|  |  |
| --- | --- |
| ICS  | 03.120.20 |
| CCS  |

|  |
| --- |
| D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png XJBX |

A 50 |

西安市计量标准检测认证协会团体标准

T/XJBX 0067—2025

检验检测机构数据溯源操作指引

Guidelines for data traceability operations in inspection and testing institutions

2025 - XX - XX发布

2025 - XX - XX实施

西安市计量标准检测认证协会  发布

目次

[前言 III](#_Toc205750094)

[引言 V](#_Toc205750095)

[1 范围 1](#_Toc205750096)

[2 规范性引用文件 1](#_Toc205750097)

[3 术语和定义 1](#_Toc205750098)

[4 总体要求 2](#_Toc205750099)

[5 数据溯源流程 3](#_Toc205750100)

[6 技术方法与实现要求 4](#_Toc205750101)

[7 管理与监督 5](#_Toc205750102)

[8 应急响应与风险管理 6](#_Toc205750103)

1. 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。

本文件由西安市计量标准检测认证协会提出并归口。

本文件起草单位：那曲市检验检测中心。

本文件主要起草人：安亚彬。

1. 引言

在检验检测活动中，数据的真实性、完整性和可追溯性是保证检测结果科学性、公正性和权威性的核心要素。随着信息化、数字化技术的广泛应用，检验检测机构在数据采集、处理、传输、存储及归档等环节面临着数据来源不明、过程记录不全、信息篡改风险增加等问题。这不仅影响检测结论的可靠性，也可能导致监管审查或法律诉讼中的证据链缺失。

数据溯源是指通过记录与追踪数据在产生、处理、传输及保存全过程中的关键信息，实现对数据来源、处理过程及使用情况的可验证性与可重现性。通过建立系统化、标准化的数据溯源管理体系，检验检测机构不仅能够提升检测结果的可信度和重现性，还能有效满足监管部门、客户及行业对数据合规性和透明度的要求。

本文件指引结合检验检测领域的实际需求与信息化发展趋势，参考国内外相关标准与最佳实践，对数据溯源的原则、流程、技术方法和管理措施进行规范，明确从数据采集到归档全过程的操作要求，指导检验检测机构建立可验证、可复现、可审计的数据溯源体系，保障检测活动的科学性、规范性和可追溯性。

检验检测机构数据溯源操作指引

* 1. 范围

本文件规定了检验检测机构在数据溯源管理中的总体要求、原则、流程、技术方法及管理措施，涵盖数据采集、传输、处理、分析、存储、归档及调用等环节的操作规范。

本文件适用于各类从事检验检测活动的机构，包括但不限于质量检验机构、环境监测机构、食品检测机构、医疗检测实验室、计量检定机构等。本文件亦适用于相关行业管理部门、认证认可机构在监督、评审和技术指导过程中对数据溯源工作的参考。

本文件可为检验检测机构在建立或完善数据溯源体系时提供操作性指导，也可为信息系统开发商、数据管理服务提供商在设计和实施数据溯源功能时提供技术参考。

* 1. 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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 27025—2019 检测和校准实验室能力通用要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

* 1. 术语和定义

下列术语和定义适用于本文件。

数据溯源 data traceability

通过记录与追踪数据在采集、处理、传输、存储及使用全过程中的关键信息，实现对数据来源、处理过程和使用情况的验证与重现的能力。

数据完整性 data integrity

数据在其全生命周期内保持准确、完整、一致且未经未经授权篡改的特性。

元数据 metadata

描述数据属性、来源、结构、处理方式及使用条件的结构化信息，用于支持数据的理解、管理和溯源。

审计追踪 audit trail

按时间顺序记录系统活动、数据操作和变更历史的日志集合，用于追溯和验证数据的产生与变动情况。

数据版本控制 data version control

通过记录数据在修改、更新、合并等操作过程中的版本信息，实现对不同时间点数据状态的管理和回溯。

数据生命周期 data lifecycle

数据从产生、处理、传输、存储、使用直至归档或销毁的全过程。

数据安全 data security

保护数据免遭未经授权的访问、泄露、篡改、破坏或丢失的能力与措施。

* 1. 总体要求
		1. 原则要求

检验检测机构在开展数据溯源工作时，应遵循真实性、完整性、可追溯性、安全性与合规性原则，确保检测数据全生命周期可验证、可复现，并符合相关法律法规及行业标准的要求。

* + 1. 管理体系

机构应建立覆盖数据采集、传输、处理、分析、存储、归档及调用等全过程的数据溯源管理体系，并将其纳入质量管理体系或信息安全管理体系中，确保职责明确、流程规范、责任到人。

* + 1. 技术支撑

应采用适配的信息化技术手段实现数据溯源，包括但不限于自动化记录、元数据管理、审计追踪、数据版本控制及加密存储等，确保溯源信息的准确性与不可篡改性。

* + 1. 过程记录

在数据产生、处理及使用的各关键环节，应同步生成且保存包含时间戳、操作者、设备标识、数据版本等信息的过程记录，以支撑事后验证和重现。

* + 1. 人员培训

机构应定期对相关人员开展数据溯源管理与操作培训，确保人员具备数据溯源意识与技能，能够按照操作指引执行相关任务。

* + 1. 持续改进

应建立数据溯源体系的定期评估与优化机制，结合内部审核、外部评审及技术发展趋势，持续提升溯源管理水平和技术能力。

* 1. 数据溯源流程

检验检测机构应按照数据全生命周期管理的要求，对数据溯源流程进行标准化设计和实施。典型流程包括数据采集、数据传输、数据处理、数据存储、数据使用与发布、数据归档与销毁等环节，每个环节均应生成可追溯记录。

* + 1. 数据采集

在采集检测数据时，应自动记录采集时间、采集设备、操作者身份、采集环境及原始数据文件的唯一标识。

原始数据应在采集后立即进行完整性校验，并生成校验码（如哈希值）用于后续验证。

对于自动化检测设备，应确保系统日志可记录采集过程中的所有参数设置与运行状态。

* + 1. 数据传输

数据传输应采用加密通道（如TLS/SSL、VPN等）确保传输安全。

传输过程应生成记录，包括起始时间、结束时间、传输路径、接收方信息及传输文件的完整性验证结果。

对跨系统、跨网络传输，应增加数字签名或双向认证机制，防止数据被篡改或替换。

* + 1. 数据处理

任何数据处理操作（如格式转换、数据清洗、计算分析等）应自动记录处理时间、操作者、处理工具及算法版本。

处理前后数据均应存储并关联版本信息，保留可重现的操作路径。

对关键分析环节，应保存运行日志及中间结果文件。

* + 1. 数据存储

存储系统应具备访问控制和权限管理功能，确保仅授权人员可访问相应数据。

存储数据应进行定期备份，并在备份记录中注明备份时间、存储位置、备份介质编号等信息。

应建立防篡改机制（如WORM存储、区块链存证）保障数据不可随意修改。

* + 1. 数据使用与发布

在调用或发布数据时，应记录调用/发布时间、用途、接收方信息及所使用数据的版本号。

对外发布的数据应经过审批流程，并保留发布审批记录与发布内容备份。

* + 1. 数据归档与销毁

数据归档应记录归档时间、归档位置、文件清单及校验码。

数据销毁应有审批和执行记录，注明销毁方式（物理销毁或安全擦除）、销毁时间、执行人及见证人信息。

对涉及法律诉讼、监管调查的数据，应暂停销毁直至相关事项结束。

* 1. 技术方法与实现要求
		1. 总则

检验检测机构应结合业务类型、数据特性与信息化水平，选择并部署适用的技术手段实现数据溯源管理。技术方案应保证溯源数据的准确性、完整性、可追溯性与不可篡改性，并具备可扩展和可持续运行能力。

* + 1. 元数据管理

元数据应覆盖数据全生命周期的重要属性，包括但不限于数据标识、采集时间、采集设备型号及编号、操作者身份、处理算法版本、存储位置及访问记录。

应采用统一的元数据编码与格式标准，支持跨平台、跨系统的互联互通与解析。

元数据应与原始数据及处理结果进行关联存储，确保关联关系的持久性和可验证性。

元数据存储应具备防篡改机制，并配置定期备份与完整性校验功能。

* + 1. 审计追踪与日志管理

系统应自动生成并保存操作日志，记录数据在采集、传输、处理、存储、发布、归档及销毁各环节的时间戳、操作者、操作类型、数据标识及结果状态。

审计日志应采用不可篡改的存储机制（如只读介质、区块链存证等）确保真实性。

应设置日志访问权限，防止未经授权的修改与删除。

审计追踪数据的保存期限应满足法规及合同要求，并在到期前进行归档或备份。

* + 1. 数据版本控制

对任何数据的新增、修改、合并及删除操作，系统应自动生成版本号并保留历史版本。

版本记录应包含版本号、创建时间、变更内容摘要、变更人及变更原因。

应支持基于版本号的一键回溯，确保检测结论和数据分析结果可复现。

对关键检测数据，建议采用差异化存储与全量备份结合的方式，提高版本管理效率。

* + 1. 数据完整性与真实性保障

应采用哈希算法（如SHA-256）或数字签名对关键数据及溯源记录进行校验，并在数据传输、备份、调用等环节验证完整性。

对比校验结果应自动生成记录，并在异常情况下触发告警与事件响应流程。

对采集自外部系统或第三方机构的数据，应保留数据来源证明及传输链路验证记录。

* + 1. 加密与访问控制

数据在传输与存储过程中应采用加密技术（如AES、RSA等）防止非法窃取与篡改。

应实施基于角色的访问控制（RBAC）或基于属性的访问控制（ABAC），确保用户仅能访问其工作范围内的数据。

应定期对用户权限进行审查，及时撤销离职或岗位变动人员的访问权限。

对涉及敏感信息的数据，应采用分级保护策略，并配置多因素身份认证。

* + 1. 新兴技术应用

对于高价值或高敏感度的检测数据，可引入区块链技术进行分布式存证，实现跨机构的数据溯源与验证。

结合人工智能技术进行溯源数据的异常检测与模式识别，提高风险发现的及时性。

利用云计算和边缘计算技术优化数据存储与处理效率，确保大规模数据的溯源可行性。

* 1. 管理与监督
		1. 管理体系建设

检验检测机构应将数据溯源管理纳入整体质量管理体系和信息安全管理体系，形成制度、流程、技术和人员四个方面的综合保障框架。制度应涵盖数据溯源的管理目标、职责分工、运行机制、考核办法及改进措施，并通过文件化形式予以发布和执行。

* + 1. 组织与职责

应设立或指定专门的管理部门负责数据溯源工作的统筹与监督，明确机构负责人、技术负责人、信息管理员、业务操作员等在数据采集、处理、存储、传输、发布及归档等环节的具体职责。对涉及关键信息的岗位，应实行岗位分离和权限隔离，防止单一人员对数据链路的完全控制。

* + 1. 人员能力与培训

机构应建立数据溯源相关岗位的能力标准与培训体系，对新入职及在岗人员定期开展数据管理、信息安全、法规标准、应急处理等方面的培训。培训记录应完整保存，并纳入人员考核结果，作为岗位任职和晋升的重要依据。

* + 1. 内部监督与检查

应制定年度内部审核计划，定期对数据溯源的完整性、准确性、可追溯性进行抽查与全流程检查。检查内容应涵盖制度落实情况、溯源记录完整性、技术防护措施有效性及异常处理闭环情况。对发现的问题应形成整改清单，明确责任人、整改时限及验证结果。

* + 1. 外部监督与合规审查

应配合主管部门、认证认可机构及第三方评估机构开展监督检查，按要求提供完整的溯源链信息、审计日志及相关证明材料。对外部审查中发现的不符合项，应立即制定整改计划，并将整改结果在内部通报，以推动全员改进。

* + 1. 持续改进与绩效评估

应建立基于绩效考核的持续改进机制，将数据溯源的有效性和规范性纳入机构年度绩效评价。通过分析监督检查、用户反馈及新技术应用效果，定期优化溯源管理流程与技术手段，确保体系的长期适应性和先进性。

* 1. 应急响应与风险管理
		1. 总则

检验检测机构应建立覆盖数据全生命周期的应急响应与风险管理体系，确保在数据溯源过程中发生异常或突发事件时，能够快速定位问题、有效处置并恢复正常运行，最大限度地减少对检测活动的影响。该体系应纳入机构整体质量管理与信息安全管理框架，并与业务连续性管理相衔接。

* + 1. 风险识别与评估

机构应定期开展风险识别，覆盖数据采集、传输、处理、存储、发布、归档及销毁等所有环节。

风险因素包括但不限于硬件设备故障、软件漏洞、网络攻击、非法访问、数据篡改、操作失误、自然灾害及停电等。

应采用风险矩阵法、失效模式与影响分析（FMEA）等方法，对风险发生的可能性和影响程度进行评估，并形成风险清单。

* + 1. 风险防控措施

对高风险环节应制定预防措施，如多级权限控制、双人复核、自动化完整性校验、防篡改存储等。

关键数据应实施多副本存储及异地容灾备份，并定期进行备份有效性验证。

对外部网络访问应采用防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等安全防护手段。

* + 1. 异常监测与告警

系统应具备实时监测功能，能够发现数据缺失、完整性校验失败、异常访问行为等情况。

异常事件发生时，应自动触发告警，通过多渠道（短信、邮件、系统弹窗等）通知管理人员。

告警信息应包含事件类型、发生时间、受影响的数据范围及初步建议措施。

* + 1. 应急处置流程

应急处置流程如下：

1. 机构应制定详细的应急处置预案，包括事件分级、应急响应小组组成、职责分工、处置步骤及恢复计划；
2. 发生数据异常或溯源记录异常时，应立即启动应急响应，优先保护原始数据与溯源链完整性；
3. 在应急处置过程中，应同步记录所有操作及决策，以便事后审计与改进。
	* 1. 恢复与改进

应在应急事件结束后开展事件调查，分析根本原因并提出防范建议。

对应急响应过程进行复盘，评估预案的有效性并及时修订。

对暴露出的技术或管理薄弱环节，应制定整改措施并跟踪落实，形成闭环管理。

* + 1. 演练与培训

应定期组织数据溯源应急演练，包括桌面推演和实战模拟，检验预案可行性与人员应对能力。

应将应急响应与风险管理培训纳入年度培训计划，确保相关人员熟悉流程与操作要点。

