ICS 33.050
CCS M 30

团　体　标　准

T/TAF 181—2023

网络产品应急响应安全要求　管理要求

Security requirements for network product emergency response—Management requirements

2023-09-11 发布　　2023-09-11 实施

电信终端产业协会　发布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
3.1　网络产品 1
3.2　应急事件 1
3.3　应急响应 1
3.4　风险评估 2
4　缩略语 2
5　网络产品应急响应安全管理框架、流程 2
6　安全事件分类分级 3
6.1　安全事件分类 3
6.2　安全事件分级 4
7　应急响应预案建立 5
7.1　预案计划编排准备 6
7.2　基础环境保障 7
7.3　应急演练 7
8　应急响应处置管理 8
8.1　事件响应上报 8
8.2　制定和实施行动方案 8
8.3　技术分析前的应急恢复 8
8.4　遏阻 8
8.5　消除威胁 9
8.6　恢复 9
8.7　响应终止 9
附录 A（资料性） 网络产品的应急响应要求与不同类型活动的对应关系 10
参考文献 11

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。

本文件中的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、上海泰峰检测认证有限公司、博鼎实华（北京）技术有限公司。

本文件主要起草人：吴荣春、刘欣东、罗丹、张亚薇、薄菁、宋祥烈、刘向东。

引　　言

随着各行业、领域信息化工作的深入开展，越来越多承载信息系统的网络产品进入了运行维护阶段。然而，提供运行维护服务的各类组织的能力水平参差不齐，需方缺乏评价方法、手段及规范。而且网络产品作为支持信息化领域建设的重要组成部分，需要制定针对网络产品的应急响应安全管理要求，以便当网络产品发生事故时，能够在最短时间启动应急响应机制。本文件主要针对网络产品在整个应急响应管理生命周期中从应急预案建立、应急响应处置管理等方面提出网络产品的应急响应安全管理要求。

网络产品应急响应安全要求　管理要求

1　范围

本文件规定了网络产品在运行维护阶段应满足的应急响应安全管理要求，主要从应急预案建立、应急响应处置管理等方面提出针对网络产品使用方的安全管理要求。

本文件适用于指导网络产品的使用方建立和维护网络产品应急响应管理体系，也可为网络设备生产方和第三方机构开展测评时提供参考。

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 20984—2022　信息安全技术　信息安全风险评估方法

GB/T 20985.2—2020　信息技术　安全技术　信息安全事件管理　第2部分：事件响应规划与准备指南

GB/T 20986　信息安全技术　信息安全事件分类分级指南

GB/T 22240—2020　信息安全技术　信息系统安全等级保护定级指南

3　术语和定义

下列术语和定义适用于本文件。

3.1

网络产品　network product

作为网络组成部分以及实现网络功能的硬件、软件或系统，按照一定的规则和程序实现信息的收集、存储、传输、交换和处理。

[来源：GB/T 39276—2020,3.2]

3.2

应急事件　emergency event

导致或即将导致运行维护服务对象运行中断、运行质量降低，以及需要实施重点时段保障的事件。

[来源：GB/T 28827.3—2012,3.2]

3.3

应急响应　emergency response

组织为预防、监控、处置和管理应急事件所采取的措施和活动。

[来源：GB/T 28827.3—2012,3.3]

3.4

风险评估 risk assessment

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。
[来源：GB/T 28827.3—2012,3.2]

4 缩略语

下列缩略语适用于本文件。
BIA：业务影响分析（Business Impact Analysis）
UPS：不间断电源（Uninterruptible Power Supply）

5 网络产品应急响应安全管理框架、流程

在风险管理的基础上，本文件提出了一套基于业务连续性管理的网络产品应急响应安全管理框架（如图 1 所示）和应急响应安全管理流程（如图 2 所示）。

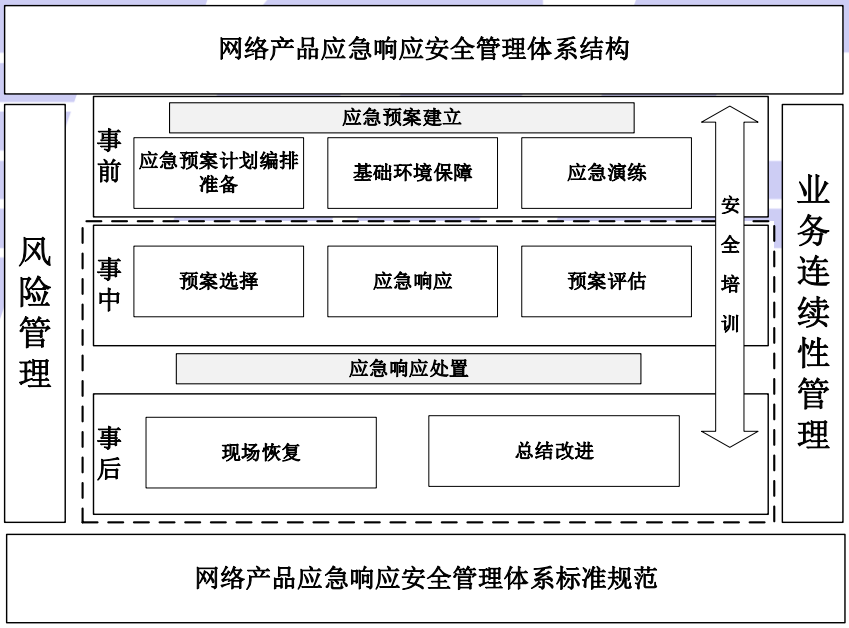

图 1 应急响应安全管理框架

应急响应安全管理框架以突发网络安全事件为关注核心，以保障业务连续性、最大程度减少损失为目标，在管理组织结构和管理标准规范的基础上，从事前（应急响应安全管理计划编排准备、基础环境保障、应急演练），事中（预案选择、应急响应、预案评估）、事后（现场恢复、总结改进）以及贯穿整个应急过程的安全培训出发，构建完整的响应处置体系。

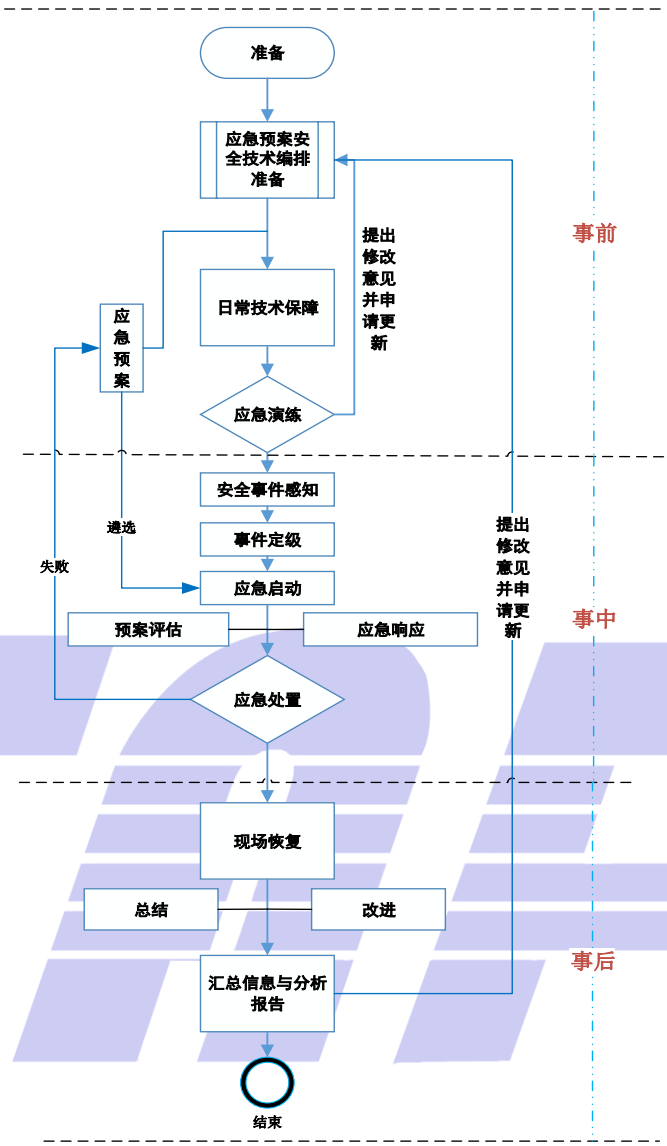

图 2 应急响应安全管理流程

应急响应安全管理流程是面向网络产品在整个应急响应管理生命周期，流程贯穿于应急预案准备到启动应急响应以及事后的现场恢复等各个方面。

6 安全事件分类分级

6.1 安全事件分类

网络产品安全事件分为恶意程序、网络攻击事件、数据攻击事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件、其他事件等十个基本分类。参照 GB/T 20986，说明如下：

a) 恶意程序：指带有恶意意图所编写的一段程序，该程序插入网络损害网络中的数据、应用程序或操作系统，或影响网络的正常运行；

b) 网络攻击事件：指通过技术手段对网络实施攻击而导致业务损失或造成社会危害的网络安全事件；
c) 数据安全事件：通过技术或其他手段对数据实施篡改、假冒、泄露、窃取等导致业务损失或造成社会危害的网络安全事件；
d) 信息内容安全事件：指通过网络传播危害国家安全、社会稳定、公共安全和利益的有害信息导致业务损失或造成社会危害的网络安全事件；
e) 设备设施故障事件：指由于网络自身出现故障或设备设施受到破坏或干扰而导致业务损失或造成社会危害的网络安全事件；
f) 违规操作事件：是指人为故意或意外地损害网络功能而导致业务损失或造成社会危害的网络安全事件；
g) 安全隐患事件：指网络中出现能被攻击者利用的漏洞或隐患，一旦被利用可能对网络造成破坏，进而导致业务损失或造成社会危害的网络安全事件。提前发现这些漏洞或隐患能防范由此引起的其他网络安全事件；
h) 异常行为事件：指网络本身稳定性不足或违规访问网络造成访问、流量等异常行为，进而导致业务损失或造成社会危害的网络安全事件；
i) 不可抗力事件：是指因突发事件损害网络的可用性而导致业务损失或造成社会危害的网络安全事件；
j) 其他事件：指未归为上述分类的网络安全事件。

6.2 安全事件分级

6.2.1 事件影响对象的重要程度

事件影响对象的重要程度根据国家安全、社会秩序、经济建设和公众利益以及业务对事件影响对象的依赖程度进行评估，分为3个等级，特别重要、重要和一般。参照GB/T 22240-2020，说明如下：

a) 特别重要：受到破坏后，对国家安全造成危害，或对社会秩序、经济建设和公共利益造成严重危害或特别严重危害；
b) 重要：受到破坏后，对社会秩序、经济建设和公共利益造成危害，或对相关公民、法人和其他组织的合法权益造成严重或特别严重损害，但不危害国家安全；
c) 一般：指受到破坏后，对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序、经济建设和公共利益。

6.2.2 业务损失的严重程度

业务损失的严重程度由网络的硬件/软件、功能和数据的损坏导致业务中断影响的严重程度进行评估，其大小可取决于恢复业务正常运行和消除网络安全事件负面影响所需付出的代价，分为4个级别：特别严重、严重、较大和较小，说明如下：

a) 特别严重：造成网络大面积瘫痪，使其丧失业务处理能力，或重要数据/敏感个人信息遭到严重破坏，恢复业务正常运行和消除安全事件负面影响所需付出的代价巨大，对于事发组织是不可承受的；
b) 严重：造成网络长时间中断或局部业务瘫痪，使其业务处理能力受到极大影响，或重要数据/敏感个人信息遭到破坏，恢复业务正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c） 较大：造成网络中断，导致业务处理能力受到较大影响，或数据/敏感个人信息受到损害，恢复业务正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d） 较小：造成网络短暂中断，导致业务处理能力受到一定影响，或数据/敏感个人信息受到影响，恢复业务正常运行和消除安全事件负面影响所需付出的代价较小。

6.2.3 社会危害的严重程度

社会危害的严重程度根据对国家安全、社会秩序、经济建设和公众利益等方面的危害程度进行评估，分为4个级别：特别重大、重大、较大和一般，说明如下：

a） 特别重大：波及一个或多个省市的大部分地区，危害到国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者特别严重损害公众利益；

b） 重大：波及一个或多个地市的大部分地区，影响到国家安全，引起社会恐慌，对经济建设有恶劣的负面影响，或者严重损害公众利益；

c） 较大：波及一个或多个地市的部分地区，不影响国家安全，但是扰乱社会秩序，对经济建设或者公众利益造成一般损害，对相关公民、法人或其他组织的利益会造成严重损害或特别严重损害；

d） 一般：波及一个地市的部分地区，不影响国家安全、社会秩序、经济建设和公众利益，但是对相关公民、法人或其他组织的利益会造成一般损害。

6.2.4 安全事件等级划分

根据网络产品的事件影响对象的重要程度、业务损失的严重程度、社会危害的严重程度，将网络安全事件划分为特大重大事件、重大事件、较大事件、一般事件四个等级。网络安全事件等级划分及对应描述情况见表1。

表 1 网络安全事件等级划分

事件等级	描述
特大重大事件	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，或 b） 造成特别重大的社会危害。
重大事件	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） 导致特别重要事件影响对象遭受严重的业务损失或导致重要事件影响对象遭受特别严重的业务损失，或 b） 造成重大的社会危害。
较大事件	较大事件发生在特别重要或一般的事件影响对象上，并且： a） 导致特别重要事件影响对象遭受较大或较小的业务损失，或重要事件影响对象遭受严重或较大的业务损失，或导致一般事件影响对象遭受较大（含）以上级别的业务损失，或 b） 造成较大的社会危害。
一般事件	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，或 b） 造成一般的社会危害。

7 应急响应预案建立

7.1 预案计划编排准备

7.1.1 应急预案体系管理

使用方在实施应急预案体系管理时应主要从梳理应急预案需求、明确应急预案目的、制定应急预案计划等方面考虑应急预案体系管理是否完备。说明如下：

a) 梳理应急预案需求

结合应急响应安全管理计划编排准备，梳理实际网络设备应急预案需求，应急预案的需求收集至少包含：网络产品资产类型、网络产品管理方式、网络产品运行拓扑、网络产品风险脆弱点以及当网络产品发生故障后必要的应急技术手段等。

b) 明确应急预案目的

明确网络产品在组织机构信息系统中的重要作用，确定网络产品作为整个应急预案管理体系中的关键要素，将网络产品暴露在外的脆弱点、风险点充分管理起来。

c) 制定应急预案计划

在制定应急预案计划时应考虑应急能力分析评估、业务响应分析、应急策略制定、应急预案的编制、审核和发布、实施和改进等。

d) 制定应急响应策略

制定应急响应策略时应考虑在业务中断、系统宕机、网络瘫痪等信息安全事件发生后，可以快速有效地恢复信息系统运行的方法。这些策略应涉及在业务影响分析（BIA）中确定的应急响应的恢复目标。

7.1.2 风险评估

使用方应标识网络产品的资产价值，识别网络产品的脆弱性，分析各种威胁发生的可能性。风险评估具体内容见 GB/T 20984—2022 的第 5 章风险评估实施。

7.1.3 业务影响分析

使用方应在风险评估的基础上，分析各种信息安全事件发生时对业务功能可能产生的影响，进而确定应急响应的恢复目标。

7.1.4 编制应急响应计划文档

使用方应编制详尽的应急响应计划文档，应急响应计划应涵盖网络产品应急操作的技术能力，并适应业务需求。可根据实际情况对其内容进行适当的调整、充实和本地化，以满足特定的系统、操作和需求。应急响应计划应明确、简洁、易于在紧急情况下执行。使用方在设计应急响应的计划文档时应有完备的管理和维护流程。可参照GB/T 20985.2—2020使用，说明如下：

a) 应建立完备的应急响应计划文档，并由专人负责保持和分发；
b) 应急响应计划文档应有多份拷贝，并在主要涉及的重要场所都有保存；
c) 应设立多个应急响应人员（安全员）管理保存应急响应计划文档；
d) 针对应急响应计划文档中涉及对网络产品应急操作技术的相关内容，应确保一定的知悉范围，可按照实际需求纳入组织机构自身的关键文档质量管理体系；
e) 应保证应急响应计划的有效性，业务流程的变化、系统的变更、人员的变更都应在应急响应计划文档中及时反映；
f) 应急响应计划在测试、演练和信息安全事件发生后实际执行时，其过程均应有详细的记录，并应对测试、演练和执行的效果进行评估，同时对应急响应计划文档进行相应的修订；
g) 应急响应计划文档应定期评审和修订，至少每年一次。

7.1.5 应急人员管理

使用方在应急响应人员管理过程中应按照领导小组、实施小组、日常运行小组等角色各司其职在日常工作、故障响应、重点时段保障等不同类型活动中完成网络产品应急响应工作，网络产品的应急响应要求与不同类型活动的对应关系参见附录A。

应急响应领导小组：由组织机构管理层及承担网络产品建设运维的主管领导干部组成，具体职责包括制定工作方案，提供人员和物质保证，审核批准应急响应策略，审核批准应急响应预案，制定应急演练方案，批准和监督应急响应预案的执行，指导应急响应实施小组的应急处置工作，启动定期评审、修订应急响应预案以及负责组织的外部协作。

应急响应实施小组：由承担网络产品建设运维的主管领导干部及具体实施运维人员组成，当由于网络产品系统崩溃、病毒攻击、非法入侵、异常宕机等原因造成网络运行异常或瘫痪时，根据信息安全事件的发展态势和实际控制需要提供网络安全技术保障，具体负责现场应急处置工作，尽快恢复网络正常运行同时负责事件书面报告提交。

应急日常运行小组：由组织机构信息中心相关人员组成，负责做好网络产品信息安全的日常巡查及日志保存工作，以确保及早发现网络产品异常。同时负责信息安全事件发生后的损失控制和损害评估，并协助应急响应实施小组快速实施应急响应工作。

7.2 基础环境保障

7.2.1 数据保障

应定时对网络产品的运行数据、配置文件和运行软件进行备份。保证在网络发生重大故障时，数据不丢失，业务不中断。

7.2.2 硬件保障

在网络建设环境对网络数据可靠性要求较高时，宜具备硬件冗余、备份等保障措施。说明如下：

a) 中心网络设备运行网为 1+N 套设备（一主多备），在参数配置和线路上完成备份的预备；
b) 对路由器、交换机、终端服务器等主要网络设备、模块，采取按照一定比例（具体比例需要根据实际情况调研）集中备份；一旦发生故障可立即切换到备品备件，不影响网络正常运行；
c) 对出口链路采用多出口负载均衡的备份方式，防止单链路故障；
d) 对已过保修期的设备，为了确保设备正常运行，宜提前购买维保服务；
e) 对汇聚层多网络设备采用集群系统，既协同工作又互为备份。

7.2.3 供电保障

在网络建设环境对供电可靠性要求较高时，宜具备供电保障措施，如中心机房应具备至少双电路供电，机房内 UPS 以并联冗余方式链接，再辅以油机供电。

7.2.4 通信保障

在应急响应基础环境保障中应确保通信信息的准确性和可连通性。说明如下：

a) 确保通信信息的准确性，保证应急日常运行小组人员和各负责人手机畅通；
b) 可连通性，保障业务期间信息通畅，能及时知晓和反馈信息。

7.3 应急演练

网络产品应根据实际应用需要开展应急演练工作，以检验应急响应工作的有效性，每年保障至少一次应急演练。在应急演练管理实施过程中应制定详细的应急演练实施方案，方案中应包括以下内容：

a) 应急演练的背景、目的和假设。这一部分应对应急演练进行基本介绍，让全体参与者对演练有初步的了解。
b) 应急演练流程。该部分通过流程图的方式，明确整个事件流程、需要完成的任务、可能出现的情况等。
c) 网络架构图、应急恢复策略及应急故障处理。这一部分为技术人员提供指引，包括熟知网络拓扑结构以及故障发生时所应进行的行动。
d) 事故上报模板、任务分配表以及岗位职责。这一部分明确了应急演练中各部门的职责和个人的任务，通过提供模板提高上报速度。

8 应急响应处置管理

8.1 事件响应上报

在实施应急响应安全管理流程时可参考图 2 应急响应安全管理流程。各级别网络安全事件应急响应上报总体要求见表 2。

表 2 事件响应上报要求

事件等级	上报要求
特大重大事件	事件发生时，立即启动应急预案，开展处置工作，控制事件发展，并将事件相关情况在事发第一时间向应急响应实施小组、应急响应领导小组上报。 事件发生后，应急日常运行小组需每小时将应急处置进展情况向应急响应领导小组汇报，直至处置结束。 事件处置结束后，应急响应实施小组应编制正式书面报告，并于 12 小时内提交应急响应领导小组。
重大事件	事件发生时，立即启动应急预案，开展处置工作，控制事件发展，并将事件相关情况在事发 30 分钟内向应急响应实施小组、应急响应领导小组上报。 事件发生后，应急日常运行小组需每 2 小时将应急处置进展情况向应急响应领导小组汇报，直至处置结束。 事件处置结束后，应急响应实施小组应编制正式书面报告，并于 1 天内提交应急响应领导小组。
较大事件	事件发生时，立即启动应急预案，开展处置工作，控制事件发展，并将事件相关情况在事发 1 小时内向应急响应实施小组、应急响应领导小组上报。 事件处置结束后，应急响应实施小组应编制正式书面报告，并于 3 天内提交应急响应领导小组，并备案。
一般事件	事件发生时，立即启动应急预案，开展处置工作，控制事件发展，并将事件相关情况在事发 1 小时内向应急响应实施小组、应急响应领导小组上报。 事件处置结束后，应急响应实施小组应编制正式书面报告，并于 5 天内提交应急响应领导小组，并备案。

8.2 制定和实施行动方案

行动方案包括对网络事件作出响应、修复，恢复网络系统至操作状态，或评估信息网络的风险所必要的行动。

8.3 技术分析前的应急恢复

进行技术分析前的网络系统应急恢复，应仔细评估潜在的技术和操作影响，以防止系统再次泄密。应保留事故中的数据，待以后进行分析。

8.4 遏阻

遏阻是通过短期的战术行动来阻止访问一个受到影响的网络产品或信息系统，限制入侵的程度，并阻止入侵者造成更多的损害。

8.5 消除威胁

在恢复服务之前，所有的威胁和风险应从网络产品和信息系统中清除。消除威胁行动包括修复网络、删除恶意软件、修复或减轻漏洞、修改访问控制等。

8.6 恢复

恢复受影响的信息系统、网络产品，使系统和网络恢复运行状态，并采取跟进策略防止事件再次发生。恢复策略包括从可信任的备份重建、验证系统数据完整性、更改系统口令、提高网络和主机安全等。

8.7 响应终止

应急实施小组完成特大和重大安全事件处置后对问题解决情况进行验证，验证内容包括问题和故障是否得到完全修复；应急处理过程中对网络和系统所做更改是否已完全恢复至正常运行时的状态；应急处置过程中的日志是否已进行完整保存。验证通过后，应急实施小组将处置结果同步至应急运行小组并将处置结果上报应急领导小组，应急领导小组收到相关领导部门结束建议后，宣布终止应急响应；应急运行小组将响应终止的决定通报各相关部门和人员。

附 录 A
（资料性）
网络产品的应急响应要求与不同类型活动的对应关系

网络产品的应急响应要求贯穿应急准备、监测与预警、应急处置和总结改进 4 个主要阶段，每个阶段中包括若干工作内容，这些工作内容覆盖了日常工作、故障响应和重点时段保障等不同类型的活动。表 A.1 描述了不同类型活动与工作内容的基本对应关系。

表 A.1　网络产品的应急响应要求与不同类型活动的对应关系表

主要阶段	工作内容	日常工作	故障响应	重点时段保障
应急准备	建立应急响应组织	√		√
	制定应急响应制度	√		√
	风险评估与改进	√		√
	划分应急事件级别	√		√
	预案制定	√		√
	培训与演练	√		√
监测预警	日常监测与预警	√	√	√
	核实与评估		√	
	预案启动		√	
应急处置	应急调度		√	√
	排查与诊断		√	√
	处理与恢复		√	
	事件升级		√	
	持续服务		√	
	事件关闭		√	
总结改进	应急工作总结		√	
	应急工作审核		√	
	应急工作改进	√	√	√

参 考 文 献

[1] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范
[2] GB/T 22239—2019 信息安全技术 信息系统安全等级保护基本要求
[3] GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范
[4] GB/T 28827.3—2012 信息技术服务运行维护 第3部分：应急响应规范
[5] GB/T 39276—2020 信息安全技术 网络产品和服务安全通用要求

电信终端产业协会团体标准

网络产品应急响应安全要求　管理要求

T/TAF181—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：82052809
电子版发行网址：www.taf.org.cn