|  |  |
| --- | --- |
| ICS | 35.020 |
| CCS | L 70 |

|  |
| --- |
| 61 |

陕西省地方标准

DB 61/T XXXX—XXXX

检验检测机构资质认定

第31部分：电子数据管理规范

点击此处添加标准名称的英文译名

XXXX - XX - XX发布

XXXX - XX - XX实施

       发布

目次

[前言 II](#_Toc174456033)

[1 范围 1](#_Toc174456034)

[2 规范性引用文件 1](#_Toc174456035)

[3 术语和定义 1](#_Toc174456036)

[4 基本要求 1](#_Toc174456037)

[5 数据管理 1](#_Toc174456038)

[5.1 数据采集 1](#_Toc174456039)

[5.2 数据存储 2](#_Toc174456040)

[5.3 数据使用 2](#_Toc174456041)

[5.4 数据加工 2](#_Toc174456042)

[5.5 数据传输 2](#_Toc174456043)

[5.6 数据提供 2](#_Toc174456044)

[5.7 数据公开 2](#_Toc174456045)

[5.8 数据删除 2](#_Toc174456046)

[6 数据安全 2](#_Toc174456047)

[7 证实方法 3](#_Toc174456048)

[7.1 验证内容 3](#_Toc174456049)

[7.2 验证方法 3](#_Toc174456050)

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。

本文件是DB61/T 1327《检验检测机构资质认定》的第21部分。DB61/T 1327已经发布了以下部分：

1. 第1部分：评审指南；
2. 第2部分：现场试验考核技术要求；
3. 第3部分：设备检定和校准结果确认要求；
4. 第4部分：设备期间核査要求；
5. 第5部分：检验检测报告编制规范；
6. 第6部分：评审员管理要求；
7. 第7部分：内部审核要求；
8. 第8部分：检验检测机构从业人员行为要求；
9. 第9部分：设备验证要求；

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。

本文件由陕西省市场监督管理局提出并归口。

本文件起草单位：陕西省质量认证认可协会、西安思源学院、中国合格评定国家认可中心、陕西省计量测试学会、西北国家计量测试中心办公室、西安市质量与标准化研究院、中国国检测试控股集团陕西有限公司、陕西高速公路工程试验检测有限公司、陕西诺盈自动化仪表有限公司、陕西通标认证中心有限公司。

本文件主要起草人：董敏、杨洁、王阳、胡畅、李磊、付磊、李元沉、苏美冬、李军荣、马腾、温美晨、王涛、韩晓宇、王诤。

本文件为首次发布。

本文件由陕西省质量认证认可协会负责解释。

联系信息如下：

单位：陕西省质量认证认可协会

电话：029-87290790, 029-87291424

地址：陕西省西安市新城区西五路68号

检验检测机构资质认定

第31部分：电子数据管理规范

* 1. 范围

本文件规定了检验检测机构电子数据管理基本要求、数据管理、数据安全和证实方法的要求。

本文件适用于获得资质认定检验检测机构电子数据管理。

* 1. 规范性引用文件

本文件没有规范性引用文件。

* 1. 术语和定义

本文件没有需要界定的术语和定义。

* 1. 基本要求

组织应明确检验检测机构电子数据管理边界，制定方针、目标和原则，并形成文件。

电子数据应覆盖检验检测机构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。

电子数据管理应包括数据生命周期各个阶段：数据采集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据删除等。

应建立数据安全风险评估机制，有效实施并持续改进。

* 1. 数据管理
     1. 数据采集

应建立数据采集操作方法，覆盖检验检测机构电子数据采集全过程，明确数据采集的数据源、获取目的，并应对数据采集的环境、设施和技术工具进行评估。

应规范数据采集渠道及其采集数据格式、采集流程和采集方式，并定期评估数据采集操作方法的合规性。

应使用计算机终端、移动设备或自动化采集仪器设备通过人工填报、人工导入或自动采集等方式采集数据。

采集的数据应进行电子化处理形成电子数据。

应保留采集数据的原始记录，数据来源可追溯。

* + 1. 数据存储

应依据相关标准对数据存储的环境、设施和技术工具进行评估。

应按照检验检测机构电子数据类型明确其存储方式、存储格式和存储介质及存储期限。

应采取必要的技术措施满足不同层次数据加密存储需求。

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。

* + 1. 数据使用

应明确数据使用制度，建立数据使用监控机制，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。

应建立访问控制机制，使其在规定的权限范围内使用数据。

使用敏感信息时，应采用必要的数据脱敏技术。

* + 1. 数据加工

应根据检验检测数据相关适用标准的要求以及业务需求建立数据加工全操作方法，保证数据可用性和安全性。

应对检验检测数据加工处理过程的操作记录进行保存，以满足数据可追溯要求。

* + 1. 数据传输

应建立数据传输操作方法，对数据传输的环境、设施和技术工具进行安全评估。

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。

* + 1. 数据提供

应明确数据提供活动涉及的职能部门、岗位和用户的职责和权限，保证数据提供的有效性。

应对数据提供活动进行监控，并记录数据提供活动日志。

* + 1. 数据公开

应建立数据公开发布管理制度，明确发布数据使用者的权利和义务。

应提供数据发布清单，包括数据摘要、数据格式、更新频率等内容,以及使用条件等。

应定期审核发布数据资源的使用报告。

* + 1. 数据删除

应建立数据删除制度，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。

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。

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。

* 1. 数据安全

组织应明确检验检测机构电子数据管理安全策略，建立数据安全风险评估机制，有效实施并持续改进。

在数据采集和存储时，应采用必要的安全措施。

在数据使用、加工、提供和公开时，应采用必要的数据脱敏技术。

在数据传输和提供时，应采用数据加密、安全通道等管控措施。

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。

* 1. 证实方法
     1. 验证内容

第4章～第6章中的要求，以及环境要求。

* + 1. 验证方法

应对数据管理活动及其数据操作进行监测，对数据处理活动及其数据操作服务的访问进行监控。

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。

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。

