ICS 35.020
CCS L 80

DB23

黑 龙 江 省 地 方 标 准

DB 23/T 3505—2023

网络安全事件应急处置规范

2023-07-05 发布　　2023-08-04 实施

黑龙江省市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由黑龙江省互联网信息办公室提出并归口。

本文件起草单位：黑龙江大学、国家计算机网络应急技术处理协调中心黑龙江分中心、安天科技集团股份有限公司、绿盟科技集团股份有限公司。

本文件主要起草人：伍一、于佳华、李晗、尹尚书、彭加亮、于洪君、林峰、孙树鹏、尤秀、孙洪磊。

网络安全事件应急处置规范

1 范围

本文件规定了网络安全事件应急处置的术语和定义、工作原则、事件分类与分级、机构和职责、应急处置流程及措施、日常防范和应急准备等。

本文件适用于与黑龙江省网络安全事件相关的各级网络安全应急办公室、网络运营者、网络产品和服务提供者、网络安全应急技术支撑队伍应急处置、日常防范和应急准备等工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18030 信息技术 中文编码字符集

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 20985 信息技术 安全技术 信息安全事件管理指南

GB/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

网络数据

任何以电子方式对信息的记录（以下简称数据）。

3.2

信息系统

应用、服务、信息技术资产或其他信息处理组件。

3.3

网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠的运行状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.4

网络安全事件

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件（以下简称事件）。

3.5

应急处置

通过采取技术手段实现网络安全事件发生后的迅速有效控制。

4 工作原则

4.1 坚持统一领导、分级负责、密切协同。
4.2 坚持统一指挥、快速反应、科学应对。
4.3 坚持谁主管谁负责、谁运行谁负责。

5 事件分类与分级

5.1 事件分类

5.1.1 恶意程序事件

恶意程序事件包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、恶意代码内嵌网页事件、恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件、混合攻击程序事件和其他恶意程序事件等 10 个子类。

5.1.2 网络攻击事件

网络攻击事件包括网络扫描探测事件、网络钓鱼事件、漏洞利用事件、后门利用事件、后门植入事件、凭据攻击事件、信号干扰事件、拒绝服务事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、DNS 污染事件、WLAN 劫持事件、流量劫持事件、BGP 劫持攻击事件、广播欺诈事件、失陷主机事件、供应链攻击事件、APT 事件和其他网络攻击事件等 21 个子类。

5.1.3 数据安全事件

数据安全事件包括数据篡改事件、数据假冒事件、数据泄露事件、社会工程事件、数据窃取事件、数据拦截事件、位置检测事件、数据投毒事件、数据滥用事件、隐私侵犯事件、数据损失事件和其他数据安全事件等 12 个子类。

5.1.4 信息内容安全事件

信息内容安全事件包括反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、权益侵害事件、信息滥发事件、网络欺诈事件和其他信息内容安全事件等 8 个子类。

5.1.5 设备设施故障事件

设备设施故障事件包括技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件和其他设备设施故障事件等 5 个子类。

5.1.6 违规操作事件

违规操作事件包括权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件、人员可用性破坏事件、资源未授权使用事件、版权违反事件和其他违规操作事件等 9 个子类。

5.1.7 安全隐患事件

安全隐患事件包括网络漏洞事件、网络配置合规缺陷事件、其他安全隐患事件等 3 个子类。

5.1.8 异常行为事件

异常行为事件包括访问异常事件、流量异常事件和其他异常行为事件等 3 个子类。

5.1.9 不可抗力事件

不可抗力事件包括自然灾害事件、事故灾难事件、公共卫生事件、社会安全事件和其他不可抗力事件等 5 个子类。

5.1.10 其它事件

其它事件指未归为上述分类的网络安全事件。

5.2 事件分级

5.2.1 概述

按照事件影响对象的重要程度、业务损失的严重程度和社会危害的严重程度三个要素，网络安全事件分为 4 个级别：特别重大事件、重大事件、较大事件和一般事件，由高到低分别为Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级。

5.2.2 Ⅰ级事件（特别重大网络安全事件）

特别重大事件发生在特别重要的事件影响对象上，并且：

a) 导致特别严重的业务损失；
b) 造成特别重大的社会危害。

5.2.3 Ⅱ级事件（重大网络安全事件）

重大事件发生在特别重要或重要的事件影响对象上，并且：

a) 导致特别重要的事件影响对象遭受严重的业务损失或导致重要的事件影响对象遭受特别严重的业务损失；
b) 造成重大的社会危害。

5.2.4 Ⅲ级事件（较大网络安全事件）

较大事件发生在特别重要或重要或一般的事件影响对象上，并且：

a) 导致特别重要的事件影响对象遭受较大或较小的业务损失，或重要的事件影响对象遭受严重或较大的业务损失，或导致一般的事件影响对象遭受较大（含）以上级别的业务损失；
b) 造成较大的社会危害

5.2.5 Ⅳ级事件（一般网络安全事件）

一般事件发生在重要或一般的事件影响对象上，并且：

a) 导致较小的业务损失；
b) 造成一般的社会危害。

6 机构和职责

6.1 机构

6.1.1 各级网络安全应急指挥部，指所在地区、部门网络安全事件应急预案中规定的本级网络安全应急指挥机构。

6.1.2 各级网络安全应急办公室，指所在地区、部门网络安全事件应急预案中规定的本级网络安全应

急指挥部的办事机构。

6.1.3　网络运营者，指网络的所有者、管理者和网络服务提供者。

6.1.4　网络产品和服务提供者，指网络设备、网络安全产品和服务的提供者。

6.1.5　省应急支撑单位，指按照《黑龙江省网络安全事件应急预案》有关规定，省委网信办牵头组织评估和认定的我省网络安全应急技术支撑队伍。

6.2　职责

6.2.1　各级网络安全应急指挥部，负责统一领导、组织和指挥所在地区、部门网络安全事件应急处置工作。

6.2.2　各级网络安全应急办公室，负责本级网络安全应急指挥部的事务性工作，具体负责本地区、本部门、本单位网络安全事件应急处置的组织和协调。

6.2.3　网络运营者，负责所拥有、管理网络的网络安全事件应急处置。

6.2.4　网络产品和服务提供者，负责按照国家法律法规以及服务合同要求协助网络安全应急办公室、网络运营者进行网络安全事件应急处置。

6.2.5　省应急支撑单位，负责在省网络安全应急办公室的组织指导下提供技术支持。

7　应急处置流程及措施

7.1　一般要求

7.1.1　相关机构可参考本标准制定的流程及措施开展网络安全事件应急处置工作，如上级部门相关通报中包含具体处置措施，建议满足上级部门相关要求的同时，结合本标准部分流程及措施开展应急处置工作。

7.1.2　网络运营者应当制定网络安全应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生网络安全事件时，立即启动应急预案，采取相应补救措施，并按照规定向有关主管部门报告。

7.2　Ⅰ级事件（特别重大网络安全事件）

7.2.1　处置流程

发生Ⅰ级网络安全事件后，网络运营者、网络安全应急办公室、应急支撑单位、网络产品和服务提供者按图A.1所示流程进行应急处理，见附录A。

7.2.2　处置管理措施

7.2.2.1　网络运营者

7.2.2.1.1　立即启动本单位网络安全应急预案进行紧急处置，同时填写《网络安全事件上报表（网络运营者）》，见附录B中表B.1。

7.2.2.1.2　立即向所在市（地）、部门网络安全应急办公室及有关主管部门报告。

7.2.2.1.3　及时向所在市（地）、部门网络安全应急办公室报告事态发展变化情况和处置进展情况。

7.2.2.1.4　配合国家网络安全应急办公室组织的调查取证。

7.2.2.1.5　按照要求采取备份数据、保护设备、排查隐患等应急措施。

7.2.2.1.6　按照要求恢复受破坏的网络和信息系统正常运行。

7.2.2.1.7　保留应急恢复过程中相关证据。

7.2.2.1.8　配合国家网络安全应急办公室组织的调查评估。

7.2.2.2　市（地）、部门网络安全应急办公室

7.2.2.2.1　立即组织先期处置。
7.2.2.2.2　组织进行事件级别研判，同时填写《网络安全事件上报表（网络安全应急办公室）》，见附录C中表C.1，若初判为特别重大（Ⅰ级）网络安全事件，立即向本级网络安全应急指挥部、省网络安全应急办公室报告。
7.2.2.2.3　配合国家网络安全应急办公室启动本地区、本部门Ⅰ级响应。
7.2.2.2.4　启动24小时值班，派员参加省网络安全应急办公室工作。
7.2.2.2.5　及时向省网络安全应急办公室报告事态发展变化情况和处置进展情况。
7.2.2.2.6　配合国家网络安全应急办公室组织的调查取证。
7.2.2.2.7　掌握本地区、本部门网络和信息系统受事件影响情况，并向省网络安全应急办公室报告。
7.2.2.2.8　协助国家网络安全应急办公室研究对策。
7.2.2.2.9　执行国家网络安全应急办公室决策部署。
7.2.2.2.10　提出其他市（地）、部门协调需求。
7.2.2.2.11　提出省网络安全应急技术支撑队伍支持需求。
7.2.2.2.12　督促相关运行单位有针对性地加强防范，防止事态蔓延。
7.2.2.2.13　协调配合网络安全事件引发的其他突发事件的应急处置。
7.2.2.2.14　按照国家网络安全应急办公室要求结束Ⅰ级响应。
7.2.2.2.15　配合国家网络安全应急办公室组织的调查评估。

7.2.2.3　省网络安全应急办公室

7.2.2.3.1　组织进行事件级别再次研判，同时填写《网络安全事件上报表（网络安全应急办公室）》，见附录C中表C.1，若研判为特别重大（Ⅰ级）网络安全事件，立即向省网络安全应急指挥部、国家网络安全应急办公室报告。
7.2.2.3.2　配合国家网络安全应急办公室启动Ⅰ级响应。
7.2.2.3.3　启动24小时值班，派员参加国家网络安全机构工作。
7.2.2.3.4　及时向国家网络安全应急办公室报告事态发展变化情况和处置进展情况。
7.2.2.3.5　配合国家网络安全应急办公室组织的调查取证。
7.2.2.3.6　协助国家网络安全应急办公室研究对策。
7.2.2.3.7　执行国家网络安全应急办公室决策部署。
7.2.2.3.8　督促相关运行单位有针对性地加强防范，防止事态蔓延。
7.2.2.3.9　提出其他省（市）协调需求。
7.2.2.3.10　开展市（地）间、部门间的工作协调。
7.2.2.3.11　协调省网络安全应急技术支撑队伍向相关市（地）、部门提供技术支持。
7.2.2.3.12　协调配合网络安全事件引发的其他突发事件的应急处置。
7.2.2.3.13　按照国家网络安全应急办公室要求结束Ⅰ级响应。
7.2.2.3.14　配合国家网络安全应急办公室组织的调查评估。

7.2.2.4　省应急支撑单位

7.2.2.4.1　协助省网络安全应急办公室提出事件处置对策意见。
7.2.2.4.2　协助省网络安全应急办公室进行调查取证。
7.2.2.4.3　按照省网络安全应急办公室要求，向相关市（地）、部门提供技术支持。

7.2.2.5 网络产品和服务提供者

7.2.2.5.1 按照国家法律法规以及服务合同要求协助网络运营者进行应急处置。

7.2.2.5.2 为调查取证、调查评估提供技术支持和协助。

7.2.3 处置技术措施

7.2.3.1 常规技术措施

7.2.3.1.1 备份系统日志、应用日志、数据库日志、审计日志、网络及安全设备日志，用于分析和溯源。相关网络日志留存周期不少于六个月。

7.2.3.1.2 检测网络设备、安全设备的安全配置情况，包括管理员账号权限与口令、配置策略、日志、访问记录等。

7.2.3.1.3 抓取被破坏系统的网络流量，检测异常流量。

7.2.3.1.4 检测异常端口与服务，关闭与业务无关端口。

7.2.3.1.5 使用专用工具检测操作系统、数据库、应用系统的安全性，发现木马、后门等，应先备份再删除。

7.2.3.1.6 重置操作系统、应用系统、数据库系统的管理员账号口令，检测用户配置策略是否正常。

7.2.3.1.7 检测操作系统、应用系统、数据库系统、开发框架、中间件的安全补丁更新情况及漏洞扫描情况。

7.2.3.1.8 检测应用系统对通过人机接口或通信接口输入数据的验证措施是否有效。

7.2.3.1.9 检测被破坏应用系统的源代码，分析代码的安全性。

7.2.3.1.10 对被破坏的应用系统开启 7×24 小时安全检测。

7.2.3.1.11 检测审计系统的工作情况，确保相关审计功能开启、审计内容和记录保存完整。

7.2.3.1.12 检测数据通信安全的有效性，确认数据传输经过加密且保证数据完整性。

7.2.3.1.13 采取其他可发现系统隐患或漏洞的技术措施。

7.2.3.1.14 检查门禁系统与视频监控系统，确保功能的可用，用于随时调用和查看。

7.2.3.1.15 其他技术措施检查与维护备品备件与冗余线路、电路，可随时根据需要替换上线。

7.2.3.2 证据留存技术措施

通过查看被攻击系统的硬件、软件配置参数、审计记录，以及从安全管理制度和人员状况等方面进行取证调查，通过截图、拍照、备份等方式收集被攻击证据，应包含以下方面：

a) 对于网络安全事件，应对被破坏系统进行断网处理，保护好系统环境，等待专业人员处置；
b) 留存当前信息系统网络拓扑图和网络拓扑结构；
c) 留存当时系统运行状态的虚拟机快照；
d) 留存系统运行状态，包括帐户登录记录、网络连接状态、文件访问状态、进程运行状态、内存镜像等易失数据；
e) 保留被破坏系统的数据、文件、源代码、异常现象拍照或截图等；
f) 在删除恶意文件前，应先做好备份，同时保存各恶意文件的哈希校验值；
g) 留存系统硬件（主机设备、网络设备、安全设备）设备及其配置参数清单；
h) 留存系统软件（操作系统）、应用软件（数据库、中间件、开发框架）的配置参数清单；
i) 留存应用程序文件列表及源代码；
j) 留存系统运维记录、系统审计日志（网络日志、操作系统日志、数据库日志、中间件日志、应用程序操作日志等）、安全产品日志；

k) 留存网络、操作系统、数据库、中间件、应用程序操作等账号权限（角色、组、用户等）的分配列表；
l) 留存其他应留存的相关证据。

7.3 Ⅱ级事件（重大网络安全事件）

7.3.1 处置流程

发生Ⅱ级网络安全事件后，网络运营者、网络安全应急办公室、应急支撑单位、网络产品和服务提供者按图D.1所示流程进行应急处理，见附录D。

7.3.2 处置管理措施

7.3.2.1 网络运营者

7.3.2.1.1 立即启动本单位网络安全应急预案进行紧急处置，同时填写《网络安全事件上报表（网络运营者）》，见附录 B 中表 B.1。
7.3.2.1.2 立即向所在市（地）、部门网络安全应急办公室及有关主管部门报告。
7.3.2.1.3 及时向所在市（地）、部门网络安全应急办公室报告事态发展变化情况和处置进展情况。
7.3.2.1.4 配合省网络安全应急办公室组织的调查取证。
7.3.2.1.5 按照要求采取备份数据、保护设备、排查隐患等应急措施。
7.3.2.1.6 按照要求恢复受破坏的网络和信息系统正常运行。
7.3.2.1.7 保留应急恢复过程中相关证据。
7.3.2.1.8 配合省网络安全应急办公室组织的调查评估。

7.3.2.2 市（地）、部门网络安全应急办公室

7.3.2.2.1 立即组织先期处置。
7.3.2.2.2 组织进行事件级别研判，同时填写《网络安全事件上报表（网络安全应急办公室）》，见附录 C 中表 C.1，若初判为重大（Ⅱ级）网络安全事件，立即向本级网络安全应急指挥部、省网络安全应急办公室报告。
7.3.2.2.3 配合省网络安全应急办公室启动本市（地）、本部门Ⅱ级响应。
7.3.2.2.4 启动 24 小时值班，派员参加省网络安全应急办公室工作。
7.3.2.2.5 及时向省网络安全应急办公室报告事态发展变化情况和处置进展情况。
7.3.2.2.6 配合省网络安全应急办公室组织的调查取证。
7.3.2.2.7 掌握本市（地）、本部门网络和信息系统受事件影响情况，并向省网络安全应急办公室报告。
7.3.2.2.8 协助省网络安全应急办公室研究对策。
7.3.2.2.9 执行省网络安全应急办公室决策部署。
7.3.2.2.10 提出其他市（地）、部门协调需求。
7.3.2.2.11 提出省网络安全应急技术支撑队伍支持需求。
7.3.2.2.12 协助省网络安全应急办公室尽快控制事态。
7.3.2.2.13 督促相关运行单位有针对性地加强防范，防止事态蔓延。
7.3.2.2.14 指导事发单位采取措施，备份数据、保护设备、排查隐患等。
7.3.2.2.15 指导事发单位恢复受破坏的网络和信息系统正常运行。
7.3.2.2.16 协调配合网络安全事件引发的其他突发事件的应急处置。
7.3.2.2.17 按照省网络安全应急办公室要求结束Ⅱ级响应。

7.3.2.2.18　配合省网络安全应急办公室组织的调查评估。

7.3.2.3　省网络安全应急办公室

7.3.2.3.1　组织进行事件级别再次研判，若研判为重大（Ⅱ级）网络安全事件，立即向省网络安全应急指挥部、国家网络安全应急办公室报告。
7.3.2.3.2　向省网络安全应急指挥部提出启动Ⅱ级响应建议，经批准后启动Ⅱ级响应。
7.3.2.3.3　启动24小时值班。
7.3.2.3.4　及时掌握事态发展变化情况和处置进展情况。
7.3.2.3.5　组织调查取证，并填写《网络安全事件现场调查表》，见附录E中表E.1。
7.3.2.3.6　重大事项及时向国家网络安全应急办公室报告。
7.3.2.3.7　组织有关市（地）、部门、应急技术支撑队伍研究对策、进行部署。
7.3.2.3.8　组织有关市（地）、部门尽快控制事态。
7.3.2.3.9　督促相关运行单位有针对性地加强防范，防止事态蔓延。
7.3.2.3.10　开展市（地）间、部门间的工作协调。
7.3.2.3.11　协调省网络安全应急技术支撑队伍向相关市（地）、部门提供技术支持。
7.3.2.3.12　协调配合网络安全事件引发的其他突发事件的应急处置。
7.3.2.3.13　报省网络安全应急指挥部批准后结束Ⅱ级响应，一般要在7个工作日内完成应急处置。
7.3.2.3.14　组织开展调查评估，并填写《网络安全事件调查评估报告》（模板），见附录F。
7.3.2.3.15　向国家网络安全应急办公室报送调查评估报告。

7.3.2.4　省应急支撑单位

7.3.2.4.1　协助省网络安全应急办公室提出事件处置对策意见。
7.3.2.4.2　协助省网络安全应急办公室进行调查取证。
7.3.2.4.3　按照省网络安全应急办公室要求，向相关市（地）、部门提供技术支持。

7.3.2.5　网络产品和服务提供者

7.3.2.5.1　按照国家法律法规以及服务合同要求协助网络运营者进行应急处置。
7.3.2.5.2　为调查取证、调查评估提供技术支持和协助。

7.3.3　处置技术措施

按7.2.3进行。

7.4　Ⅲ级事件（较大网络安全事件）

7.4.1　处置流程

发生Ⅲ级网络安全事件后，网络运营者、网络安全应急办公室、应急支撑单位、网络产品和服务提供者按图G.1所示流程进行应急处理，见附录G。

7.4.2　处置管理措施

7.4.2.1　网络运营者

7.4.2.1.1　立即启动本单位网络安全应急预案进行紧急处置，同时填写《网络安全事件上报表（网络运营者）》，见附录B中表B.1。
7.4.2.1.2　立即向所在市（地）、部门网络安全应急办公室及有关主管部门报告。

7.4.2.1.3　及时向所在市（地）、部门网络安全应急办公室报告事态发展变化情况和处置进展情况。
7.4.2.1.4　配合所在市（地）、部门网络安全应急办公室组织的调查取证。
7.4.2.1.5　按照要求采取备份数据、保护设备、排查隐患等应急措施。
7.4.2.1.6　按照要求恢复受破坏的网络和信息系统正常运行。
7.4.2.1.7　保留应急恢复过程中相关证据。
7.4.2.1.8　配合所在市（地）、部门应急机构组织的调查评估。

7.4.2.2　市（地）、部门网络安全应急办公室

7.4.2.2.1　立即组织先期处置。
7.4.2.2.2　组织进行事件级别研判，同时填写《网络安全事件上报表（网络安全应急办公室）》，见附录C中表C.1，若研判为较大（Ⅲ级）网络安全事件，4小时内向本级网络安全领导机构、省网络安全应急办公室报告。
7.4.2.2.3　根据事件的性质和情况启动Ⅲ级响应。
7.4.2.2.4　按照本市（地）、本部门应急预案做好应急处置工作。
7.4.2.2.5　及时向省网络安全应急办公室报告事态发展变化情况。
7.4.2.2.6　组织调查取证，并填写《网络安全事件现场调查表》，见附录E中表E.1。
7.4.2.2.7　提出省网络安全应急技术支撑队伍支持需求。
7.4.2.2.8　指导事发单位采取备份数据、保护设备、排查隐患等应急措施。
7.4.2.2.9　指导事发单位恢复受破坏的网络和信息系统正常运行。
7.4.2.2.10　根据事件处置情况结束Ⅲ级响应，应急处置一般要在72小时内完成。
7.4.2.2.11　组织开展调查评估，并填写《网络安全事件调查评估报告》，见附录F。
7.4.2.2.12　向省网络安全应急办公室报送调查评估报告。

7.4.2.3　省网络安全应急办公室

7.4.2.3.1　及时掌握事态发展变化情况。
7.4.2.3.2　将有关重大事项及时通报相关市（地）和部门。
7.4.2.3.3　协调省网络安全应急技术支撑队伍向相关市（地）、部门提供技术支持。
7.4.2.3.4　接收相关市（地）、部门报送的调查评估报告。

7.4.2.4　省应急支撑单位

7.4.2.4.1　按照省网络安全应急办公室要求，向相关市（地）、部门提供技术支持。

7.4.2.5　网络产品和服务提供者

7.4.2.5.1　按照国家法律法规以及服务合同要求协助网络运营者进行应急处置。
7.4.2.5.2　为调查取证、调查评估提供技术支持和协助。

7.4.3　处置技术措施

按7.2.3进行。

7.5　Ⅳ级事件（一般网络安全事件）

7.5.1　处置流程

发生Ⅳ级网络安全事件后，网络运营者、网络安全应急办公室、网络产品和服务提供者按图H.1所示流程进行应急处理，见附录H。

7.5.2 处置管理措施

7.5.2.1 网络运营者

7.5.2.1.1 立即启动本单位网络安全应急预案进行紧急处置，同时填写《网络安全事件上报表（网络运营者）》，见附录B中表B.1。

7.5.2.1.2 立即向所在市（地）、部门网络安全应急办公室及有关主管部门报告。

7.5.2.1.3 根据事件的性质和情况启动Ⅳ级响应。

7.5.2.1.4 及时向所在市（地）、部门网络安全应急办公室报告事态发展变化情况和处置进展情况。

7.5.2.1.5 保留应急恢复过程中相关证据。

7.5.2.1.6 根据事件处置情况结束Ⅳ级响应，应急处置一般要在48小时内完成。

7.5.2.2 市（地）、部门网络安全应急办公室

7.5.2.2.1 及时掌握事态发展变化情况。

7.5.2.3 网络产品和服务提供者

7.5.2.3.1 按照国家法律法规以及服务合同要求协助网络运营者进行应急处置。

7.5.2.4 处置技术措施

按7.2.3进行。

8 日常防范和应急准备

8.1 日常管理

8.1.1 日常工作

8.1.1.1 各市（地）、各部门、各单位应做好网络安全日常管理工作，包括但不限于：

a) 建立健全网络安全组织领导体系；
b) 制定网络安全规划和管理制度；
c) 制定并完善网络安全事件应急预案；
d) 健全网络安全应急处置和通报机制；
e) 实施网络安全等级保护制度；
f) 提升网络安全技术防护能力；
g) 做好网络安全检查、网络安全监测及预警管控、隐患排查、风险评估和容灾备份；
h) 加强网络安全队伍建设和人员培训等。

8.1.1.2 网络产品和服务提供者应做好日常应急准备工作，包括但不限于：

a) 发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施；
b) 按照国家法律法规及服务合同要求做好应急准备工作等。

8.1.2 人员保障

各市（地）、各部门、各单位应加强网络安全应急技术支撑队伍建设，选拔具有网络和信息系统管理经验和专业技能的人员从事网络安全管理工作，有条件的单位应建立网络安全管理专职队伍和应急技术支撑专业队伍，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援等工作。

8.1.3 经费保障

各市（地）、各部门、各单位应建立稳定的网络安全经费投入机制，有条件的单位应安排相关经费，重点支持网络安全等级保护、网络安全防护能力建设、网络安全服务、人员培训等工作。

8.1.4 宣传培训

各市（地）、各部门、各单位应加强网络安全的有关法律法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。加强网络安全应急预案的培训，提高防范意识和技能。

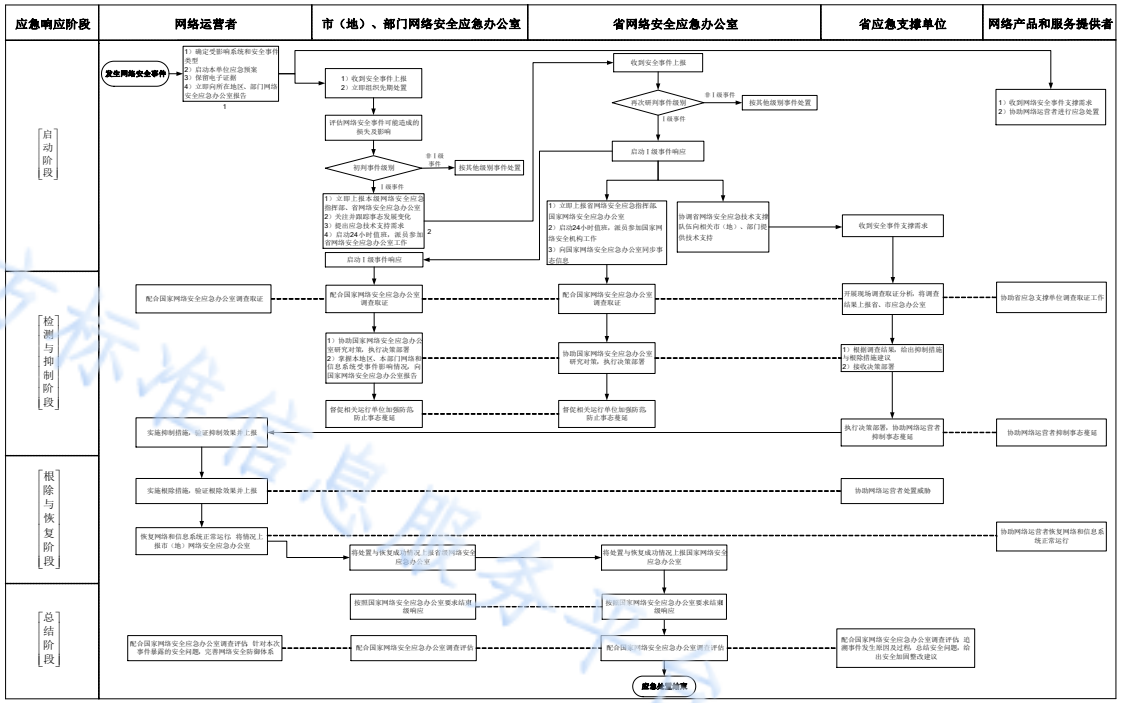
8.2 技术措施

各市（地）、各部门、各单位应及时接收相关网络安全公告以及通告，跟踪新兴和热点网络安全技术发展动态，开展网络安全审计和评估，及时对安全设备和系统进行安全、升级、加固。

8.3 应急演练

各市（地）、各部门、各单位应定期组织演练，检验应对网络安全事件的能力、应急工作的准备情况及各机构的协同配合能力。通过演练检验和完善应急预案，提高实战能力。

附 录 A
（规范性）
Ⅰ级事件处置流程图



注1：填写表单，附录B 网络安全事件上报表（网络运营者）

注2：填写表单，附录C 网络安全事件上报表（网络安全应急办公室）

图 A.1 Ⅰ级事件处置流程图

附 录 B
（规范性）
网络安全事件上报表（网络运营者）

表 B.1 网络安全事件上报表（网络运营者）

事发单位名称		报告时间	
主管单位		所在区/县	
报告人		联系电话	
通讯地址		电子邮件	
涉事系统名称		事发时间	
涉事系统业务功能			
涉事系统资产信息	（域名/URL/IP）		
事件描述			
事件来源	□自行发现 □合作机构报送 □上级通报 □其他 具体情况：		
事件类型	恶意程序	□计算机病毒 □网络蠕虫 □特洛伊木马 □僵尸网络 □恶意代码内嵌网页 □恶意代码宿主站点 □勒索软件 □挖矿病毒 □混合攻击程序 □其他	
	网络攻击	□网络扫描探测 □网络钓鱼 □漏洞利用 □后门利用 □后门植入 □凭据攻击 □信号干扰 □拒绝服务 □网页篡改 □暗链植入 □域名劫持 □域名转嫁 □DNS 污染 □WLAN 劫持 □流量劫持 □BGP 劫持攻击 □广播欺诈 □失陷主机 □供应链攻击 □APT □其他	
	数据安全	□数据篡改 □数据假冒 □数据泄露 □社会工程 □数据窃取 □数据拦截 □位置检测 □数据投毒 □ 数据滥用 □隐私侵犯 □数据损失 □其他	
	信息内容安全	□反动宣传 □暴恐宣扬 □色情传播 □虚假信息传播 □权益侵害 □信息滥发 □网络欺诈 □其他	
	设施设备故障	□技术故障 □配套设施故障 □物理损害 □辐射干扰 □其他	
	违规操作	□权限滥用 □权限伪造 □行为抵赖 □故意违规操作 □误操作 □人员可用性破坏 □资源未授权使用 □版权违反 □其他	

表 B.1 网络安全事件上报表（网络运营者）（续）

	安全隐患	□网络漏洞 □网络配置合规缺陷 □其他
	异常行为	□访问异常 □流量异常 □其他
	不可抗力	□自然灾害 □事故灾难 □公共卫生 □社会安全 □其他
	其他	□其他事件
造成的影响	□业务中断 □系统破坏 □数据丢失 □其他 具体情况：	
影响范围	□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他 具体情况：	
判定事件等级	□Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 判定依据：	
事件发展趋势		
预案执行情况		
采取紧急措施		

附 录 C
（规范性）
网络安全事件上报表（网络安全应急办公室）

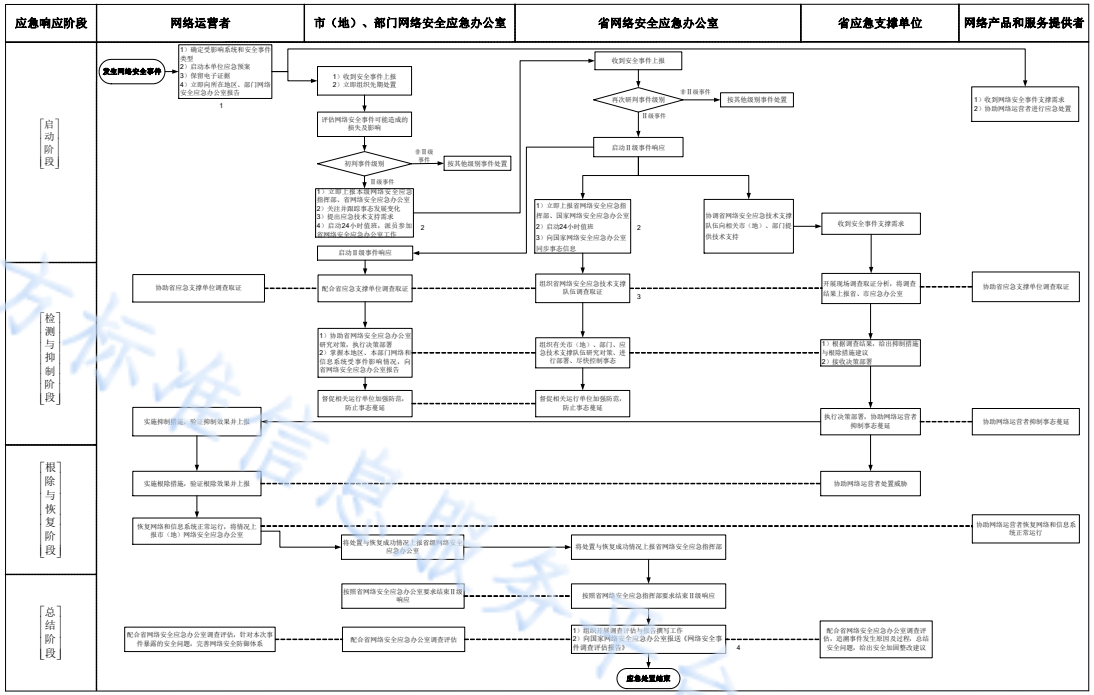
表C.1 网络安全事件上报表（网络安全应急办公室）

应急办全称		报告时间	
应急办联系人		联系电话	
事发单位名称		接收事发单位报告时间	
主管单位		所在区/县	
涉事系统名称		事发时间	
涉事系统业务功能			
涉事系统资产信息	（域名/URL/IP）		
事件描述			
事件来源	☐自行发现 ☐合作机构报送 ☐上级单位通报 ☐其他 具体情况：		
事件类型	恶意程序	☐计算机病毒 ☐网络蠕虫 ☐特洛伊木马 ☐僵尸网络 ☐恶意代码内嵌网页 ☐恶意代码宿主站点 ☐勒索软件 ☐挖矿病毒 ☐混合攻击程序 ☐其他	
	网络攻击	☐网络扫描探测 ☐网络钓鱼 ☐漏洞利用 ☐后门利用 ☐后门植入 ☐凭据攻击 ☐信号干扰 ☐拒绝服务 ☐网页篡改 ☐暗链植入 ☐域名劫持 ☐域名转嫁 ☐DNS 污染 ☐WLAN 劫持 ☐流量劫持 ☐BGP 劫持攻击 ☐广播欺诈 ☐失陷主机 ☐供应链攻击 ☐APT ☐其他	
	数据安全	☐数据篡改 ☐数据假冒 ☐数据泄露 ☐社会工程 ☐数据窃取 ☐数据拦截 ☐位置检测 ☐数据投毒 ☐ 数据滥用 ☐隐私侵犯 ☐数据损失 ☐其他	
	信息内容安全	☐反动宣传 ☐暴恐宣扬 ☐色情传播 ☐虚假信息传播 ☐权益侵害 ☐信息滥发 ☐网络欺诈 ☐其他	
	设施设备故障	☐技术故障 ☐配套设施故障 ☐物理损害 ☐辐射干扰 ☐其他	
	违规操作	☐权限滥用 ☐权限伪造 ☐行为抵赖 ☐故意违规操作 ☐误操作 ☐人员可用性破坏 ☐资源未授权使用 ☐版权违反 ☐其他	
	安全隐患	☐网络漏洞 ☐网络配置合规缺陷 ☐其他	
	异常行为	☐访问异常 ☐流量异常 ☐其他	

表C.1 网络安全事件上报表（网络安全应急办公室）（续）

	不可抗力	□自然灾害 □事故灾难 □公共卫生 □社会安全 □其他
	其他	□其他事件
造成的影响	□业务中断 □系统破坏 □数据丢失 □其他 具体情况：	
影响范围	□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他 具体情况：	
本地区/本部门其他信息系统是否受影响	□是 □否 具体情况：	
判定事件等级	□Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 判定依据：	
网络安全事件的发展趋势		
预案执行情况		

附 录 D
（规范性）
II 级事件处置流程图



注1：填写表单，附录B 网络安全事件上报表（网络运营者）

注2：填写表单，附录C 网络安全事件上报表（网络安全应急办公室）

注3：填写表单，附录E 网络安全事件现场调查表

注4：填写表单，附录F 网络安全事件调查评估报告

图 D.1 II 级事件处置流程

附 录 E
（规范性）
网络安全事件现场调查表

表E.1 网络安全事件现场调查表

应急办	单位名称			
	联系人		联系电话	
	到场人员			
应急支撑队伍	单位名称			
	联系人		联系电话	
	到场人员			
主管地区/部门	单位名称			
	联系人		联系电话	
	到场人员			
涉事单位	单位名称			
	联系人		联系电话	
	到场人员			
涉事系统现状	信息系统名称			
	涉事系统业务功能			
	涉事系统资产信息	（域名/URL/IP）		
	事件描述			
	事件来源	□自行发现 □合作机构报送 □上级单位通报 □其他 具体情况：		
	造成的影响	□业务中断 □系统破坏 □数据丢失 □其他 具体情况：		
	影响范围	□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他 具体情况：		
	信息系统资产名单	□当前系统结构拓扑图 □系统硬件设备及其配置参数清单 □系统软件、应用软件配置参数清单 □应用程序文件列表及源代码 □系统运维记录 □系统审计日志 □账号权限分配列表 □单位应急处置人员联系表 □其他		
	预处理措施			

表E.1 网络安全事件现场调查表（续）

<table>
<tr><td rowspan="14">事件处置</td><td colspan="2">分析事件成因</td><td></td></tr>
<tr><td rowspan="11">判定事类型</td><td>恶意程序</td><td>☐计算机病毒 ☐网络蠕虫 ☐特洛伊木马 ☐僵尸网络 ☐恶意代码内嵌网页 ☐恶意代码宿主站点 ☐勒索软件 ☐挖矿病毒 ☐混合攻击程序 ☐其他</td></tr>
<tr><td>网络攻击</td><td>☐网络扫描探测 ☐网络钓鱼 ☐漏洞利用 ☐后门利用 ☐后门植入 ☐凭据攻击 ☐信号干扰 ☐拒绝服务 ☐网页篡改 ☐暗链植入 ☐域名劫持 ☐域名转嫁 ☐DNS 污染 ☐WLAN 劫持 ☐流量劫持 ☐BGP 劫持攻击 ☐广播欺诈 ☐失陷主机 ☐供应链攻击 ☐APT ☐其他</td></tr>
<tr><td>数据安全</td><td>☐数据篡改 ☐数据假冒 ☐数据泄露 ☐社会工程 ☐数据窃取 ☐数据拦截 ☐位置检测 ☐数据投毒 ☐ 数据滥用 ☐隐私侵犯 ☐数据损失 ☐其他</td></tr>
<tr><td>信息内容安全</td><td>☐反动宣传 ☐暴恐宣扬 ☐色情传播 ☐虚假信息传播 ☐权益侵害 ☐信息滥发 ☐网络欺诈 ☐其他</td></tr>
<tr><td>设施设备故障</td><td>☐技术故障 ☐配套设施故障 ☐物理损害 ☐辐射干扰 ☐其他</td></tr>
<tr><td>违规操作</td><td>☐权限滥用 ☐权限伪造 ☐行为抵赖 ☐故意违规操作 ☐误操作 ☐人员可用性破坏 ☐资源未授权使用 ☐版权违反 ☐其他</td></tr>
<tr><td>安全隐患</td><td>☐网络漏洞 ☐网络配置合规缺陷 ☐其他</td></tr>
<tr><td>异常行为</td><td>☐访问异常 ☐流量异常 ☐其他</td></tr>
<tr><td>不可抗力</td><td>☐自然灾害 ☐事故灾难 ☐公共卫生 ☐社会安全 ☐其他</td></tr>
<tr><td>其他</td><td>☐其他事件</td></tr>
<tr><td colspan="2">判定事件级别</td><td>☐Ⅰ级 ☐Ⅱ级 ☐Ⅲ级 ☐Ⅳ级
判定依据：</td></tr>
<tr><td colspan="2">保留证据</td><td>☐被攻击操作系统信息 ☐日志信息
☐账号信息 ☐源代码信息
☐其他</td></tr>
<tr><td colspan="2">勘察现场</td><td>☐最新的信息系统网络拓扑图
☐系统硬件设备及其配置参数清单（☐主机设备 ☐网络设备 ☐安全设备 ☐其他_____）
☐系统软件的配置参数清单（☐操作系统 ☐数据库 ☐中间件 ☐其他_____）
☐应用程序文件列表及源代码
☐系统运维记录
☐系统审计日志（☐网络日志 ☐操作系统日志 ☐数据库日志 ☐中间件日志 ☐应用程序操作日志 ☐其他_____）
☐账号权限（角色、组、用户等）分配列表（☐网络 ☐操作系统 ☐数据库 ☐中间件 ☐应用程序 ☐其他_____）</td></tr>
<tr><td colspan="2">消除影响的措施</td><td></td></tr>
<tr><td colspan="2">溯源攻击的过程及结果</td><td></td></tr>
</table>

表E.1 网络安全事件现场调查表（续）

	系统恢复的过程及结果	
	后期整改建议	
处置人员签字	应急办代表	
	应急支撑队伍代表	
	主管部门负责人	
	事发单位负责人	

附 录 F
（资料性）
网络安全事件现场调查评估报告（模板）

一、事发单位

二、事件简述

简述该网络安全事件的发现、上报、处置、恢复等过程。

三、涉事系统情况

描述涉事系统的业务功能以及主管部门、承建单位、运维单位等情况，开展网络安全等级保护、网络安全风险评估情况等。

四、事件成因及影响

描述该网络安全事件发生的起因，以及造成的影响范围和具体影响。

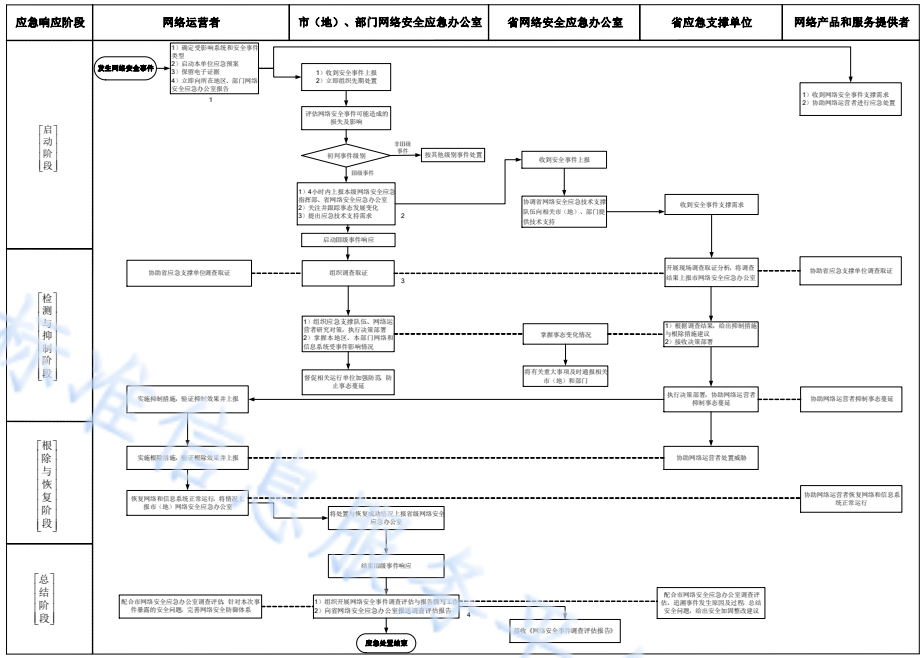
五、整改措施

描述防范网络安全事件再次发生采取的整改措施，以及经验总结。

六、处理情况

描述对发现的违法违规问题采取的处罚、问责等处理情况。

附 录 G
（规范性）
III 级事件处置流程图



注1：填写表单，附录B 网络安全事件上报表（网络运营者）

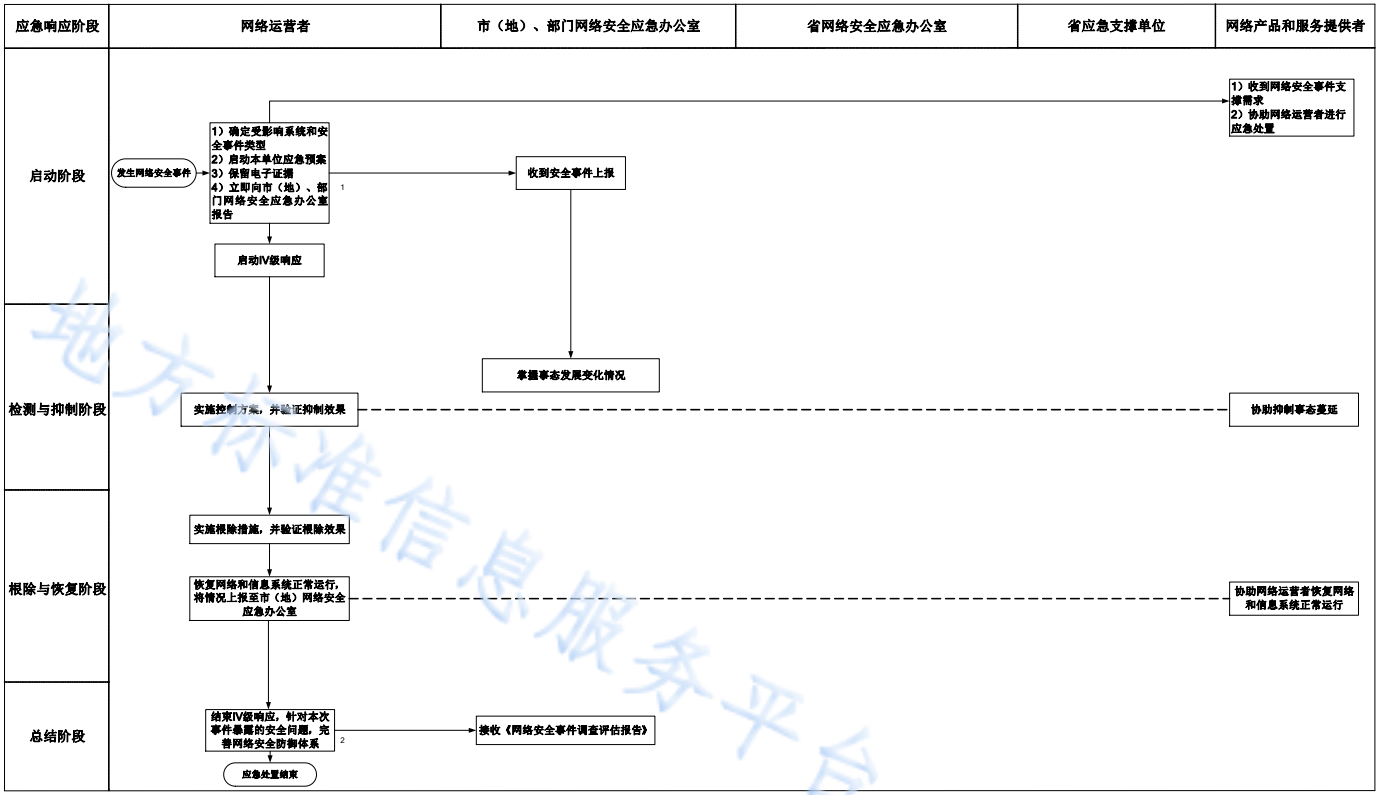
注2：填写表单，附录C 网络安全事件上报表（网络安全应急办公室）

注3：填写表单，附录E 网络安全事件现场调查表

注4：填写表单，附录F 网络安全事件调查评估报告

图 G.1 III 级事件处置流程

附 录 H
（规范性）
IV 级事件处置流程图



注1：填写表单，附录B 网络安全事件上报表（网络运营者）

注2：填写表单，附录F 网络安全事件调查评估报告

图 H.1 IV 级事件处置流程

参考文献

[1] 中华人民共和国网络安全法

[2] 国家网络安全事件应急预案（中网办发文〔2017〕4 号）

[3] 黑龙江省网络安全事件应急预案（黑政办规〔2021〕5 号）

DB 23/T 3505—2023

黑 龙 江 省

地 方 标 准

DB23/T 3505--2023

网络安全事件应急处置规范

黑龙江省互联网信息办公室

印制