# 数据安全应急处置办法

# 编制说明

标准起草工作组

2025 年 11 月

# 目　录

## 1 必要性

随着数据作为关键生产要素的重要性日益凸显，数据安全事件频发已成为威胁国家安全、经济运行和社会稳定的重大风险。《中华人民共和国数据安全法》明确提出建立数据安全应急处置机制的要求。为有效应对数据泄露、篡改、丢失及非法利用等安全事件，规范应急处置流程，提升组织应急响应能力，特制定本标准。

本标准旨在为数据处理者提供一套规范、高效、可操作的数据安全事件应急响应指南，覆盖事件分级、组织职责、处置流程、技术支撑及总结改进等环节，形成“监测－预警－处置”闭环管理，强化数据全生命周期安全保障能力。

## 2 工作简述

### 2.1 任务来源

本标准根据四川省网络空间安全协会数据安全团体标准制修订计划立项，由四川省网络空间安全协会归口，由成都工业职业技术学院牵头组织编制。

### 2.2 起草单位

本标准牵头起草单位：成都工业职业技术学院；

本标准参加起草单位：杭州安恒信息技术股份有限公司、全域数据信息安全重点联合实验室西南实验室。

### 2.3 起草过程

2025 年 7 月，成都工业职业技术学院向四川省网络空间安全协会提交《数据安全应急处置办法》团体标准项目建议书；

2025 年 8 月，召开《数据安全应急处置办法》团体标准启动会议，会议讨论了数据安全公开处理技术的重要性、标准框架及核心内容，确定了标准起草的总体框架、主要内容、人员分工等，确定了初步草案稿；

2025 年 9 月，由四川省网络空间安全协会邀请专家对《数据安全应急处置办法》立项评审并给出修改意见，标准成功立项，成立标准起草工作组；

2025 年 10 月，编制组根据专家意见修改标准文本，编写编制说明，团体标准《数据安全应急处置办法》已具备发布征求意见稿的质量水平；

2025 年 11 月，在“四川省网络空间安全协会微信公众号”和全国团体标准信息平台发布了团体标准《数据安全应急处置办法》征求意见稿和编制说明，通过网络向全社会广泛征求意见。

## 3 标准编制原则和主要内容

### 3.1 编制原则

本标准的制定工作遵循合规性、公开透明、协商一致、科学性等原则。

a) 合规性：在标准制订过程中，严格遵循国家已颁布的相关法律法规，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和《网络数据安全管理条例》等，并与相关国家标准 GB/T 36635-2018 和 GB/T 41479-2022 等保持一致；

b) 公开透明性：在标准制订过程中，确保成员享有平等的权利，并承担相应的义务。修订过程向所有成员开放，反映成员需求，通过公开的渠道向所有成员提供团体的标准化组织机构、运行机制、决策规则、标准制定程序及标准化工作进展等方面的信息；

c) 协商一致性：在标准制订过程中，以协商一致为原则，按照标准制定程序考虑利益相关方的不同观点，协调争议，妥善解决对实质性问题的反馈意见，获得团体成员的普遍同意；

d) 科学合理性：有利于科学合理利用资源，推广科学技术成果，增强产品的安全性、通用性、可替换性，提高经济效益、社会效益、生态效益，做到技术上先进，经济上合理；

e) 满足市场和创新需求性：在标准制订过程中，以满足市场和创新需要为目标，聚焦新技术、新产业、新业态和新模式，填补标准空白。

### 3.2 主要内容

本标准共分为8章，包括数据安全应急组织，安全事件分级与判定、应急处置办法以及工作改进几个方面，旨在明确各方职责、规范应急处置流程、统一关键动作技术指引、固化经验总结与能力提升路径，从而提升各类组织在遭遇数据安全突发事件时的快速反应能力、专业处置能力和持续改进能力，最大限度减少事件造成的损失和影响。具体如下：

1．范围：明确标准适用于数据全生命周期中的安全事件应急处置；

2．规范性引用文件：明确标准引用的规范性文件；

3．术语和定义：规范数据安全事件、应急处置、数据泄露等关键术语；

4．缩略语：明确标准中缩略语对应名称；

5．应急组织与职责：明确应急领导小组、工作小组及各团队（技术、法律、专家等）的职责分工；

6．事件分级与判定：将事件分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级），并明确判定标准与响应时限；

7．数据安全应急处置：涵盖调度准备、溯源分析、遏制根除、数据恢复、证据管理、事件关闭等全流程；

8．总结改进：包括应急处置总结、能力审核及改进计划，形成闭环管理。

## 4 技术论证与效果

### 4.1 技术要求和指标来源依据

本标准参考了《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》等法律法规，其中明确规定了数据处理者需制定应急处置预案、及时处置安全事件、履行报告义务等要求，为本标准提供了法律层面的顶层设计和合规性基础；

此外，本标准参考了GB/T 38645-2020、GB/T 22239-2019等国家标准中关于应急响应组织、流程、演练的通用框架和原则，确保了本标准与国内通用信息安全体系的一致性。

### 4.2 技术路线

本标准的制定结合起草单位在数据安全应急响应中的典型案例与技术积累。标准制定遵

循了“风险驱动、流程导向、分级处置、持续改进”的技术路线，具体包括：风险与事件识别、建立组织与职责框架、事件分级与响应联动、规范应急处置全流程、集成合规与证据管理、闭环管理与持续优化。

### 4.3 预期社会效益

本标准批准发布后，预期能够提升各级组织针对数据安全事件应急响应效率与规范性，提高数据安全防护能力，同时降低事件造成的经济损失与声誉影响，此外还能为监管机构、行业组织提供统一的应急处置参考框架。

## 5 对标情况

本标准在制定过程中充分考虑了与国内外相关标准的协调一致性，并与现行的法律法规和强制性国家标准保持了良好的衔接，以确保标准的科学性、适用性和有效性。具体分析如下：

a) 本标准与 GB/T 38645-2020 衔接，聚焦数据安全场景；

b) T/CSAS 0007-2025 全面梳理数据安全监测预警关键要素，明确监测信息采集、监测信息处理、监测信息分析和监测信息展示，规范预警类别、预警事件、预警方式和预警展示，为各行业、各领域构建数据安全监测预警体系提供指导和参考意见，从而与本标准形成“预警－处置”闭环；

c) GB/T 37988-2019 提出了数据安全能力成熟度框架，明确了成熟度各等级的数据安全要求及相关评估方法，本标准参考了 GB/T 37988-2019 应急响应要求；

d) 本标准参考了 ISO/IEC 27035 系列标准的事件处理流程；

e) 本标准借鉴了 NIST SP 800-61 的应急响应最佳实践。NIST SP 800-61 侧重信息安全管理与防护方面的操作实践和技术细节，尤其强调事件响应步骤（准备－检测－分析－遏制－清除－恢复－总结），为企业和机构提供操作性指南。

## 6 标准实施建议

### 6.1 组织措施

成立专门的标准实施工作组，负责统筹协调标准的实施工作，明确各部门的职责和分工。

开展标准宣传与培训，提高其对标准的理解和执行能力，切实提升相关职能人员的应急响应能力。

### 6.2 技术措施

各组织建议部署日志审计、SIEM、DLP 等技术设备或系统，支持事件监测与溯源，同时建立应急响应平台，实现流程自动化与协同处置。

### 6.3 过渡办法

对于已建立应急机制的组织可按本标准调整和优化现有流程，确保业务数据安全。

对于未建立机制的组织应按照标准的实施步骤，建立数据安全事件定级机制以及应急处置工作流程，逐步完善应急能力。

## 7 需要说明的主要问题

本标准在编制过程中未出现需要说明的主要问题。

## 8 其他说明事项

本标准在编制过程中未出现其他说明事项。