

T/JXEA

江西省工程师联合会团体标准

T/JXEA 354—2026

档案数字资源长期保存与管理规范

Specification for long-term preservation and management of 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 总体要求	2
5 数字资源采集与整合	2
6 数字资源存储与备份	2
7 数字资源安全防护	2
8 数字资源迁移与格式转换	3
9 监督检查与持续改进	3
附 录 A（资料性）档案数字资源长期保存风险管理指南	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XXX提出。

本文件由XXX归口。

本文件起草单位：

本文件主要起草人：

引 言

档案数字资源是新时代档案事业发展的核心载体，承载着国家和社会的重要记忆，其真实性、完整性、可用性和安全性直接关系到档案价值的有效发挥。随着信息化建设深入推进，档案数字化进程加快，档案数字资源总量大幅增长，技术迭代频繁，长期保存与管理面临载体失效、格式兼容、安全风险等诸多挑战，亟需统一规范的技术标准和管理要求。为破解当前档案数字资源管理乱象，规范各级各类档案保管机构的保存管理行为，保障档案数字资源跨代际安全传承，特制定本文件。

本文件立足实际需求，整合相关标准规范，明确全流程管理要求，为档案数字资源长期保存与管理提供科学指引，助力档案事业高质量发展。

档案数字资源长期保存与管理规范

1 范围

本文件规定了档案数字资源长期保存与管理的总体要求，包括分级策略、管理要求、归档与移交接收、存储与保管、备份与恢复、转换与迁移、利用与共享、安全与保密、评价与改进等内容。

本文件适用于各级综合档案馆、专门档案馆、部门档案馆，以及机关、团体、企业事业单位和其他组织开展档案数字资源的长期保存与管理工作。其他类型的档案保管机构可参照使用。

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 18894 电子文件归档与电子档案管理规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 9361 计算机场地安全要求

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 20984 信息安全技术 信息安全风险评估方法

3 术语和定义

3.1

档案数字资源 digital archival resources

以数字形式存在的各类档案信息资源，包括电子档案及其元数据、档案目录数据、传统载体档案数字化成果等。

3.2

电子档案 electronic archives

机关、团体、企业事业单位和其他组织以及个人在履行法定职责或者处理事务过程中，通过计算机等电子设备形成、办理、传输、存储的，对国家和社会具有保存价值并归档保存的各种信息记录。

3.3

元数据 metadata

描述电子档案内容、结构、背景及其管理过程的数据。

3.4

长期保存 long-term preservation

采用技术措施和管理方法，确保档案数字资源在跨越技术代际的更替过程中持续保持真实性、完整性、可用性和安全性的活动。

3.5

备份 backup

为防止数据丢失，将档案数字资源复制或转换到其他非易失性存储载体或独立系统上的方式或过程。

3.6

在线备份 online backup

将备份数据存储在能被系统直接或自动访问的备份设备上的备份方式或过程。

3.7

离线备份 offline backup

将备份数据存储在脱离备份对象所在计算机网络系统，经人工安装才能访问的备份设备上的备份方式或过程

3.8

异地备份 off-site backup

将备份数据存储在地点的备份方式或过程

4 总体要求

档案数字资源长期保存与管理应遵循以下基本要求：合规性要求，即档案数字资源的采集、存储、管理、利用和销毁全过程须符合国家档案法律法规及本规范规定；真实完整性要求，即应采取技术与管理措施保证数字资源内容、结构与背景信息的真实性和完整性，防止未经授权修改、删除或损毁；安全可靠要求，即应按照GB/T 22239-2019的相关规定，对数字资源实施分级安全防护，保障存储环境、传输链路及访问权限的全面安全；持续可用性要求，即应定期检测存储介质状态，及时实施格式迁移与数据修复，确保资源在规定保存期限内始终处于可读、可访问状态；系统规范性要求，即应建立覆盖采集、整合、存储、备份、安全防护、迁移及监督各环节的系统化管理制度，明确各岗位职责与操作规程；全生命周期管理要求，即应对档案数字资源从形成或采集至最终处置的完整生命周期实施连续、可追溯的管理，建立完备的管理档案。

5 数字资源采集与整合

档案数字资源的采集应遵循完整性、准确性、及时性和规范性原则。采集范围应覆盖本单位职能活动形成的全部具有保存价值的数字文件，包括：业务系统中产生的结构化与非结构化数字文件；纸质档案及其他实物档案经数字化扫描或摄录形成的数字副本；外部接收的具有档案价值的电子文件及数据集合。采集前须制定采集方案，明确采集对象、格式要求、元数据著录规则、质量检验标准及交接程序。原生数字文件采集应在文件形成后规定时限内完成，采集格式应符合GB/T 18894-2016附录中规定的推荐格式清单；对于业务系统导出的数据，应同步采集完整的元数据，并对采集结果进行数据完整性验证，计算文件哈希值并记录在元数据中。数字化加工形成的数字资源，其分辨率、色彩模式、文件格式应满足档案数字化相关标准的规定，数字化成果移交前须经质量审核，审核内容包括图像质量、内容核对、元数据完整性及文件命名规范性。采集完成的数字资源应进行分类整合，按照预定的分类方案、档案全宗及类目层级进行组织，建立规范的目录结构，确保资源逻辑关联的完整性；整合过程中发现重复、错漏或格式不符的资源，须进行修正、补录或格式转换后方可入库。

6 数字资源存储与备份

存储系统建设应满足档案数字资源长期保存对容量、性能、可靠性和可扩展性的综合要求。存储架构应采用分级存储策略：在线存储层用于存放经常访问的活跃档案，采用磁盘阵列等高性能介质；近线存储层用于存放低频访问档案，采用低功耗磁盘或磁带库等介质；离线存储层用于灾难备份，宜采用磁带库或光盘库等离线介质，并保存于异地安全场所。存储环境须符合GB/T 9361-2011规定的机房环境要求，温湿度、防尘、防磁、防火、防水等条件应满足各类存储介质的长期保存需求。备份制度应遵循“3-2-1备份原则”，即至少保留3份数据副本，分布于2种不同类型的存储介质，其中至少1份存储于异地，异地距离应不少于50千米。备份频次应根据档案数字资源的重要程度分级设定：重要档案数字资源的在线备份频次不得低于每日一次，其他资源的备份频次不得低于每周一次；全量备份与增量备份应结合使用，备份恢复策略须经过验证测试，确保在规定时间内能够完成数据恢复。存储介质应定期进行健康状态检测，检测周期不超过12个月，检测内容包括物理损伤、读取错误率、剩余寿命预估等指标；对于接近使用寿命或出现错误率上升的介质，应立即启动数据迁移程序，将数据转移至状态良好的新介质。所有存储、备份及介质检测操作均须记录操作日志，日志内容包括操作时间、操作人员、操作对象、操作类型及结果，日志保存期限不短于资源保存期限。

7 数字资源安全防护

档案数字资源安全防护应依据GB/T 22239-2019的等级保护要求，结合档案资源的重要性与敏感性，实施与保护等级相匹配的安全控制措施。物理安全防护要求存储档案数字资源的数据中心或档案机房须按照GB/T 9361-2011的A类或B类机房标准建设，配置门禁控制、视频监控、防雷接地、消防报警及自动灭火等设施，非授权人员禁止进入核心存储区域。网络与系统安全防护要求档案信息系统须部署防火墙、入侵检测、漏洞扫描等网络安全设施；涉密档案的存储系统应与互联网实施物理隔离；系统漏洞补丁应在评估安全风险后及时安装，安装前须在测试环境验证；所有系统账户须实施最小权限原则，超级管理员账户须采用双因素身份认证。访问控制要求应建立基于角色的访问控制体系，根据人员职责设定相应的资源访问权限；档案数字资源的查阅、下载、修改、删除等操作须经过授权审批；所有访问操作应生成审计日志，日志须防篡改保存，保存期限不少于6个月。数据加密与完整性保护要求涉及国家秘密及敏感信息的档案数字资源，在存储和传输过程中须采用符合国家密码管理规定的加密算法进行加密保护；所有入库数字资源须生成哈希校验值（推荐采用SHA-256算法），并定期执行完整性校验，发现校验异常须立即启动应急响应程序。安全风险管理工作应按照GB/T 20984-2022的规定，定期开展档案信息系统安全风险评估，识别资产脆弱性、威胁及安全风险，制定针对性的风险处置方案。

8 数字资源迁移与格式转换

数字资源迁移是应对技术环境变化、维持资源长期可用性的重要手段，分为存储介质迁移和文件格式迁移两类。存储介质迁移应按计划主动实施，迁移时机的选择须综合考虑介质剩余寿命、技术淘汰趋势及读取设备可用性，原则上在介质寿命到期前2年启动迁移工作；迁移完成后须对迁移结果进行全面完整性校验，校验通过后方可注销旧介质，注销须记录并经档案管理负责人审批。文件格式迁移应优先选择国际通行的开放标准格式，文本类文档推荐迁移至PDF/A格式（符合GB/T 22239-2019对可信格式的要求），图像类推荐TIFF格式，音视频类推荐无损或低压缩编码的开放格式；格式迁移须确保内容、结构和元数据的完整传递，迁移前须进行小批量测试验证，迁移后须对随机抽取不少于5%的样本文件进行人工抽检，确认内容无损失；每次迁移操作须记录迁移日期、来源格式、目标格式、迁移工具名称与版本、操作人员、校验结果等信息，并将该记录附入资源元数据。对于无法自动转换或内容复杂的特殊格式文件，如CAD图纸、专有数据库文件等，应评估格式依赖风险，必要时同步保存原始格式文件及相关查看软件的完整安装包与授权信息。格式迁移不得修改档案内容，对于因格式特性导致部分排版样式发生变化的情况，须在元数据中予以记录说明。

9 监督检查与持续改进

档案行政管理部门及单位档案管理机构应建立针对数字资源长期保存与管理工作的定期监督检查制度，检查周期不超过12个月。监督检查的内容应涵盖：存储介质状态及备份有效性，格式迁移计划执行情况，安全防护措施落实情况，元数据著录完整性及规范性，人员培训与资质情况，管理制度建设及执行情况，以及系统运行日志与操作记录的完整性。监督检查可采用文件核查、系统抽测、实地查验等多种方式，对于发现的问题须出具书面整改通知，被检查单位应在规定时限内完成整改并反馈结果。单位应每年组织一次档案数字资源保存现状自评，自评内容参照本规范各章节要求逐项核查，形成自评报告，自评报告应纳入本单位档案管理工作年报。持续改进要求包括：依据监督检查结果、自评发现的问题及新技术发展情况，定期修订本单位数字档案管理规程，修订周期原则上不超过3年；应关注档案数字资源保存领域新技术进展，适时引入技术成熟、安全可靠的新型存储介质、新型校验技术及新型访问服务技术；应积极参加上级档案行政管理部门组织的数字档案管理人员业务培训，确保管理人员具备与岗位职责相匹配的专业能力，并通过演练方式定期验证灾难恢复预案的有效性，演练频次不少于每年一次，演练结果应记录存档并作为持续改进的依据。

附录 A (资料性)

档案数字资源长期保存风险管理指南

A.1 范围

本附录提供了档案数字资源长期保存过程中可能面临的风险识别、风险评估、风险应对及风险监控的指导，旨在帮助档案保管机构建立系统的风险管理机制，确保档案数字资源的持续安全。

A.2 风险识别

A.2.1 技术风险

硬件故障：存储设备（磁盘、磁带、光盘驱动器等）物理损坏或寿命终结。

软件过时：操作系统、数据库管理系统、应用软件版本升级导致不兼容。

格式淘汰：文件格式被主流软件放弃支持，无法正常解析。

数据损坏：存储介质老化、电磁干扰、病毒攻击导致数据比特级错误。

A.2.2 管理风险

制度缺失：未建立完善的长期保存管理制度或制度未有效执行。

人员变动：关键技术人员离职，知识传承中断。

操作失误：误删除、误覆盖、错误配置导致数据丢失。

备份失效：备份策略不当或备份载体损坏导致恢复失败。

A.2.3 环境风险

自然灾害：火灾、水灾、地震、雷击等损毁存储设施。

温湿度失控：空调故障导致温湿度超出存储载体允许范围。

电力故障：突然断电导致设备损坏或数据写错误。

物理安全：非法入侵、盗窃、破坏等。

A.2.4 安全风险

网络攻击：黑客入侵、勒索病毒加密数据。

数据泄露：未经授权的访问导致敏感信息外泄。

权限滥用：内部人员违规操作或窃取数据。

A.2.5 法律与合规风险

法规变化：新的法律法规对数据保存期限、隐私保护提出更高要求。

知识产权：使用的软件或格式涉及侵权风险。

证据效力：无法证明档案数字资源的真实性，导致法律凭证价值丧失。

A.3 风险评估

A.3.1 风险分析维度

发生概率：风险事件发生的可能性，分为高、中、低三档。

影响程度：风险事件对档案数字资源造成的损失，分为严重、中等、轻微三档。

风险等级：综合概率和影响，确定风险等级（一级、二级、三级），一级为最高风险。

A.4 风险应对

A.4.1 风险规避

采用成熟、稳定的技术和产品，避免使用实验性、小众软件。

选择开放标准、广泛支持的文件格式（如PDF/A、TIFF、JPEG2000等）。

建立严格的权限管理和操作审计机制，减少人为失误。

A.4.2 风险减轻

实施多套备份（在线、离线、异地、异质），降低单点故障影响。

定期开展四性检测，及时发现数据损坏并恢复。

部署防火墙、入侵检测、防病毒系统，增强网络安全。

配备UPS、精密空调、自动灭火系统，保障环境安全。

A.4.3 风险转移

购买数据安全保险，转移部分经济损失。

将部分非核心数据托管至可信的第三方专业机构。

A.4.4 风险接受

II 对于发生概率极低、影响轻微的风险，可接受并持续监控。

制定应急预案，确保风险发生时能快速响应。

A.5 风险监控

A.5.1 监控措施

建立风险清单，定期更新风险状态。

持续监测存储设备健康状态（如SMART信息、磁带错误率）。

跟踪技术发展动态，关注文件格式、软件版本的生命周期。

定期组织内部审计和应急演练，检验风险应对措施的有效性。

A.5.2 风险报告

每年编制风险管理报告，向管理层汇报主要风险及应对情况。

发生重大风险事件时，立即启动应急预案，并及时向上级主管部门报告。

A.6 风险管理文档

风险管理应形成并保持以下文档：

- a) 风险清单（含风险类别、事件、概率、影响、等级、责任人）。
 - b) 风险应对计划（含具体措施、实施时间、预期效果）。
 - c) 风险监控记录（含监控时间、监控内容、发现的问题、处理结果）。
 - d) 应急预案（含响应流程、联系人、资源清单）。
 - e) 应急演练记录（含演练时间、参与人员、演练过程、改进建议）。
-