ICS 01.140.20
CCS L 70

DB23

黑 龙 江 省 地 方 标 准

DB 23/T 3511—2023

智慧实验室信息化管理规范

2023－07－05 发布　　2023－08－04 实施

黑龙江省市场监督管理局　　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这些专利的责任。

本文件由中共黑龙江省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：黑龙江省网络空间研究中心、哈尔滨理工大学、黑龙江省林业设计研究院。

本文件主要起草人：方舟、宋雪、于斌、杨霄璇、曲家兴、白瑞、李锐、黄海、李晗、孟庆川、关志博、郑德承、孙腾、于洋、徐雪吟、孙迎港。

智慧实验室信息化管理规范

1 范围

本文件提供了智慧实验室信息化管理的总体要求、管理内容、监督和评估等方面的相关要求规范。

本文件适用于不同领域智慧实验室的信息化管理，可以作为智慧实验室信息化建设、管理的指导文件。

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 27427—2022 实验室仪器设备管理指南

GB/T 39555—2020 智能实验室 仪器设备 气候、环境试验设备的数据接口

GB/T 39556—2020 智能实验室 仪器设备 通信要求

GB/T 40024—2021 实验室仪器及设备 分类方法

GB/T 40343—2021 智能实验室 信息管理系统 功能要求

RB/T 028—2020 实验室信息管理系统规范管理

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧实验室 wisdom laboratory

通过现代信息技术手段，对传统实验室进行数字化改造，实现设备联网、数据共享、信息化管理、智能监控等功能的实验室。

3.2

实验室信息化管理 labor information management

指利用信息技术手段，对实验室资源进行数字化管理，并实现实验室设备自动化控制、数据采集、处理和分析等功能的管理活动。

3.3

实验室活动 laboratory activity

实验室中从事的检测、测试、校准、验证与后续检测、测试、校准、验证相关的抽样等活动的统称。

注：检测、校准有时也称为试验。

[来源：GB/T 40343—2021，3.2，有修改]

3.4

实验室信息管理系统 laboratory information management system

通过获取、分析、报告、存储等手段，对实验室活动数据进行管理的计算机系统。

注：本文件中用数据表示实验室内的所有结构化和非结构化数据和信息，而非仅指试验数据。

[来源：GB/T 40343—2021，3.3]

4 缩略语

下列缩略语适用于本文件。

LIMS： 实验室信息管理系统（Laboratory Information Management System）

IDS： 入侵检测系统（Intrusion Detection Systems）

IPS： 入侵防护系统（Intrusion Prevention System）

5 总体要求

智慧实验室信息化管理应当符合科学性、可靠性、安全性、公正性的原则。应对智慧实验室建设和实验室活动所产生的物联化、互联化、智能化的信息进行管理，其管理内容包括并不限于：

——组织管理，包括建立组织机构、流程和标准；

——LIMS；

——自动感知能力；

——信息收集分析能力；

——自动实现诉求能力；

——其他管理内容，包括智慧实验室设备管理、环境管理、人员管理、数据管理、网络管理、安全管理、信息安全管理、资源管理、知识产权管理等。

6 管理内容

6.1 组织管理

6.1.1 建立智慧实验室信息化管理的组织机构，由管理员、信息技术人员和安全保障人员等组成。其中，智慧实验室管理员负责制定信息化管理的方针、政策和标准；信息技术人员负责设计和实施信息系统，建立数据平台和开发应用程序；安全保障人员负责保障智慧实验室信息系统的安全性和稳定性。

6.1.2 制定智慧实验室信息化管理的流程和标准，标准应当符合国家和行业规范要求，包括数据安全、网络安全、电源稳定性、设备运行稳定性等。

6.2 LIMS

6.2.1 应针对整体工作和环境而进行开发设计 LIMS，用于收集、处理、记录、报告、存储或检索实验室活动数据和信息，LIMS 应具备提供数字化、自动化、智能化管理手段的能力，使智慧实验室能够更加智能化、自动化、数字化地运行。

6.2.2 应实现智慧实验室管理信息的共享和交流。

6.2.3 智慧实验室应保证 LIMS 的便携和适用，其功能一般包括但不限于：

a) 应确保 LIMS 实现从客户需求到出具数据、报告等技术过程和结果的电子化管理功能。

b) 应确保 LIMS 实现质量监控和评价过程及其结果的电子化管理功能。

c) 应确保 LIMS 实现资源和行政活动过程及其结果的电子化管理功能。

d) 应确保 LIMS 运行中所有过程数据和结果的查询分析、统计、报告功能。

6.3 自动感知能力

应按感知系统进行统一的功能管理，感知系统将实验室人员、设备、样件、环境等要素信息化，并能感知人员、设备、样件、环境等的状态，生成状态信息。例如：通过传感器测量环境信息，通过识别

器感知设备、样件及人员的状态等。

6.4 信息收集分析能力

应能够实现实验室系统自有数据的采集、存储和分析，并借助一定算法将数据转化为智慧实验室人员的心理、语言或行为诉求。例如具有自有大数据采集工具、内外部应用程序调用、外部大数据平台对接、海量多源异构数据挖掘、大数据处理等功能组件。

6.5 自动实现诉求能力

自动实现诉求能力应能够将代表实验室人员诉求的信息转变成控制信息，并通过控制系统自动实现实验室人员的诉求，进而逐步优化对人员、设备、样件、环境等要素的管理。例如：针对特定研究人员设定工作温度后，实验室系统可自动通过网络达成温度控制；实验人员运用多种方法进行某项实验，系统能够通过实验结果得出一定规律并自动给出实验参考方案。

6.6 其他管理内容

6.6.1 设备管理

6.6.1.1 应建立完善的智能设备管理系统，实现数字化档案管理。智慧实验室信息化管理的硬件设备主要包括计算机、服务器、传感器、通信设备、网络设备等，软件设备主要包括操作系统、数据库、应用程序、安全管理软件等内容。

6.6.1.2 应制定设备管理计划、维护机制，包括定期维护、检修、升级、自动备份配置信息等，确保设备的正常运行和延长设备寿命。

6.6.1.3 应具有联网状态下的设备状态信息监测与管理功能。

6.6.1.4 设备处置和报废。应及时处理已经失效或不能继续使用的设备，根据设备的品牌、型号、规格、年限、使用情况等因素进行评估，并制定相应的处置方案。在处理设备时，应符合相关法规和环保要求，确保对环境的影响达到最小化。

6.6.2 环境管理

6.6.2.1 智慧实验室环境应定期进行监测，采集的温度、湿度、气体浓度、光照强度等参数应定期记录，保证智慧实验室环境的适宜性和稳定性。

6.6.2.2 智慧实验室环境管理系统由传感器、控制器、网络通信等多个部分组成，其中传感器通过实时监测实验室内的各种参数，确保内部环境的稳定和安全。控制器则负责对传感器获取到的数据进行处理和分析，根据设定的程序和规则，对智慧实验室内的设备进行控制，从而达到优化环境的目的。网络通信模块负责把所有数据上传至服务器端，提供给管理人员进行远程监控和管理。

6.6.2.3 应注意对环境管理系统进行定期维护和检测，确保其正常运行，并及时更新升级系统软件，以适应新的应用场景和需求。

6.6.3 人员管理

6.6.3.1 对智慧实验室管理员、技术员等相关人员进行定期的信息技术培训，提高其信息化管理水平。

6.6.3.2 应建立健全的人员权限管理规程，根据智慧实验室需求和工作岗位，实现数字化赋权管理。

6.6.3.3 应建立问题预警和处理机制，管理员应当及时解决智慧实验室信息化管理中存在的问题。

6.6.3.4 应根据已经明确的各项工作的职责、权限和义务，例如人事档案管理、考勤管理、薪酬管理、职业发展规划等方面的信息，结合人才特长和能力，生成特定人员的自适配权限策略。

6.6.3.5　应制定使用人员的培训和学习计划，例如建立和保持使用人员培训程序，明确使用规程、安全事项、应急预案、新增功能等培训内容和培训效果评价细则，组织有效的培训并评价。

6.6.4　数据管理

6.6.4.1　数据的数字化管理。数据应分类存储、备份和管理，保证智慧实验室数据的完整性和安全性，数据的采集、处理、分析和共享应严格按照相关规定进行。

6.6.4.2　数据采集、存储和处理。应采用专门的数据管理系统进行存储和处理，定期进行数据管理系统的更新和维护，以确保数据的准确性和完整性。需建立统一的数据标准，制定统一的数据命名规则、存储格式、备份策略等，确保数据的一致性和可维护性。

6.6.4.3　数据平台应当能够有效地集成和处理智慧实验室的各种数据和信息，包括实验数据、设备状态数据、环境数据、工作流程数据等。

6.6.4.4　应对智慧实验室中的数据进行分类分级管理，设置不同层级的访问权限，保护重要数据的安全性和完整性。

6.6.4.5　应制定相应的数据共享政策和流程，保障数据共享的合法性和权益，建立数据共享平台，通过数据共享来提高智慧实验室的工作效率和科研成果转化率。

6.6.4.6　应遵循数据生命周期管理策略对数据进行创建、初始存储、删除等全周期管理操作。

6.6.5　网络管理

6.6.5.1　应具有完善的网络管理机制，覆盖智慧实验室内的物联网、互联网等无线/有线网络。

6.6.5.2　应具有完善的信息共享机制，包括共享平台、信息交流等，让相关人员及时了解智慧实验室信息化管理的最新动态。

6.6.5.3　应具有网络访问权限管理机制，管理员根据不同的职责和权限设置不同的账号和操作权限，以防止信息泄露和非法操作。

6.6.5.4　应建立网络应急响应机制。在发生信息安全事故或者网络发生异常情况时，可及时启动应急预案，进行快速响应和处理。

6.6.6　安全管理

6.6.6.1　应制定完善的安全管理制度，实现安全策略管理数字化。安全管理制度宜覆盖硬件安全、软件安全、数据安全、网络安全、信息安全、系统安全等保护措施。

6.6.6.2　加强安全监控和预警。利用物联网技术，对智慧实验室内的硬件、环境等进行全方位监控，及时发现并处理安全隐患，避免出现安全事故。同时，利用智能预警系统，对智慧实验室的安全风险进行预测和预警，为智慧实验室安全管理提供科学依据。

6.6.6.3　应加强保障软件安全的措施。服务器和信息系统终端应自动安装安全补丁，定期更新病毒库，设置应用程序白名单，防止未授权的访问和存储介质接入。

6.6.6.4　应建立完善的数据保护措施。采取多重措施来保护数据的安全。例如，数据的备份、加密、权限控制等都是常见的数据安全措施。同时，在数据的存储、传输和使用过程中，应采取数据加密、备份等措施，确保数据的安全性和可靠性。

6.6.6.5　网络安全的保护措施应覆盖物联网安全和互联网安全，包括但不限于物理隔离、搭建内部局域网、实施网络分段、设定网关过滤、强密码、加装防病毒软件/防火墙/IDS/IPS 等保护物联网、互联网安全的常见措施。

6.6.6.6　应建立完善的信息安全管理体系，确保信息安全策略与信息化管理的保密性、完整性、一致性原则相适应。宜对智慧实验室的系统资源进行实时监测，对智慧实验室内的工作人员进行信息安全教育培训，增强人员的信息安全意识和技能。

6.6.6.7　应建立系统安全策略清单，主要包括访问控制、身份认证、日志审计等安全策略集合。

6.6.7　资源管理

6.6.7.1　应建立资源清单。制定统一的资源清单和资产管理制度，及时更新和维护资源信息，保证资源的合理利用和维护。

6.6.7.2　应实现资源共享。可通过虚拟化技术、区域块链等方式实现资源共享，提高资源的共享率。

6.6.7.3　应提高资源利用效率。通过资源性能监控和优化，提高资源利用效率，降低智慧实验室的运营成本。

6.6.8　知识产权管理

6.6.8.1　应建立智慧实验室知识产权管理规范，可集成至 LIMS 界面统一管理。

6.6.8.2　应建立智慧实验室知识产权策略，对研发活动进行集中统一的监测管理，加强对知识产权的全过程保护。

6.6.8.3　应建立知识产权库。将智慧实验室的各类知识进行归纳总结，建立知识库，方便工作人员进行查阅和使用。

6.6.8.4　应推行知识产权共享。通过知识共享和交流，促进智慧实验室内部的合作和创新。

7　监督和评估

7.1　监督机制

7.1.1　监督机制的建立原则

7.1.1.1　合法性原则。监督机制必须符合相关法律法规的规定，不能违反法律法规的规定，不能侵犯个人隐私等合法权益。

7.1.1.2　公正性原则。监督机制必须公正、客观、无私心，不能存在偏颇或不公的现象，不能被特定群体或个人所控制。

7.1.1.3　适度原则。监督机制的力度应该适度，不能过分干涉智慧实验室的正常运转，也不能过于宽松，导致管理规范无法得到有效执行。

7.1.1.4　可操作性原则。监督机制必须具有可操作性，即在实践中能够被有效贯彻执行，以保证其有效性。

7.1.2　监督内容

7.1.2.1　确定监督对象。确定需要被监督的对象，明确监督的重点和范围。

7.1.2.2　选择监督方式。选择适合智慧实验室特点和要求的监督方式，比如设立专门的监督机构或者采用现有的监督机构。

7.1.2.3　制定监督周期。明确监督的周期和频率，建立相应的档案和记录，以便随时查阅。

7.1.2.4　落实监督措施。根据智慧实验室的具体情况，采取相应的监督措施，比如加强人员培训、技术检测、设备管理等。

7.1.2.5　反馈监督结果。对监督结果进行反馈，及时发现问题并加以解决，确保监督机制的有效性和智慧实验室管理的规范性。

7.1.3　监督机制的实施

7.1.3.1　加强智慧实验室信息化管理意识，提高管理水平和技术水平。

7.1.3.2　建立健全智慧实验室信息化管理制度，明确各项管理规范和要求。

7.1.3.3　采取科学、有效的监督措施，完善监督机制，确保管理规范的执行。

7.1.3.4　应具有完善的备案机制，对智慧实验室信息化管理的各项工作进行备案，以便监督和评估。

7.2　评估机制

7.2.1　评估内容

7.2.1.1　评估目标

智慧实验室信息化管理评估的主要目标是评估智慧实验室信息化建设的基础设施和管理制度的完备程度，衡量智慧实验室信息化管理现状与规范标准之间的差距，为智慧实验室信息化管理提供改进和优化建议。

7.2.1.2　基础设施评估

对智慧实验室信息化基础设施进行评估，包括硬件及软件设备、网络设施和安全环境等方面。评估要点包括：硬件及软件设备是否满足智慧实验室教学和科研需求；网络设施是否稳定、流畅、安全；智慧实验室安全环境是否达到标准等。

7.2.1.3　管理制度评估

对智慧实验室信息化管理制度进行评估，包括智慧实验室信息化管理制度是否规范、完备，是否能够满足日常管理需求；智慧实验室信息化管理人员是否专业、能力强，是否能够有效地运用信息技术手段进行管理等。

7.2.1.4　信息安全评估

对智慧实验室信息系统的安全性进行评估，包括数据和信息安全、网络和系统安全等方面。评估要点包括：数据和信息的保密性、完整性、可用性是否得到充分保障；网络与系统是否设置了合理的权限控制、加密防护等安全措施。

7.2.1.5　科研效果评估

对智慧实验室科研效果进行评估，包括智慧实验室使用情况、科研成果、开放共享程度等方面。评估要点包括：科研人员对智慧实验室信息化管理系统（平台）使用情况和满意度；科研成果质量是否达到预期目标等。

7.2.2　评估方法

7.2.2.1　评估标准

制定评估标准来评估智慧实验室信息化管理。包括智慧实验室的信息技术配置是否满足其业务需求、信息化管理系统是否有效、智慧实验室的信息化水平是否提高等方面。

7.2.2.2　问卷调查

通过问卷调查的方式获取科研人员对智慧实验室信息化建设的看法和建议，了解智慧实验室信息化管理现状和存在的问题。

7.2.2.3　实地考察

通过实地考察的方式对智慧实验室信息化基础设施、管理制度、信息安全等方面进行检查和评估，获得真实、全面的信息。

7.2.2.4　性能测试

通过对智慧实验室信息化硬件、软件设备进行性能测试，评估其稳定性、流畅性、安全性等方面。

7.2.2.5　专家评审

通过组织相关专家对智慧实验室的基础设施、管理制度、信息安全、科研效果等方面进行专业评估审查。

7.2.3 评估结果

7.2.3.1 应通过统一的信息发布评估结果。

7.2.3.2 应制定基于评估结果的改进和优化方案。

参考文献

[1] GB/Z 27429-2022 实验室科研数据不确定性评估指南

[2] DB34/T 4433-2023 检测实验室公正性风险评估技术规范

[3] 中华人民共和国网络安全法（中华人民共和国主席令第五十三号）

[4] 中华人民共和国数据安全法（中华人民共和国主席令第八十四号）