ICS 35.020
CCS L 70

DB6101

西　　安　　市　　地　　方　　标　　准

DB 6101/T 3189—2024

检验检测数据管理规范　数据安全

2024－06－04 发布　　2024－07－04 实施

西安市市场监督管理局　　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。

本文件由西安市市场监督管理局提出并归口。

本文件起草单位：瑞特认证检测集团有限公司、陕西瑞智信息技术有限公司、中铁一局集团有限公司、陕西汉通建设工程质量检测有限公司、陕西省建筑工程质量检测中心有限公司、西安市质量与标准化研究院、西安尚易安华信息科技有限责任公司、国网陕西省电力公司西安供电公司、湖北铁建工程检测有限公司。

本文件主要起草人：曹原、王晖、祁喆、胡亚芹、曹珺溥、畅亚文、张源、刘欣、刘娟、范文丽、田鹏辉、刘雯、王磊、马良。

本文件由瑞特认证检测集团有限公司负责解释。

本文件首次发布。

本文件在实施过程中如有疑问或建议，请将咨询或修改建议等信息反馈至下列单位：

单位：瑞特认证检测集团有限公司

地址：陕西省西安市蓝田县华胥镇西北家具工业园区新港七路8号

电话：029-82889599

邮编：710523

检验检测数据管理规范　数据安全

1　范围

本文件规定了检验检测数据管理总则、基本要求、数据安全管理和证实方法的要求。

本文件适用于西安市检验检测数据管理的数据安全要求。

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 11457　信息技术　软件工程术语

GB/T 37973　信息安全技术　大数据安全管理指南

GB/T 37988　信息安全技术　数据安全能力成熟度模型

3　术语和定义

GB/T 11457、GB/T 37973、GB/T 37988界定的术语和定义适用于本文件。

3.1

数据安全

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.2

大数据

具有数量巨大、种类多样、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理技术进行有效组织、存储、计算、分析和管理的数据集。

[来源：GB/T 37973—2019，3.1]

3.3

数据脱敏

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019，3.12]

3.4

完整性

系统或部件防止未授权访问或修改计算机程序或数据的程度。

[来源：GB/T 11457—2006，2.789]

4　总则

检验检测业务数据处理活动主要围绕着检验检测的业务功能展开，产生的数据包括但不限于：样品信息、见证取样信息、抽样信息、受理信息、检验信息和报告信息。

检验检测业务数据的生命周期各个阶段包括：数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据删除。

5 基本要求

5.1 组织应明确检验检测数据安全策略，制定方针、目标和原则，形成文件。
5.2 数据安全应覆盖数据生命周期相关的业务、系统和应用，并明确与之相关的岗位、人员和职责。
5.3 应建立数据安全风险评估体制机制，有效实施，并持续改进其有效性和效率。
5.4 应建立数据安全应急响应体系，包括应急预案、应急演练、监测与预警、应急处置流程、保障措施等内容。

6 数据安全管理

6.1 数据收集

6.1.1 应建立数据收集操作规程，覆盖检验检测数据收集全过程，明确数据收集的数据源、获取目的，并应对数据收集的环境、设施和技术工具进行评估。
6.1.2 应采取必要的技术手段对数据收集过程进行监视，规范数据获取渠道及其获取数据格式、获取流程和获取方式，并定期评估数据获取操作规程的合规性。
6.1.3 应在数据获取、清洗、标识、加载过程中，采用必要的安全措施。

6.2 数据存储

6.2.1 应建立数据存储安全管理操作规程，按照检验检测数据类型确定数据存储期限进行留存，对数据存储的环境、设施和技术工具进行评估。
6.2.2 应采取必要的技术措施满足不同层次数据加密存储能力。
6.2.3 应在数据副本、备份、归档、留存、密钥管理过程中，采用必要的安全措施。

6.3 数据使用

6.3.1 应明确数据使用制度，对数据使用全过程进行有效监控，使用数据前进行安全评估，符合要求后方可使用，数据使用后应进行有效跟踪并评估其安全影响。
6.3.2 应综合业务需要采用访问控制机制。
6.3.3 应在展示敏感信息时，采用必要的数据脱敏等技术。

6.4 数据加工

6.4.1 应建立数据加工安全操作规程，根据检验检测数据相关适用标准的要求以及业务需求，对敏感检验检测数据进行脱敏处理，保证数据可用性和安全性。
6.4.2 应对检验检测数据脱敏处理过程的操作记录进行保存，以满足数据脱敏处理安全审计要求。

6.5 数据传输

6.5.1 应建立数据传输安全操作规程，通过部署安全通道、数据加密等措施保证大数据系统中数据传输的保密性，对数据传输的环境、设施和技术工具进行评估。
6.5.2 应采用断点续传、超时重新连接等技术机制，保障数据传输任务的可靠性，并具备对传输数据的完整性进行验证的能力。

6.6 数据提供

6.6.1 应建立数据提供安全操作规范、规程，明确数据提供活动涉及的职能部门和岗位相关的用户职责和权限，保证数据提供安全策略的有效性。
6.6.2 应对数据提供活动进行监控，并采用数据加密、安全通道等管控措施提供数据，定期评估数据提供通道的安全性。
6.6.3 应制定数据提供活动安全审计策略和审计日志管理操作规范，记录数据提供活动日志。

6.7 数据公开

6.7.1 应建立数据主动公开发布管理制度和操作规范，明确发布数据使用者的权利和义务。
6.7.2 应提供数据发布清单，包括发布数据摘要、数据格式、更新频率等内容,以及使用条件等。
6.7.3 应定期审核发布数据资源的使用报告。

6.8 数据删除

6.8.1 应建立组织的数据删除流程，明确删除安全要求，对删除数据进行审批、记录，确保所有过程可控、可溯源、可审计。
6.8.2 应建立不可逆数据删除机制，配置必要的数据删除工具，能根据业务场景需求以不可逆方式删除相关的数据及其衍生的各种副本数据。
6.8.3 应建立数据删除效果评估和复核机制，定期检查已被删除的数据是否还能访问。

7 证实方法

7.1 验证内容

数据收集、存储、使用、加工、传输、提供、公开、删除各阶段的要求。

7.2 验证方法

7.2.1 应对数据处理活动及其数据操作服务的安全进行监测，对数据处理活动及其数据操作服务的访问进行监控。
7.2.2 应定期对检验检测系统的安全控制措施进行检查，使所采取的安全措施覆盖数据生命周期各个阶段。
7.2.3 应定期安排或在爆发网络攻击、重大安全漏洞时，及时开展专项安全检查。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[3] GB/T 35274—2023 信息安全技术 大数据服务安全能力要求
[4] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求
[5] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求