

T/JXEA

江西省工程师联合会团体标准

T/JXEA 356—2026

档案数字资源元数据长期保存与更新管理规范

Standard for long-term preservation and update management of metadata for archival
digital resources

（征求意见稿）

2026—XX—XX 发布

2026 - XX- XX 实施

江西省工程师联合会 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 总则	2
5 不同类型数字资源的元数据管理	2
5.1 公文文件的元数据要求	2
5.2 文献资料的元数据标准	2
5.3 影像档案的元数据管理	2
5.4 音视频档案的元数据规范	2
5.5 数据库档案的元数据组织	2
6 元数据的保存与封装	2
7 元数据的更新与维护	3
8 元数据的真实性保护与审计	3
9 风险管理与应急预案	4
附录 A（规范性） 档案数字资源元数据长期保存与更新管理规要求现场考核实施细则	5
附录 B（规范性） 档案数字资源元数据审计日志管理规范	7

前 言

本文件依据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***提出。

本文件由江西省工程师联合会归口。

本文件起草单位：。

本文件主要起草人：。

引 言

元数据作为档案数字资源的“灵魂”，是实现档案科学组织、有效管理和长期传承的核心支撑，直接关系到档案的真实性、完整性、可用性和安全性。随着档案数字化建设的深入，各类档案元数据类型日益丰富、规模持续扩大，元数据不规范、更新无序、保存失控等问题，严重影响档案数字资源的长期利用与价值发挥。为规范档案数字资源元数据管理流程，统一元数据保存、更新、保护的技术标准和要求，特制定本规范。

本规范适用于各类档案保管单位，涵盖全类型档案元数据，贯穿元数据生命周期全流程，为档案机构开展元数据管理工作提供科学指引，助力提升元数据管理规范化水平，保障档案数字资源的长期安全与高效利用。

档案数字资源元数据长期保存与更新管理规范

1 范围

本规范规定了档案数字资源元数据长期保存与更新管理的技术标准和要求，旨在保障档案真实性、完整性、可用性和安全性。适用于国家及地方各级档案馆、企业、高校、医疗及司法等各类档案保管单位。涵盖文本、电子文件、多媒体、结构化数据、工程及科研数据等全类型档案元数据。管理流程贯穿入库前审核、保存维护、利用更新及应急处置全过程。涉及国防、医疗、金融等特殊领域时，还需同步遵守行业保密及信息安全规范。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅该日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有修改单）适用于本文件。

GB 2312 信息交换用汉字编码字符集（基本集）

GB 7408 数据元和交换格式 信息交换 日期和时间表示法

GB/T 13989 国家基本比例尺地形图分幅和编号

GB/T 22080 信息安全管理要求

GB/T 34978 信息安全技术 移动智能终端个人信息保护技术要求

DA/T 1 档案工作基本术语

3 术语和定义

3.1

档案元数据 archival metadata

指档案机构为了对数字档案资源进行科学组织、有效管理和长期保存而创建或关联的结构化信息，包括描述性元数据、结构性元数据、保存性元数据和权限控制元数据。[来源：DA/T 1，3.1]

3.2

元数据规范化 metadata normalization

指按照国际或国家标准和行业规范，将档案元数据统一为规定的格式、结构和内容标准的过程，确保元数据的一致性、可交换性和互操作性。[来源：GB/T 22080，3.2]

3.3

元数据生命周期管理 metadata lifecycle management

指从元数据的初始生成、入库编目、持续维护、版本更新、格式迁移至最终保存销毁的全过程管理，涵盖元数据的创建、更新、使用、保护和审计等各环节[来源：GB 2312，3.3]。

3.4

元数据真实性保护 metadata authenticity protection

指采取技术手段确保档案元数据在创建、保存和使用过程中不被篡改、完整保存、来源可追溯的保护措施，包括数字签名、校验码验证、审计追踪等[来源：GB 7408，3.4]。

3.5

元数据版本管理 metadata version management

指对元数据的每次更改、升级或修订进行记录和管理，保留完整的版本演变历史，确保可随时追溯元数据的修改过程和原始状态[来源：GB/T 13989，3.5]。

3.6

元数据互操作性 metadata interoperability

指不同系统和平台之间通过规范化的元数据格式和交换机制，能够有效交互和共享档案信息的能力[来源：GB/T 34978，3.6]。

4 总则

档案机构在进行元数据管理时应遵循规范性、完整性、真实性、可持续性的综合原则。规范性原则要求元数据的生成、更新、存储应严格按照统一的标准和规范进行；完整性原则要求元数据应包含档案识别、保存和利用所需的所有必要信息；真实性原则要求元数据准确反映档案的实际状况，不得篡改或虚假记载；可持续性原则要求预测元数据格式和技术的长期生存周期，防止技术过时导致的信息丧失。档案机构应成立元数据管理专门小组，由档案业务人员、技术人员、安全管理人员等组成，定期（至少每年）评估本机构元数据的管理现状，制定改进计划。对于新增的数字资源，入库前必须进行元数据规范性审核，确保元数据完整规范。档案机构应建立元数据更新的标准操作流程，包括更新申请、审核批准、版本管理、质量验证三个关键环节。所有参与元数据管理工作的人员应每年接受不少于30小时的专业培训，内容包括元数据标准规范、更新管理工具、真实性保护技术等。

5 不同类型数字资源的元数据管理

5.1 公文文件的元数据要求

公文档案元数据应包含：文件标题、发布机构、发布日期、文件号、密级、保存期限、版本信息等描述性元数据；页面顺序、签署人、印鉴位置等结构性元数据；原始格式、转换历史、扫描参数、校验码等保存性元数据。对于具有法律效力的公文，应在元数据中记录数字签名信息和签署人身份。公文元数据应采用XML格式编码，符合GB 7408的日期时间规范。

5.2 文献资料的元数据标准

文献档案元数据应包含：书名、作者、出版社、出版日期、ISBN/ISSN、内容摘要、关键词等基本信息；页数、装订方式、色彩模式等物理特征；原始版本、扫描版本的文件格式和分辨率等参数；版权信息、使用限制等权限信息。对于特殊文献如手稿、古籍，应增加历史来源、装帧特征、保存状况等元数据。

5.3 影像档案的元数据管理

影像档案元数据应包含：拍摄对象、拍摄地点、拍摄时间、拍摄者等内容信息；色彩模式、分辨率、色彩空间、ICC配置文件等技术参数；扫描设备、扫描日期、扫描操作人员等采集信息；版本标记、修复记录等维护信息。应在元数据中详细记录色彩管理信息，确保长期色彩再现的一致性。

5.4 音视频档案的元数据规范

音视频档案元数据应包含：内容描述、制作者、制作日期、时长等基本信息；采样率、比特率、编码方式、帧率等技术参数；原始格式、转换历史、多版本信息；字幕、评论、附加轨道等关联信息。应在元数据中记录音视频的关键帧位置和内容大纲，方便快速检索和定位。

5.5 数据库档案的元数据组织

结构化数据档案元数据应包含：数据库名称、数据库类型、数据表清单等架构信息；字段定义、数据类型、约束条件等字段级元数据；数据量统计、更新频率、版本历史等维护信息；数据来源、数据质量评估结果、隐私保护措施等控制信息。应建立数据字典作为补充元数据，详细说明每个字段的含义和使用规范。

6 元数据的保存与封装

档案机构应采用标准化的元数据保存结构，将元数据、档案内容、技术文档、质量验证信息组织成逻辑关联的整体。元数据应采用XML或JSON格式存储，禁止使用专有格式。元数据文件应与

对应的档案文件存储在同一逻辑容器内，形成自描述的档案包。元数据应包含唯一的全局标识符（如UUID），确保每条元数据都能被唯一定位和追踪。

元数据最小集合应包括档案标题、创建日期、创建者、内容摘要、档案类型、保存级别、访问限制等描述性元数据；文件页序、层级关系、组织结构等结构性元数据；原始格式、转换历史、存储位置、校验码、数字签名等保存性元数据；访问控制信息、使用许可、隐私保护说明等权限元数据。对于重要档案，应在元数据中添加质量验证信息：扫描参数、转换工具版本、验证人员、验证时间等。元数据应与档案内容一起存储，而不应单独存放在档案管理系统中，以确保长期可迁移性。

7 元数据的更新与维护

档案元数据的更新应遵循严格规范的流程，确保每一次变更都有据可查、可控可溯。所有更新申请应当明确说明更新理由及所涉及的元数据字段，申请内容应具体、清晰，便于审核人员准确判断更新的必要性和合理性。更新申请应由授权的审核人员进行审查与批准，审核人员应当具备相应的专业知识和权限，对更新内容进行独立评估，确认其符合相关标准和规范要求。在获得批准后，应当在完整保留原始版本的基础上生成新的版本副本，确保原始数据不被覆盖或损毁。对新版本中的相关字段进行更新后，应开展全面检验，检验内容包括但不限于数据的完整性、格式规范性、与其他字段的逻辑一致性以及与档案内容的匹配程度。经检验合格后方可投入使用，投入使用前还应完成必要的系统同步和备份操作。更新操作的全部信息，包括申请单号、审核意见、操作人员、操作时间、更新前后内容对比等，均应详细记录并存档备查。

档案机构应建立元数据周期性维护计划，将元数据检验纳入日常管理范畴。对重要档案，每年应至少进行一次全面检验，核查元数据的完整性、准确性与一致性；对于一般档案，至少每两年进行一次维护。检验内容应包括必填字段是否完整、数据格式是否符合标准、内容是否与档案实际情况一致、各元数据项之间的逻辑关系是否合理等。检验过程中发现的任何错误或不一致情况，应及时记录、分析原因并予以纠正，必要时启动版本更新流程。检验记录和纠正结果应作为元数据管理档案的重要组成部分，长期保存。

每条元数据应包含完整的版本信息，包括版本号、版本创建时间、修改者及修改说明等。版本号应采用语义版本命名规则，如1.0、1.1、2.0等，以直观反映元数据的升级程度和变更性质。主版本号变更表示发生重大结构调整或内容重构，次版本号变更表示进行局部修正或补充。档案机构应当保留元数据的完整版本历史，严格禁止覆盖或删除旧版本，确保每一历史版本均可随时调阅。完整保留版本历史的做法，既便于追溯元数据的演变过程，也为后续的质量审计、真实性验证及争议处理提供了可靠依据。

8 元数据的真实性保护与审计

档案机构应当对所有重要元数据计算并保存密码学校验码，建议采用SHA-256或安全性更强的算法。校验码的生成应在元数据创建或更新时立即完成，确保从源头开始建立完整性保护机制。校验码应当与元数据分离存储，避免因同一存储介质的损坏或篡改而导致校验码同时失效。分离存储的方式可以包括不同物理设备、不同存储载体或不同管理系统。每次访问或使用元数据时，应当重新计算其校验码并与预先保存的校验码进行比对，以立即发现任何未经授权的篡改行为。对于校验码比对失败的情况，应当自动触发告警机制，暂停相关元数据的使用，并启动调查程序。对于具有法律效力的元数据，应当采用数字签名技术进行保护，由授权人员使用符合GB/T 22080国家标准的数字证书进行签署。数字签名应当覆盖元数据的核心字段，确保签名信息与元数据内容紧密绑定，任何对元数据的修改都将导致签名失效。

档案机构应当建立全面的元数据审计日志系统，记录所有对元数据的操作行为。审计日志的内容应至少包括操作人身份标识、操作时间（精确到毫秒并符合GB 7408标准）、操作类型（如创建、修改、删除、查询、导出、恢复等）、所涉及的元数据字段、修改前后的内容对比、操作结果（成功或失败）等关键信息。对于批量操作，还应当记录操作范围和数据量统计。审计日志本身也应当受到严格的完整性保护，防止被篡改或删除。审计日志应当与元数据分离存储，建议采用独立的管理系统或存储介质，并设置严格的访问权限控制。档案机构应当定期对审计日志进行审查，至少每月一次，重点检查存在异常操作模式、非授权访问尝试、批量修改等可疑行为。审查过程应当

形成书面记录，包括审查时间、审查人、发现问题、处理意见等。审计日志的保存期限应当与相应档案的保存期限相同，确保在档案全生命周期内均可追溯。对于涉及国家秘密或商业秘密的元数据，其审计日志应当采用加密存储方式，加密密钥应当与日志数据分离管理，并由专人负责保管。审计日志系统的运行状态应当持续监控，确保日志记录的连续性和完整性，任何日志记录中断或丢失都应当作为安全事件及时报告和处理。

9 风险管理与应急预案

档案机构应定期进行元数据风险评估，识别可能威胁元数据安全和完整性的各类风险，包括技术风险（硬件故障、软件缺陷、格式过时）、安全风险（数据泄露、篡改、丧失）、管理风险（流程不规范、人员操作不当）、自然灾害风险等。应制定详尽的风险预案和应急处置程序。

档案机构应采用多副本保存策略确保元数据安全。至少应保留三份独立副本：工作版本用于日常维护；归档版本保存在不同的物理介质上；备份版本保存在地理位置相距足够远的异地备份中心。应建立元数据的冗余编码机制，关键元数据应采用多种编码方案分别存储。档案机构应每年进行至少两次灾难恢复演练，验证备份的可用性和恢复流程的有效性。演练应包括全量恢复和部分恢复两种场景，演练过程应形成详尽的总结报告，发现的问题应及时整改。

附录 A

(规范性)

档案数字资源元数据长期保存与更新管理规范要求现场考核实施细则

A.1 考核环境要求

现场考核应在联合会考核工作委员会指定的考核场所进行。

- A.1.1 考试场所的建筑、安全、电力、照明、消防等设施须符合国家有关标准、规定。
- A.1.2 考核场所应具备应急安全疏散条件，具有由有关部门鉴定合格的安全区域和应急疏散通道。
- A.1.3 考试场所能与非考试场所分开，考试期间能够实行封闭管理。
- A.1.4 考核场所应具有专业工程能力考核所需的电脑、网络、显示设备、测试仪器等考试业务系统。

A.2 考核流程

- A.2.1 考核方案由联合会考核工作委员会事先审批通过，考官由考核工作委员会从考官专家库中选任。
- A.2.2 由考官现场核查申请人员的身份信息是否与报名信息相符，申请人员与考官一起签字确认。
- A.2.3 根据考核类别和级别，对同批次考核人员采用统一题、自动随机、现场抽题等多种考核模式。
- A.2.4 由考官分配考核位，申请人就位后，考官验证考核初始状态后，宣布考核开始并启动计时器。
- A.2.5 考核时间到，考官即时确认申请人已脱离对考核设备的操控，并确认考核记录保存正确。
- A.2.6 申请人离场，考官复核考试成绩，在评定单上签字确认。
- A.2.7 联合会根据考核评定单，以及申请人员的申请材料初审情况，公布考核结果。

A.3 评分规则

- A.3.1 现场考核每个项目的分数由考核方案规定，各个项目总分数应为100分。
- A.3.2 现场考核项目为实际操作或演示，每个项目均有明确评价指标，达成为满分，未达成为零分。
- A.3.3 现场考核项目均规定有时间限制，申请人超时后仍未脱离对考核设备的操控，视为零分。
- A.3.4 现场考核的项目可以采用图文答题方式，但此类项目的分数占比不能超过50%。
- A.3.5 现场考核的所有项目总评分超过80分以上（含80分），视为考核合格。
- A.3.6 原则上现场考核的每个项目只有零分和满分两个结果，但如果现场两位考官均同意给予特殊评分，则由现场两位考官和申请人一同写明原因并签字确认，封存所有现场记录，上报联合会的考核工作委员会复核，复核通过后评分成绩有效。

A.4 可复核性要求

- A.4.1 申请人不允许携带任何外接的存储介质、计算设备等进入考场。
- A.4.2 考前，考官应复核考核设备和系统，确保无连接外网、预存答案、特殊工具等情况，并签字确认。
- A.4.3 考核过程中，不允许申请人将考核设备与任何非指定设备进行数据交互。
- A.4.4 考核过程由现场数字摄像头、自动录屏软件等进行考场记录，该记录应保留半年。
- A.4.5 所有申请人现场编辑的工程代码、电路光路设计、美术工程等数字内容，均应保存2个月，必要时录制现场运行视频或拍照存证。

A.5 现场考核的争议处理

- A.5.1 考核场所应张贴考核工作委员会指定的考场纪律，并由考官现场宣读。
- A.5.2 违反考场纪律者，考官可即时终止其考核资格，并记录在考核评定单上。
- A.5.3 现场考核期间，因考场故障导致考核中断，考官可延长考核时间，并记录在考核评定单上。
- A.5.4 考核出现重大异常，考官可立即上报考核工作委员会备案，申请更换在线考核的日程、场所、试卷等，并将考核工作委员会的决定通知申请人。
- A.5.5 考核争议和处置，均以考核场所的录屏、录像、录音等获取的数据信息作为证据，考官的书面、口头申明为重要参考资料。
- A.5.6 考核工作委员会对所有的考核争议具有最终决定权。

A.6 成绩公布

- A.6.1 现场考核成绩应在联合会考核工作委员会指定的登录网址进行公布和查询。
- A.6.2 考核成绩，联合会根据现场考核评分数据汇总以及考核评定单进行成绩审核并公布。
- A.6.3 申请人对现场考核成绩有异议，可在成绩公布后15天内向联合会考核工作委员会提请复核，联合会考核工作委员会应在10个工作日内完成复核，并公布复核结论。

附录 B
(规范性)
档案数字资源元数据审计日志管理规范

B.1 目的与适用范围

本附录规定了档案数字资源元数据审计日志的记录、存储、保护和审查要求，旨在确保元数据操作的透明性、可追溯性和不可否认性，为元数据的真实性保护提供支撑。本附录适用于所有从事档案数字资源元数据管理的单位和人员。

B.2 审计日志的记录内容**B.2.1 基本记录项**

每次对元数据的操作均应记录以下基本信息：

操作标识：全局唯一的操作流水号

操作时间：精确到毫秒的时间戳（符合GB 7408）

操作人员：操作者的唯一标识（用户ID或数字证书DN）

操作类型：创建、修改、删除、查询、导出、恢复等

操作对象：被操作的元数据唯一标识符（UUID）

操作结果：成功、失败（含失败原因代码）

B.2.2 详细记录项

对于修改类操作，应额外记录：

修改前内容：被修改字段的原始值

修改后内容：被修改字段的新值

修改字段列表：本次操作涉及的所有元数据字段

修改理由：经审核批准的修改申请编号或理由说明

审核人：批准本次修改的审核人员标识

B.3 审计日志的存储要求**B.3.1 存储格式**

审计日志应采用结构化格式记录，推荐使用JSON或XML，并应符合以下要求：

每条日志记录独立成行或独立节点

日志文件应使用UTF-8编码

日志文件命名应包含起止时间范围

B.3.2 存储安全

审计日志应与元数据分离存储，不得存储在单一存储介质中

重要审计日志应计算校验码（SHA-256）并单独保存

涉及国家秘密或商业秘密的审计日志应加密存储

审计日志至少保存三份副本，其中至少一份为离线备份

B.3.3 保存期限

审计日志的保存期限应与对应元数据的保存期限相同。元数据销毁后，其审计日志还应继续保存不少于3年。

B.4 审计日志的保护措施**B.4.1 完整性保护**

采用哈希链技术，每条日志记录包含前一条日志记录的哈希值

每日生成日志文件的数字摘要并对外公布或可信存证

定期（每周）对审计日志进行完整性校验

B.4.2 防篡改措施

审计日志应采用“一次写入多次读取”的存储策略

日志文件生成后应设置为只读状态

关键日志记录应添加数字签名

B.4.3 访问控制

审计日志的访问权限应严格限制，仅授权审计人员可读

任何对审计日志的访问行为本身应被记录

禁止直接修改或删除已生成的审计日志

B.5 审计日志的审查

B.5.1 定期审查

每月对审计日志进行一次常规审查，检查异常操作模式
每季度进行一次深度分析，评估元数据操作的整体合规性
每年进行一次全面审计，形成年度审计报告

B.5.2 异常审查

出现以下情况时应立即启动异常审查：

检测到元数据校验码不匹配

发现未经授权的元数据访问尝试

收到关于元数据真实性的投诉或质疑

发生安全事件或数据泄露

B.5.3 审查记录

每次审查应形成审查记录，包括审查时间、审查人、审查范围、发现的问题、处理意见

审查记录应作为档案保存，保存期限不少于5年

B.6 附则

B.6.1 本附录由发布机构负责解释。

B.6.2 本附录自发布之日起施行。