调查等相关管理工作。数据安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等主观和客观因素，对网络和信息系统中的数据造成泄露、篡改、毁损、丢失、非法使用等，对社会造成负面影响的事件。

第三条 数据安全事件处理工作坚持统一领导、快速反应、科学处置、预防为主的原则，建立健全的数据安全风险防范体系，强化党委、政府部门的主导作用，落实数据处理者的主体责任，降低发生数据安全事件的可能性，有效减少数据安全事件对国家安全、社会稳定的损害。

第四条 本办法中的数据处理者，是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。

#  事件分类分级

第五条 按照事件发生原因、对数据的影响类型，将数据安全事件划分为以下类型：

（一）数据泄露：由于缺乏有效的安全措施、人员操作失误或有意窃取等，导致发生数据泄露、恶意窃取、未授权访问等影响数据保密性的事件。

（二）数据篡改：由于缺乏有效的安全措施、人员有意或无意操作等，导致发生数据被未授权更改等影响数据完整性的事件。

（三）数据毁损：由于缺乏有效的安全措施、人员有意或无意操作等，导致发生数据被破坏、毁损、数据质量下降等影响数据可用性的事件。

（四）数据丢失：由于缺乏有效的安全措施、人员有意或无意操作等，导致发生数据丢失、难以恢复的事件。

（五）数据非法使用：由于缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致数据被未授权或超出授权范围使用、加工的事件。

第七条 根据国家网络安全事件应急相关要求和数据安全事件对公众利益和单位合法权益、社会秩序、经济建设、国家安全和社会稳定的影响程度，并按照事件的影响范围及持续时间等因素，将事件等级从高到低划分为三级：特别重大数据安全事件、重大数据安全事件和一般数据安全事件。当事件同时满足多个级别的定级条件时，按最高级别确定事件等级；特殊时期（如重大活动、重大节点等）发生的安全事件级别应在原有级别上提升一级，特别重大数据安全事件不再向上提升。

第八条 特别重大数据安全事件是指其发生能够导致特别严重的影响或破坏的重大数据安全事件。符合下列情形之一的，为特别重大数据安全事件：

（一）发生核心数据被泄露、篡改、毁损、丢失、非法使用等安全事件；

（二）发生数据泄露、篡改、毁损、丢失、非法使用等事件，对国家安全和社会稳定构成特别严重威胁的情况；

（三）其他对国家安全、社会秩序、经济建设等构成特别严重威胁、造成特别严重影响的事件。

第九条 重大数据安全事件是指其发生能够导致严重影响或破坏的数据安全事件。符合下列情形之一且未达到特别重大数据安全事件的，为重大数据安全事件：

（一）发生重要数据泄露、篡改、毁损、丢失、非法使用等安全事件；

（二）发生数据泄露、篡改、毁损、丢失、非法使用等事件，对国家安全和社会稳定构成严重威胁；

（三）其他对国家安全、社会秩序、经济建设等构成严重威胁、造成严重影响的事件。

第十条 一般数据安全事件是指其发生能够导致较大影响或破坏的数据安全事件。符合下列情形之一且未达到重大数据安全事件的，为一般数据安全事件：

（一）发生一般数据被泄露、篡改、毁损、丢失、非法使用等安全事件；

（二）发生数据泄露、篡改、毁损、丢失、非法使用等事件，对国家安全和社会稳定构成一定威胁的情况；

（三）其他对国家安全、社会秩序、经济建设等构成一定威胁、造成一定影响的事件。

#  事件报告

第十一条 发生特别重大、重大数据安全事件时，数据处理者应当在事件发生后1小时内上报至所在地承担数据安全工作协调机制办公室职能的部门和行业主管部门，上报内容包括但不限于事件等级、事件内容、事件大致原因、影响范围及已采取的处置措施，并不定时上报事态发展。

第十二条 对于一般数据安全事件，数据处理者应当在事件发生后2小时内上报至行业主管部门，上报内容包括但不限于事件等级、事件内容、事件大致原因、影响范围及已采取的处置措施，并不定时上报事态发展。

第十三条 事件所在地承担数据安全工作协调机制办公室职能的部门、行业主管部门接到数据安全事件报告后，应依照下列规定上报事件情况：

（一）特别重大、重大数据安全事件逐级上报至自治区数据安全工作协调机制办公室、行业主管部门；

（二）一般数据安全事件逐级上报至设区的市级承担数据安全协调机制办公室职能的部门、行业主管部门。

第十四条 数据处理者应明确数据安全事件处置的一般和紧急联系人，一般联系人用于日常的信息沟通，紧急联系人用于发生特别重大、重大数据安全事件情况下的直接沟通，联系人须24小时保持通讯通畅，联系人及联系方式发生变化需提前3个工作日进行上报。

#  事件处理

第十五条 发生数据安全事件时，数据处理者应组织相关人员进行事件研判，进行先期处理。根据事件等级，启动处置预案；做好现场划定，实行有效的现场管控措施，快速组织各方面力量，开展应急救援，快速恢复，防止事态扩大等先期处理工作。

第十六条 响应级别依据突发事件等级分为：一级响应、二级响应、三级响应，从高到低依次对应发生特别重大、重大、一般数据安全事件。

（一）一级响应：

1.一级响应启动后，按照一级响应流程进行处理；

2.立即根据事件性质上报至所在地承担数据安全工作协调机制办公室职能的部门、行业主管部门，并组织召开应急指挥紧急会议，通报事件初始信息，商议处理事件的初步措施；

3.启动应急预案，部署应急处理相关工作，组织恢复工作的实施，收集事件响应信息，对事态发展和影响及时进行分析和评估，按需组织召开处理工作部署等，直至响应结束；

4.履行应急值守、信息汇总和协调职能，实行24小时值班制度，密切关注事件发展情况。

（二）二级响应：

1.二级响应启动后，按照二级响应流程进行处理；

2. 立即根据事件性质上报至所在地承担数据安全工作协调机制办公室职能的部门、行业主管部门，并组织召开应急指挥紧急会议，通报事件初始信息，商议处理事件的初步措施；

3.启动应急预案，组织恢复工作的实施，收集事件响应信息，对事态发展和影响及时进行分析和评估，按需组织召开处理工作部署等，直至响应结束；

4.履行应急值守、信息汇总和协调职能，实行8小时值班制度，密切关注事件发展情况。

（三）三级响应：

1.三级响应启动后，按照三级事件响应流程进行处理；

2.立即根据事件性质上报至所在地承担数据安全工作协调机制办公室职能的部门、行业主管部门，视实际情况组织召开会议通报事件详情和抢险恢复情况，直至响应结束；

3.安排人员24小时电话值班，密切关注事件发展情况。

第十七条 当发生数据安全事件时，按应急预案进行事件响应，对于超出数据处理者自身响应处理能力的安全事件，承担数据安全工作协调机制办公室职能的部门、行业主管部门应协调合规的第三方机构提供技术支持。

第十八条 进行事件响应后，当达到以下条件时，数据处理者可以提出响应结束建议。

（一）一、二级响应结束条件

数据安全隐患排除，数据恢复正常，受影响系统恢复至正常运行状态，安全威胁消除且短期内无新增重大安全风险，经自治区数据安全工作协调机制办公室批准后结束。

（二）三级响应结束条件

数据安全隐患排除，数据恢复正常，受影响系统恢复至正常运行状态，安全威胁消除，经所在地承担数据安全工作协调机制办公室职能的部门批准后结束。

#  事件调查

第十九条 数据安全事件发生后，数据处理者应在所在地承担数据安全工作协调机制办公室职能的部门和行业主管部门的监督下组织调查团队对事件发生原因、经过、影响范围、经济损失、事件责任认定等方面进行调查，并编写事件调查报告。

第二十条 数据处理者应在完成应急处置工作后10个工作日内完成事件调查，编写事件调查报告递交至所在地承担数据安全工作协调机制办公室职能的部门和行业主管部门。

第二十一条 事件所在地承担数据安全工作协调机制办公室职能的部门、行业主管部门接收到事件调查报告后，应依照下列规定递交事件调查报告：

（一）特别重大、重大数据安全事件的调查报告应逐级递交至自治区数据安全工作协调机制办公室、行业主管部门。

（二）一般数据安全事件的调查报告应递交至设区的市级承担数据安全工作协调机制办公室职能的部门、行业主管部门。

第二十二条 调查报告内容包括但不限于事件原因、性质、级别、影响范围、经济损失、处理情况、相关责任人、事件防范和整改措施等。

#  附则

第二十三条 行业主管部门针对数据安全事件管理另有规定的，从其规定。

第二十四条 本办法由广西壮族自治区大数据发展局负责解释。

第二十五条 本办法自印发之日起实施。