

《科学数据 数据存储安全管理要求》（征求意见稿）

编制说明

一、工作简况

（一）任务来源

本标准是 2019 年，国家重点研发计划“国家质量基础的共性技术研究与应用”重点专项“科学数据安全技术及基础技术标准研究”成果产出，中国科学院计算机网络信息中心向中国信息协会提出立项，协会于 2022 年 6 月 20 日正式下达立项计划，计划编号为：P2022-22。

本标准由中国信息协会提出并归口。

本标准由中国科学院计算机网络信息中心为牵头单位的起草小组组织起草。

（二）标准制订的目的

随着科学技术的发展，科学数据的产生和转化日益频繁，科学数据呈现爆发式增长，科学数据安全成为当前大数据时代的新课题。科学有效地进行新时代下的数据安全治理，确保数字经济的持续健康发展，是国家经济、社会发展的重要任务。2018 年 3 月，国务院办公厅印发《科学数据管理办法》，明确要求把确保数据安全放在首要位置。随着我国科学数据开放共享的力度不断加大，对科学数据安全的要求也在不断提升。

我国在科学数据全生命周期管理方面已有一定的实践基础。在科学数据安全标准方面，GB/T 35274-2017《大数据服务安全能力要求》、GB/T 37973-2019《信息安全技术 大数据安全管理指南》和 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》等对于科学数据全生命周期管理的数据安全管理作了规范，但其中涉及存储安全的管理要求不多。

科学数据存储安全是保障科学数据安全的基石，目前，我国相较国外存储安全实践发展起步晚，尚不存在基于科学数据特点的数据存储安全管理方面的标准。现有的国家和国际标准都不能够直接适用于科学数据存储安全的场景，科学数据存储安全方面的规范还是个空白，亟待补充和完善。通过制订团体标准《科学数据存储安全管理要求》，能够促进解决现阶段的存储安全问题，促进提升科学数据管理水平，具有现实意义。

本标准作为国家重点研发计划 NQI “科学数据安全技术及基础技术标准研究”（2019YFF0216200）的研究成果，从数据存储安全的实际问题和具有存储实践的机构的安全管理要求出发，结合现阶段科学数据存储特点和标准起草单位的存储安全实践经验，通过建立科学数据存储安全管理规范，规定科学数据存储的分类，细化数据存储活动，规范科学数据存储安全的管理要求，将在一定程度上解决现阶段关键的科学数据存储安全问题。

本标准的目的是为科学数据的存储安全管理提供指导，从安全管理制度、机房安全、网络安全、人员管理安全等方面提出通用安全要求，同时根据存储在介质上的时间和状态特点界定了临时存储、应用服务存储、长期归档三个典型阶段并分别提出存储安全要求。通过遵循本标准并采取有效措施，能够防止数据丢失、覆盖、篡改带来的损失，解决现阶段存储安全问题，提高数据安全保障能力，促进科学数据共享和

应用。

（三）主要工作过程

（1）项目启动及首次研讨会

2023年1月5日，由中国信息协会主办、北京蓝象标准咨询服务有限公司承办的《科学数据存储安全管理要求》等团体标准启动会暨首次研讨会在北京顺利召开。中国信息协会领导李红、中国标准化专家委专家（中国机械科学研究总院研究员）强毅出席会议并讲话，来自70余家企业、高校、科研院所120余名代表以线上线下的方式参加了会议，会议由北京蓝象标准咨询服务有限公司标准化工程师马建红主持。主编单位中国科学院计算机网络信息中心大数据技术与应用发展部副主任（国家基础学科公共科学数据中心主任）胡良霖代表标准编制组介绍标准草案和意见处理情况，各参编单位参与研讨。同时，强毅教授从标准化角度对标准进行了专业点评。主编单位代表对各参编单位代表所提建议和意见进行了详细的记录和解答。

会后，起草组针对启动会前和会上，各单位和专家提出的48条修改建议进行了处理，并对相应的标准文本进行修改，并于2023年2月20日将标准工作组讨论稿和意见处理表发送给相关单位，开始新一轮意见征集。

（2）第二次研讨会

2023年3月2日，《科学数据存储安全管理要求》团体标准第二次研讨会在北京以线上和线下结合的方式召开。会议主要围绕1月5日启动会以来各参编单位反馈的修改建议进行讨论，并特邀标准化专家对标准文本进行点评。来自50家企事业单位80余名代表参加了会议。会议由北京蓝象标准咨询服务有限公司首席技术官张德保主持。

中国科学院计算机网络信息中心工程师胡泊代表标准编制组，对标准的主要内容、前期工作情况、意见收集预处理情况等分别进行了介绍。随后，参会代表结合意见与处理情况，围绕标准的名称、技术框架、条款的陈述方式等方面展开了热烈的讨论。本轮意见征集共收到10条建议，经过起草组研讨，采纳8条建议，部分采纳1条建议，不采纳1条建议，结合意见处理情况并对标准文本进行修改，形成了标准征求意见稿。

（四）主要参加起草单位和工作组成员所做的工作

本标准起草工作组由中国科学院计算机网络信息中心为牵头单位组成。起草组承担了标准起草的组织、标准文本的编制、重点企业意见征求、标准编制说明的撰写和内审等工作。

二、标准编制原则和确定标准主要内容的依据

（一）确定标准主要技术指标的基本原则

本标准以《科学数据管理办法》为指导，以加强科学数据管理，保障科学数据存储安全，促进提升科学数据管理水平，提高科学数据开放共享水平为目标。

本标准的编制原则是：

（1）通用性；

本标准的编制为保障我国科学数据存储安全管理提供通用解决方案。提出通用要求的同时，根据科学数据的特点分别对临时存储、应用服务和长期归档存储阶段提出科学数据安全存储要求，适用各阶段、不同数据安全等级的科学数据，提供了通用存储安全解决方案。

(2) 实用性；

本标准根据我国国情、国家有关政策和实际使用场景制定，本标准可以填补我国在科学数据存储领域标准的空白。本标准推动政策法规的落地实施，满足开放共享切实需要；为我国科学数据管理机构提供科学数据全生存周期各个阶段的存储安全管理规范；为从事科学数据相关活动的各单位提供执行和参照依据，具有实用性；能够防止数据丢失、覆盖、篡改带来的损失，解决现阶段存储安全问题，提高数据安全保障能力。

(3) 符合性；

遵循国家现有数据安全法、等级保护等相关规定，符合国家有关法律法规和已编制标准规范的相关要求。

(二) 标准编写原则

本标准按照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。

(三) 主要依据

本标准在贯彻落实《科学数据管理办法》相关要求的基础上，通过研究分析相关国家标准和行业标准，提出本项目的研制思路。

《科学数据存储安全管理要求》团体标准拟参考引用以下相关标准：

- GB/T 9361—2011 计算机场地安全要求
- GB/T 18894—2016 电子文件归档与电子档案管理规范
- GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
- GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
- GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- DA/T 31—2017 纸质档案数字化规范
- DA/T 74—2019 电子档案存储用可录类蓝光光盘(BDGR) 技术要求和应用规范

本标准除了要与国家法律、法规和国家标准、行业标准相协调的基础上，还将与科学数据领域的标准规范体系相协调。本标准在现有标准体系中起核心基础支撑管理作用，具体属于信息安全下信息资源安全类目。

三、国外相关法律、法规和标准情况的说明

据 IDC 发布《数据时代 2025》的报告预测，全球数据总量到 2025 年将达到 175ZB，与数据同步增长的还有数据安全风险。在数字经济时代，各国对数据安全问题都高度重视。面对日益严峻的数据安全威胁，不少国家通过颁布政策法规、加强监管执法、提升安全治理技术能力等举措，全面强化数据安全保护。

欧盟发布《欧洲数据保护监管局战略计划（2020-2024）》，旨在从前瞻性、行动性和协调性三个方面继续加强数据安全保护，以保障个人隐私权。美国发布《联邦数据战略与 2020 年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。

阿联酋和新西兰分别出台《数据保护法》和《2020 年隐私法》，加强了对数据安全及个人隐私保护的规划建设；日本和新加坡分别完成了对本国《个人信息（数据）保护法》的修订，明确了个人数据权利及外部使用限制；加拿大出台的《数字宪章实施法案 2020》，提出了保护私营部门个人信息的现代化框架。欧盟发布《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》，为数据跨境流动中的数据保护问题提供了进一步指导；西班牙数据保护局发布《默认数据保护指南》，阐释了默认数据保护原则的策略、实施措施、记录和审计要求等，为企业实践数据保护原则提供具体指导。

为了应对日益复杂的信息环境和不断增长的信息安全需求，特别是存储安全需求，国际标准化（ISO）和国际电工委员会（IEC）制定了 ISO/IEC27040:2015 信息技术-安全技术-存储安全。该标准提供了详细的技术指南，以指导组织如何通过采用经过验证的一致方法来计划，降低数据存储安全性的计划，设计，文档编制和实施，以定义适当的风险缓解水平。

ISO/IEC27040:2015 界定并拓宽了存储安全性的边界，不仅仅包括存储方式、传输方式，浏览权限，还包括法律法规、人员管理、物资管理等，涵盖设备和介质的安全性、与设备和介质相关的管理活动的安全性、应用程序和服务的安全性，以及在设备和介质的使用寿命期间以及使用结束后与最终用户相关的安全性等各方面。

四、我国有关现行法律、法规和其他强制性标准的关系

近年来我国数据安全顶层制度设计加速推进。2015 年施行的《国家安全法》明确提出“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。2017 年施行的《网络安全法》将数据安全纳入网络安全范畴，网络安全等级保护制度、关键信息基础设施保护制度、个人信息保护制度等为保障数据安全提供重要制度支撑。2018 年国务院办公厅印发《科学数据管理办法》，明确要求把确保数据安全放在首要位置。2021 年 9 月 1 日施行的《中华人民共和国数据安全法》全面贯彻落实了总体国家安全观，再次规范了数据安全的全生命周期的合规性，督促各企业提升整体数据安全的保障力。至此，数据作为国家第五类生产要素、重要资产的地位日渐稳固。

同时，随着大数据、云存储技术等信息技术的快速发展和应用，国内主流互联网云厂商、第三方数据安全服务公司等都十分重视存储安全的管理和布局，不断研发存储安全技术，并取得相关存储安全认证资质，如百度智能云、中国电信天翼云、联通云数据有限公司等获得了 ISO 27040 认证。

在标准化方面，我国已发布关于云数据存储与管理方面的标准，但还缺乏针对存储安全管理方面的标准。

五、重大意见分歧的处理结果依据

本标准在标准起草过程中，对标准中的技术内容没有发生重大分歧。

六、数据验证

本标准起草组在研制期间到多个国家科学数据中心调研，基于国内外相关实际问题和存储实践经验丰富的机构的安全管理的要求，结合现阶段科学数据存储的特点，标准起草单位丰富的存储安全和科学数据管理实践经验，调研多项标准、论文和著作的存储安全现状及问题，借鉴机构管理要求，结合工作实践研制。

本标准由国家基础学科公共科学数据中心（简称“国家基础数据中心”）开展应用推广，在国家基础数据中心以及自建数据库得到数据验证。国家基础数据中心（是 20 个国家科学数据中心之一）以物理、化学、材料、动物、植物、病毒等学科领域和青海湖、黑龙江等典型区域为重点，建设完善的科学数据资源体系，汇聚包括科技项目数据在内的基础科学数据资源、强化数据产品加工和深度分析挖掘，服务国家重大项目和产业升级，充分发挥基础科学数据在我国双创战略实施中的基础支撑作用，提升我国基础科学数据资源的权威汇聚、长期保存、开放共享、分析挖掘、应用服务和驱动创新的整体能力和国际影响力，促进基础学科领域数据科学家为代表的复合型人才培养和数据科学的全面发展。

国家基础数据中心为保证数据通过平台实现可靠、稳定的对外共享服务，提供科学数据存储安全保障，参照本标准和 T/CIIA 017-2022《科学数据 安全标准体系》等系列标准规范成果，完善和修订国家基础数据中心及自建数据库的政策制度和标准规范，指导平台的建设和服务，为科学数据的共享和应用提供必要的保障。国家基础数据中心的技术规范与本标准规定的安全管理制度、机房安全、网络安全和人员管理安全等通用安全要求内容一致。国家基础数据中心的自建数据库在数据资源建设和应用服务过程方面，参考本标准各阶段存储安全要求进行数据资源管理和数据库规范化建设。

七、预期的社会经济效果

本标准可以用于指导科学数据存储安全建设和管理，保障科学数据存储安全，促进科学数据共享和应用。遵循本标准能够防止数据丢失、覆盖、篡改带来的损失，解决现阶段存储安全问题，提高数据安全保障能力。为解决科学数据管理和使用中的数据泄露、数据滥用、知识产权等问题提供支撑，增强科学数据的数据安全保障能力，促进提升科学数据管理水平。

八、贯彻标准的要求、措施建议及设立标准实施过渡期的理由；根据国家经济、技术政策需要和本标准涉及的技术改造难度等因素提出标准的实施日期的建议

建议本标准在审定、报批后尽快颁布，标委会及时组织宣贯和实施。因本标准首次制定，但执行起来难度不大，建议本标准发布即实施。

九、废止现行有关标准的建议

本标准为首次制定。