

ICS 35.240.50

CCS N 77

T

团体标准

T/CEATEC XXX—2026

试剂、标准物质数字化管理系统技术规范

Technical specification for digital management system of reagents and
reference materials

2026-XX-XX 发布

2026-XX-XX 实施

中国欧洲经济技术合作协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总体原则 1

 4.1 合规性原则 1

 4.2 全程溯源原则 2

 4.3 安全可控原则 2

 4.4 数据规范原则 2

 4.5 实用高效原则 2

5 系统总体架构 2

 5.1 总体架构 2

 5.2 数据采集层 2

 5.3 业务功能层 2

 5.4 数据管理层 3

 5.5 安全管控层 3

6 系统技术要求 3

 6.1 运行性能要求 3

 6.2 软硬件环境要求 3

 6.3 数据技术要求 4

 6.4 权限管理要求 4

7 运维要求 4

 7.1 日常运维要求 4

 7.2 周期运维 4

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。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次编制。

试剂、标准物质数字化管理系统技术规范

1 范围

本文件规定了试剂、标准物质数字化管理系统的总体原则、系统总体构架、系统技术要求、运维要求。

本文件适用于各类实验室、检验检测机构、计量校准机构、科研单位的数字化管理系统的新建、改造、部署、运维及验收评价。

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 15000.1 标准样品工作导则 第1部分：总则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 27025 检测和校准实验室能力的通用要求

GB/T 40343 智能实验室 信息管理系统 功能要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

试剂 reagent

实验室用于样品前处理、实验分析、检测校准、科学研究的各类化学试剂、生化试剂、缓冲溶液、实验溶剂、辅助实验耗材。

3.2

标准物质 reference material

具有均匀稳定特性、确定量值与不确定度，用于校准设备、评价测量方法、赋值样品、质量控制的物质与材料。

3.3

数字化管理系统 digital management system

依托计算机、物联网、大数据、条码/二维码识别技术，实现试剂、标准物质入库建档、领用审批、库存监控、有效期预警、使用记录、报废处置、溯源查询、数据统计的全生命周期数字化管理信息系统。

4 总体原则

4.1 合规性原则

系统建设与功能设计应符合GB/T 27025、GB/T 15000.1及《标准物质管理办法》的相关管控要求，适配实验室资质认定、计量溯源、内审外审等合规体系。系统管控流程、记录留存、风险防控机制应完全匹配实验室质量体系运行规则，杜绝管理漏洞与合规偏差。

4.2 全程溯源原则

系统应覆盖试剂、标准物质采购验收、入库建档、领用使用、储存保管、期间核查、剩余归还、报废处置全生命周期流程。所有物料操作环节应实现操作留痕、数据自动留存、过程可追溯、责任可定位，确保每一批次试剂、标准物质的使用链条完整、真实、可核查，保障实验数据与量值溯源的有效性。

4.3 安全可控原则

系统应建立分级权限管控、全程操作审计、风险预警防控机制，针对危化试剂、易制毒易制爆试剂、高等级有证标准物质应实行严格的分级审批、限额领用、专人管控制度。系统网络与数据安全应符合GB/T 22239等级保护要求，保障物料使用安全、数据存储安全、系统运行安全。

4.4 数据规范原则

系统应建立统一、唯一、标准化的物料编码体系与数据字段规范，统一试剂、标准物质的基础信息、批次信息、溯源信息、使用记录的数据口径。所有录入、采集、生成的数据应保证真实、准确、完整、不可篡改，满足实验室数据存档、统计分析、溯源核查的规范化要求。

4.5 实用高效原则

系统功能设计宜贴合实验室实际业务流程，简化人工操作流程，自动化实现有效期预警、库存预警、台账生成、数据统计、记录导出等功能，降低人工录入、人工统计的工作量，提升试剂与标准物质日常管理效率，适配实验室常态化、高频化管理需求。

5 系统总体架构

5.1 总体架构

系统应包含数据采集层、业务功能层、数据管理层、安全管控层。

5.2 数据采集层

5.2.1 采集方式

数据采集层应采用多模式融合采集机制，针对不同情况，使用不同的采集方式：

a) 智能识别：采集依托条码、二维码识别技术开展自动化采集，适用于带标准编码、溯源条码的商品化试剂、有证标准物质。

b) 人工辅助录入：适用于无标准编码的零散试剂、自行配制标准溶液、定制化实验耗材等无码物料，支持管理人员按照标准化字段规范手动录入物料信息。

5.2.2 采集内容

数据采集内容应包含试剂、标准物质的物料名称、规格型号、生产厂家、物料批次、溯源证书编号、有效期、储存条件、风险分类、物料等级、采购数量、入库时间、实时所在区域等信息。

5.3 业务功能层

5.3.1 基础档案管理

应实现所有试剂、标准物质电子化建档、档案修改、档案查询、档案导出全流程管理。

5.3.2 入库验收管理

应规范物料到货核验与入库包含操作人员的建档流程。

5.3.3 领用归还管理

应包含实验领用、临时借用、剩余物料归还及相关人员信息全流程管控。

5.3.4 库存与有效期管控

应实现物料库存动态监管与有效期风险前置防控。

5.3.5 期间核查管理

适配GB/T 27025实验室质量管控与标准物质质量值溯源要求。

5.3.6 报废处置管理

应规范过期、变质、失效、污染、破损及核查不合格物料的处置流程。

5.3.7 溯源台账统计

应满足实验室全链条溯源核查与合规台账管理需求。

5.4 数据管理层

数据管理层应建立统一的物料编码规则、数据字段规范、数据校验机制，对采集的原始数据进行清洗、归类、纠错、汇总。

5.5 安全管控层

5.5.1 账号安全

系统登录应启用身份核验机制，支持账号密码、动态验证码双重验证，宜支持绑定设备、IP白名单辅助管控，账号存在重大风险操作行为时，应将账号定为风险账号，并给相关人员发送信息通知与随机生成的操作码，操作码输入错误3次，将锁定账号。

5.5.2 数据安全

系统所有业务数据、物料档案数据、溯源记录、操作日志应实现加密存储，关键核心数据应禁止前台手动篡改、删除、清空。系统应建立自动化备份机制，每日完成全量数据自动备份，保障数据可恢复、不丢失。普通管理数据备份留存周期应不少于1 a，标准物质溯源、审计日志关键数据备份留存周期应不少于3 a。系统应具备数据恢复能力，可针对误操作、数据异常开展精准恢复。

6 系统技术要求

6.1 运行性能要求

系统整体运行性能应满足实验室常态化高频使用场景，保障稳定、高效、低延时运行，核心性能指标应符合以下规定：

- a) 系统全年可用率应 $\geq 99.5\%$ ，年度计划外宕机时长累计应不大于43.8 h；
- b) 常规页面访问响应时延应 ≤ 1.5 s，批量数据查询、台账导出响应时延应 ≤ 3 s；
- c) 表单数据提交、扫码入库、审批操作成功率应为100%，无数据丢包、重复提交、提交失败异常；
- d) 系统支持多用户并发操作，50位用户同时在线操作应无卡顿、无闪退、无数据冲突；
- e) 数据批量导入、批量更新正确率应为100%，保障批量运维操作可靠。

6.2 软硬件环境要求

6.2.1 软件环境

系统软件架构宜采用主流稳定的B/S架构，支持主流浏览器访问，无需客户端专属安装程序；系统后台服务、数据库、中间件应选用稳定商用或开源合规版本，具备长期技术支撑能力。系统可根据实验室需求适配私有化部署、本地服务器部署、云端部署三种模式，满足不同等级安全管控需求。

6.2.2 硬件环境

系统部署硬件应满足长期稳定运行要求，服务器、存储设备、网络设备应具备冗余容错能力；扫码采集终端、工控终端等外设应兼容系统识别协议，实现物料信息快速精准采集。

6.3 数据技术要求

6.3.1 数据唯一性

系统应建立全局唯一物料编码体系，实现一物一码、一批一码，编码规则应固定、可溯源、可解析，杜绝物料数据重复、错乱、匹配异常。

6.3.2 数据真实性与防篡改

系统所有操作产生的业务数据、日志数据、溯源数据应自动生成时间戳、操作人员身份标识、操作终端信息，历史数据应禁止手动删除、手动篡改、逆向修改，确保数据全程真实可溯。

6.3.3 数据存储与留存

系统数据存储周期应符合实验室资质认定与计量溯源存档要求，普通管理数据存储周期应不少于1 a，标准物质溯源数据、实验关联使用数据、关键操作审计日志存储周期应不少于3 a；系统应支持数据定期备份、异地备份，防止数据丢失。

6.3.4 数据完整性与准确率

系统物料档案数据、出入库数据、核查报废数据完整性应 $\geq 99\%$ ，数据准确率应 $\geq 99.5\%$ ，无关键字段缺失、数据错乱、数值异常问题。

6.4 权限管理要求

系统应遵循“最小权限、权责分离、分级授权”的原则，搭建精细化角色权限管控体系，预设系统管理员、审核管理员、普通操作员、只读查看员四类基础角色，各角色权限边界相互独立、严格隔离，系统支持自定义角色配置，可根据实验室岗位职责、业务分工增设专属权限角色，针对危化试剂、易制毒易制爆试剂、高等级有证标准物质等高危、高管控等级物料，系统应单独设置专项审批权限与领用权限，仅授权专人操作、专人管控，无对应权限人员无法发起领用、审批、处置等关键操作，所有账号新增、权限分配、权限调整、账号禁用、角色变更等权限操作，均需留存操作日志，支持溯源查询。

7 运维要求

7.1 日常运维要求

系统日常运维为每日常态化管控工作，运维人员应落实日常巡检、状态核查、问题处置、台账记录等基础工作，具体要求如下：

- a) 每日核查系统在线状态、服务运行状态、网络连通状态，确认系统无宕机、卡顿、访问异常，发现故障应及时处置并留存故障记录；
- b) 每日核查数据自动备份任务执行情况，确认全量数据、日志数据、溯源数据备份成功、无遗漏、无异常，对备份失败情况应立即补备份并排查原因；
- c) 每日监测用户登录、操作行为，排查异常登录、批量违规操作、越权访问等风险行为，及时开展风险处置与预警闭环；
- d) 每日清理系统无效缓存、冗余临时数据，保障系统运行流畅、访问响应速度达标；
- e) 对日常使用过程中发现的功能缺陷、数据异常、界面故障、设备适配问题应及时登记，建立问题台账，跟踪整改闭环。

7.2 周期运维

系统周期运维为周期性专项运维工作，应按月度、季度、年度分级落实，形成标准化、周期性运维机制，具体要求如下：

a) 月度运维：每月应开展一次全量数据完整性、准确性核验，核查物料台账、出入库记录、溯源日志、报废记录的完整性与一致性；每月应开展一次账号权限梳理，清理闲置账号、过期权限，修正不合理权限配置；

b) 季度运维：每季度应开展系统全面安全检测，包含漏洞扫描、病毒查杀、端口安全核查、接口安全校验；每季度应核查系统硬件设备运行状态、存储余量、外设适配情况，对老化、故障设备及时排查更换；每季度宜开展一次数据恢复模拟测试，验证备份数据可用性；

c) 年度运维：每年应开展系统整体性能评估，核查系统可用率、响应速度、并发承载能力等核心指标是否达标；每年应完成系统版本迭代优化、功能缺陷整改、安全策略升级；每年应整理全年运维台账、故障记录、整改记录，形成年度运维总结报告。
