**中国移动通信集团吉林有限公司**

**数据安全事件应急响应预案**

中国移动通信集团吉林有限公司

2025年9月

一、总 则

## （一）目 的

为提高中国移动通信集团吉林有限公司数据安全突发事件的能力,形成科学、有效、反应迅速的应急工作机制，确保我公司重要信息系统的实体安全、运行安全和数据安全，最大限度地降低数据安全突发事件的危害，特制定本预案。

## （二）工作原则

数据安全突发事件应急处理工作坚持统一领导、分工负责、协作配合、及时预警、快速处理、确保恢复的原则。

## （三）编制依据

《中华人民共和国网络安全法》；

《中华人民共和国数据安全法》；

《电信和互联网用户个人信息保护规定》；

《中国移动通信集团吉林有限公司客户信息安全保护管理规定》等。

## （四）适用范围

本预案适用于以下情况的应急准备、监测与预警、应急处置与支援、事后恢复与整改等数据安全突发事件应急工作。

1、中国移动吉林公司运营的重要信息系统突然遭受不可预知外力的破坏、毁损或故障；

2、中国移动吉林公司保存的重要数据信息主动或被动产生泄露、损坏和丢失，有可能造成危害的紧急网络数据安全事件。

## （五）分级响应原则

按照危害程度、影响范围等因素，中国移动吉林公司将数据安全突发事件分为特别重大、重大、较大和一般四级。事件发生后应当采取相应级别的应急处置措施。

中国移动吉林公司运营的业务系统发生数据安全事件分级标准由中国移动吉林公司在本预案中制定。法律、行政法规或上级部门另有规定的，从其规定。

# 二、组织体系和职责

中国移动吉林公司已成立网络安全领导小组和信息安全管理部，负责领导、组织、协调本省网络与信息安全各方面工作。

## （一）中国移动吉林公司网络安全领导小组的组成和安全应急职责

中国移动吉林公司网络安全领导小组在数据安全突发事件应急处理方面职责如下：

1、贯彻国家有关方针政策，审定数据安全突发事件应急响应相关政策及规定；

2、启动/终止预案，并负责数据安全突发事件应急工作的总体指挥和协调；

3、根据上级部门指示，决策重大数据安全突发事件的应急处理实施方案，并向上级部门汇报实施和进展情况；

## （二）省公司信息安全管理部的组成和安全应急职责

省公司信息安全管理部在数据安全突发事件应急处理方面职责如下：

1、负责与国家相关部门的沟通协调，并向省公司网络安全领导小组提出相关工作建议；

2、组织起草、修改中国移动吉林公司数据安全突发事件应急处理预案及相关规定；

3、按照中国移动吉林公司网络安全领导小组下达的命令和指示，具体协调处理数据安全突发事件应急工作；

4、在应急响应期间，负责中国移动吉林公司各相关部门和各地市公司之间的现场指挥协调，组织中国移动吉林公司各相关部门和各地市公司落实数据安全突发事件应急处理技术措施；

5、在应急响应期间，及时收集汇总中国移动吉林公司各相关部门和各地市公司上报/反馈的事件进展情况，向中国移动吉林公司网络安全领导小组报告并提出建议，向省通信管理局上报相关安全事件处理信息；

## （三）中国移动吉林公司数据安全突发事件应急组织体系

中国移动吉林公司网络安全领导小组负责组织、协调中国移动吉林公司各相关部门、各地市公司进行数据安全突发事件应急工作。

中国移动吉林公司各相关部门和各地市公司负责监测和分析所管网络数据安全的运行状况，配合采集日常运行数据；及时上报发现的网络数据异常情况和安全事件；在中国移动吉林公司网络安全领导小组的统一指挥下，采取有效措施，处理所管网络的数据安全事件；通知负责部门及时进行系统安全扫描、漏洞封堵、病毒杀查等措施，消除安全隐患；配合其他部门处理与所管数据安全有关的安全事件。

负责为数据安全突发事件应急处理工作提供技术支撑；协调和配合各部门、各地市公司的应急技术处理及演练；利用技术手段，对数据安全突发事件进行监测，及时收集、核实、汇总、分析、上报有关数据安全信息；保持与省通信管理局的安全事件应急处理合作。设在省公司信息安全管理部，小组的成员也包括省公司其他部门的网络信息安全应急处理联系人。

# 三、应急准备

## （一）制定应急预案

各地市公司应结合本公司的实际情况，制定本公司数据安全安全应急预案。

各地市公司应根据实际需要和形势变化，适时修订本公司应急预案。

## （二）成立应急队伍

指定专业部门负责组织、协调、指挥本公司数据安全突发事件应急工作。

重视数据安全突发事件应急人才队伍建设，选拔熟悉数据安全突发事件和网络安全的专业人员从事网络安全应急工作。

## （三）组织应急培训

应急保障队伍的人员要不定期进行应急处理的相关培训，确保熟悉工作原则、工作流程，并具备必要的技能，确保应急预案的正常实施。

## （四）建立联络机制

指定本单位数据安全突发事件应急工作联系人和联系方式，联系方式应包括手机、电子邮件等信息。各单位联系人和联系方式发送至省公司信息安全管理部报备，发生变更后应在五个工作日内重新报备。

## （五）部署安全监测手段

建设或完善数据安全突发事件监测手段，包括围绕核心生产和支撑系统的入侵行为检测系统、异常流量或攻击行为监测系统等，以准确掌握本公司网络数据安全状况。在网络或业务系统改扩建时，应同步考虑网络数据安全应急配套设施。

## （六）开展应急演练

定期开展本单位数据安全应急演练。需要各地市公司配合的，共同组织联合演练。

## （七）保障应急经费

应根据需要安排必要的专项应急经费，用于数据安全突发事件应急处理。

省公司各相关部门、各省直属中心和各地市公司根据突发事件的应急需要，提出项目支出预算申请，报有关部门批准后执行。项目资金的使用范围应包括应急系统建设及运行、应急设备、培训及演习、应急业务系统保障支援等费用。

# 四、监测和预警

## （一）数据安全事件的分级

数据安全事件根据危害和紧急程度分为 “特别重大”、“重大”、“较大”、“一般”四种，分别对应 “红”、“橙”、“黄”、“蓝”四种颜色标记。

各级数据安全事件的定义如下：

1、特别重大 (红色，RGB配色:255,0,0)

造成中国移动吉林公司数据信息系统发生大规模瘫痪，或重要数据发生大范围泄露、损坏、丢失（造成一亿以上数据信息泄露），事态的发展超出公司相关主管部门的控制能力，对国家安全、社会秩序、公共利益或者中国移动吉林公司形象造成特别严重损害的突发事件。

2、重大 (橙色，RGB配色:255,128,0)

造成中国移动吉林公司数据信息系统发生瘫痪，或重要数据发生较大面积泄露、损坏、丢失（造成一千万以上数据信息泄露），对国家安全、社会秩序、公共利益或中国移动吉林公司形象造成严重损害，需要上级部门协助处置的突发事件。

3、较大 (黄色，RGB配色:255,255,128)

造成中国移动吉林公司业务系统运转异常，或重要数据发生泄露、损坏、丢失（造成一百万以上数据信息泄露），对国家安全、社会秩序、公共利益或中国移动吉林公司形象造成一定损害，但只需在技术支撑单位协同处置的突发事件。

4、一般 (蓝色，RGB配色:0,0,255)

造成中国移动吉林公司信息系统受到破坏，或重要数据发生个别的泄露、损坏、丢失（小于一百万数据信息泄露），对本单位的权益有一定影响，但不危害国家安全、社会秩序和公共利益，可由业务系统维护部门自行处置的突发事件。

## （二）网络数据安全信息监测

应加强数据安全监测，采取多种技术或非技术途径发现、搜集系统日志信息和预警信息，加强与上机部门和其他相关单位的信息交流和情报合作。

省公司应积极开展数据安全事件的投诉、举报受理工作，向广大用户、重要信息系统单位和重要机构提供热线、电子邮件等便捷的网络安全事件投诉通道，加强与相关设备、系统供应商和网络安全服务企业的合作，不断拓宽获取数据安全事件信息和预警信息的渠道。

## （三）预警预防行动

1、预警信息报送

省公司发现或掌握以下潜在安全威胁或重大安全隐患信息（尚未造成实际危害和影响），应及时报送：

（1）给网络或系统带来较大风险的安全漏洞；

（2）出现危害性较强的恶意代码；

（3）黑客进行有组织攻击的计划。

（4）发现重要数据信息主动或被动产生泄露、损坏和丢失的迹象，有可能造成危害的紧急数据安全事件。

2、预警信息通报

接收到安全预警信息后，应立即进行调查分析，对可能引发本预案规定的“较大”以上级别数据安全突发事件的潜在威胁和隐患，应及时通过省公司向各相关部门、各地市公司发布紧急安全预警信息公告和防范建议。省公司接到紧急安全预警信息公告后，应立即组织业务系统维护和网络安全专业人员、相关设备、系统供应商和网络安全服务企业进行研究，参考防范建议采取适当的预防措施，防止数据安全事件的发生。

## （四）网络安全事件信息上报

省公司发生或发现数据安全事件后（已经造成实际危害和影响），应立即组织对事件的危害程度和影响范围进行初步评估认定。根据初步判定的事件紧急程度，按照以下要求进行信息上报。

1、紧急事件信息上报

对于初步认定符合数据安全突发事件的情况，立即向吉林省通信管理局上报情况说明。

2、一般事件信息报送

对于不符合数据安全突发情况的事件，省公司应对事件进行自行处置后，将事件发生情况、事件处置情况、相关建议信息等按月汇总后报送省通信管理局。

# 五、应急响应

## （一）先期处置

数据安全事件发生后，省公司各相关部门应针对事件的性质、特点和危害程度，及时组织全公司力量，依照有关法律、法规和规章的规定，采取先期应急响应措施。

省公司各相关部门在先期处置时，如果发现数据安全事件的处置需要其他相关单位提供支持配合，可通过向相关单位请求支援。为提高处置效率，可先通过电话等方式请求支援，后补正式公函。

应及时组织省公司各相关部门力量，依照有关法律、法规和规章的规定，配合集团，协助对方开展应急处置工作。

## （二）分级响应程序

根据本预案对数据安全突发事件的四级分类，“一般”级别的安全事件，这类事件作为日常监测、维护的内容，由省公司网络安全领导小组和通过预警信息沟通，自行处置。

在接到吉林省通信管理局指示或接到省公司、关于数据安全发生或可能发生“特别重大”、“重大”、“较大”级别的数据安全事件的紧急报告时，报请省公司网络安全领导小组批准，指示省公司各相关部门启动本预案进入相应的分级应急响应工作程序。

## （三）应急处理流程

**特别重大安全事件的应急响应：**

在特别重大安全事件发生或可能发生的情况下，按照以下流程进行处理：

1、省公司信息安全管理部立即向省公司网络安全领导小组报告事件发生和影响情况，根据初步判断提出对事件处理方案的建议，经省公司网络安全领导小组批准后实施。

2、省公司信息安全管理部向省公司各相关部门和通报安全事件情况，并指示立即启动各自相应的特别重大安全事件应急处理程序。

3、针对具体的安全事件类别采取以下的相应措施：

（1）紧急组织各技术支撑单位，在最短时间内研究事件的特点、机理、危害、解决方案及使用现有数据安全监测手段的监测方法，并在2小时内提出初步应对方案；

（2）立即使用现有安全监测手段对该事件进行监测。

4、省公司网络安全应急小组根据省公司信息安全管理部的指令，结合实际，针对具体的安全事件类别采取以下的相应措施：

（1）针对业务系统存储数据大规模损坏或丢失事件：

（a）立即组织力量全力抢修业务系统，每小时向省公司信息安全管理部汇报抢修工作进展；

（b）立即组织力量分析系统存储数据损坏或丢失的原因和有效遏制手段，每小时向省公司信息安全管理部汇报分析工作进展；

（c）根据省公司信息安全管理部的指示，配合立即对业务系统采取相应的技术措施；

（2）针对网络数据大范围泄露事件：

（a）紧急开展调查确定数据泄露原因，并在4小时内将原因上报省公司信息安全管理部；

（b）根据省公司信息安全管理部的指示，在12小时内完成工作落实；

省公司各相关部门应随时向省公司信息安全管理部报告所掌握的事件发展情况；省公司信息安全管理部应随时向集团公司上报事件的发展情况。

**重大安全事件的应急响应：**

在重大安全事件发生或可能发生的情况下，按照以下流程进行处理：

1、省公司信息安全管理部向省公司各相关部门、各地市公司和省通信管理局通报安全事件情况，并指示各地市公司立即启动各自相应的重大安全事件应急处理程序。

2、针对具体的安全事件类别采取以下的相应措施：

（1）立即组织研究该事件的特点、机理、危害，在4小时内提出初步应对方案；

（2）立即通过现有安全监测手段对安全事件进行监测，跟踪和收集相关信息。

3、各单位组根据省公司信息安全管理部的指示，结合本省实际，针对具体的安全事件类别采取以下的相应措施：

（1）针对业务系统存储数据一定规模损坏或丢失事件，应

（a）立即组织技术力量确保业务系统正常运行，确定数据损坏或丢失数量和影响程度，并在12小时内将事件分析报告上报省公司信息安全管理部；

（b）根据省公司信息安全管理部的指示，配合对事件原因进行深入调查；

（c）根据省公司信息安全管理部的指令在1小时内对相关业务系统采取相应的技术处理措施；

（2）针对网络数据一定范围泄露事件，应

（a）立即组织人员确保设备正常运行，并在6小时内将数据泄露事件原因和影响范围上报省公司信息安全管理部；

（b）根据省公司信息安全管理部的指示，在12小时内完成工作落实。

**较大安全事件的应急响应：**

在较大安全事件发生或可能发生的情况下，按照以下流程进行处理：

1、省公司信息安全管理部向省公司相关部门、各地市公司和省通信管理局通报安全事件情况，指示省公司各相关部门、各地市公司立即启动各自相应的较大安全事件应急处理程序。

2、根据指示，针对具体的安全事件类别采取如下的相应措施：

（1）立即对该事件的特点、机理、危害、解决方案进行研究，在8小时内提出初步应对方案，并上报省公司信息安全管理部；

（2）持续跟踪和收集相关信息，每24小时向省公司信息安全管理部上报事件动态；

3、根据省公司信息安全管理部的指令，结合省网实际，针对具体的安全事件类别采取以下的相应措施：

（1）针对业务系统存储数据小规模损坏或丢失事件，应

（a）立即组织技术力量确保业务系统正常运行，确定数据损坏或丢失数量和影响程度，并在12小时内将事件分析报告上报省公司信息安全管理部；

（b）根据省公司信息安全管理部的指示，配合对事件原因进行深入调查；

（2）针对网络数据一定范围泄露事件，应

（a）立即组织人员确保设备正常运行，并在6小时内将数据泄露事件原因和影响范围上报省公司信息安全管理部；

（b）根据省公司信息安全管理部的指示，在12小时内完成工作落实。

# 六、信息通报/上报

## （一）信息通报/上报时间要求

在发生或可能发生特别重大安全事件的情况下，省公司各相关部门、各地市公司应在1小时内向省公司信息安全管理部上报相关信息；在发生或可能发生重大安全事件的情况下，省公司各相关部门、各地市公司应在2小时内上报。收到上述信息后，省公司信息安全管理部应立即向省公司网络安全领导小组报告。经领导小组确认后，由省公司信息安全管理部负责立即向上级部门上报。

在发生或可能发生较大安全事件的情况下，省公司各相关部门和各地市公司应在4小时内向省公司信息安全管理部上报相关信息；省公司信息安全管理部应立即向省公司网络安全领导小组报告。经领导小组确认后，由省公司信息安全管理部负责立即向上级部门上报。

## （二）信息通报/上报的方式

事件信息的通报/上报可以通过办公系统（简称OA）、电子邮件等方式，根据事件的不同级别有以下不同的要求：

1、“特别重大”、“重大”级别的安全事件必须先通过电话通报/上报，同时通过电子邮件通报/上报，并使用电话确认对方收到；

2、“较大”级别的安全事件使用电子邮件通报/上报，并使用电话确认对方收到；

3、根据情况及时整理补充正式的OA文件通报/上报。

## （三）信息通报/上报的保障制度

1、值班制度：“较大”及以上级别的安全事件应急处理流程启动后，省公司各相关部门、各地市公司应当安排24小时安全值班。未安排值班的相关人员应在接到通知后1小时之内赶赴办公室或指定地点。

2、信息的归档整理制度：事件启动后，省公司各相关部门和各地市公司的信息部门应对通报、上报的信息以及有关部门和领导的反馈、对事件后续进展的跟踪情况进行统一编号或代号处理；任务结束后对相关信息及时归档。

# 七、应急处理流程的终止

根据省公司各相关部门、各直属中心、各地市公司和报告的数据安全事件发展和应急处理效果等情况，省公司信息安全管理部对网络数据安全状况进行分析，判断事件影响已降低到最低级别安全事件影响水平之下时，报经省公司网络安全领导小组批准后，指示省公司各相关部门、各地市公司和终止应急处理工作。

对外协调机制：

应急处理工作如涉及政府部门、重要信息系统主管部门或其他单位，由省公司信息安全管理部负责相关协调工作。

# 八、后期处置

## （一）受损系统的恢复

应急处置结束后，省公司各相关部门、各地市公司应投入必要的人力和物力，尽快将受损业务系统完全恢复至事发前水平，避免由于事件带来的连带损失扩大化。

## （二）业务安全加固和整改

省公司各相关部门、直属中心和地市公司应就数据安全事件中暴露出的业务系统弱点和缺陷尽快制定整改措施，对系统进行安全加固，消除安全隐患，并根据该次应急工作的经验和教训进一步完善修订各自的数据安全应急预案，改进应急工作部署，使其在今后更加有效地发挥作用。

## （三）情况汇报及总结

安全事件应急处理结束后，省公司各相关部门、直属中心和地市公司及时对本次安全事件发生的原因、事件规模进行调查，估算事件损失后果，对应急处理手段效果和后续风险进行评估，总结应急处理的经验教训并提出改进建议，于应急处置结束后一个月内向省公司信息安全管理部上报相关的总结评估报告。

省公司信息安全管理部在汇总分析省公司各相关部门、直属中心和地市公司上报的总结评估报告的基础上，向省公司网络安全领导小组及时上报本次事件的处理报告，包括事件规模、损失估算、应急处理手段效果评估、经验教训及下一步改进建议等。

## （四）奖惩评定及表彰

为提高数据安全应急工作的效率和积极性，按照有关规定，对在数据安全应急处理过程中表现突出的省公司部门、各直属中心、地市公司和个人给与表彰；对于处理不力，给中国移动吉林公司造成损失的省公司部门、地市公司和个人进行惩处。

# 九、附　则

## （一）预案管理与更新

本预案由省公司信息安全管理部负责管理和保存，并根据数据安全发展的实际情况及时进行修改更新。修改的预案经网络安全领导小组批准后发布实施。

## （二）制定与解释部门

本预案由省公司信息安全管理部制定并负责解释。

## （三）预案生效

本预案自印发之日起生效。