《电子档案长期保存与异地备份管理指引》

编制说明

《电子档案长期保存与异地备份管理指引》编制组

2026 年 2 月

《电子档案长期保存与异地备份管理指引》编制说明

1.任务来源

《电子档案长期保存与异地备份管理指引》的任务来源是由中国智慧工程研究会批准立项，由郴州市第一人民医院、淄博市卫生健康事业发展中心、惠州市博罗县华侨中学、山东省淄博市粮食和物资储备保障中心、北京汉龙致远科技有限公司、天津城市建设管理职业技术学院、无锡市建设工程管理服务中心（无锡市城市建设档案馆）、肇庆市水产技术推广中心、黑龙江省科学院、黑龙江省哈尔滨市方正县殡仪馆等单位起草编制。

2.目的意义

本文件的制定旨在适应数字化背景下电子档案数量快速增长、类型日益多样以及利用频率不断提高的发展趋势，针对电子档案在长期保存过程中面临的载体老化、格式失效、系统更迭、数据损毁以及单点故障风险突出等问题，建立系统、规范、可持续的电子档案长期保存与异地备份管理指引。电子档案作为组织运行、业务管理和历史记忆的重要信息资产，其真实性、完整性、可用性和安全性直接关系到管理决策、权益维护与社会责任履行。本文件通过明确电子档案长期保存技术路径、管理要求和异地备份策略，引导档案管理单位由以存储为核心向以风险防控和持续可用为核心转变，为各类组织开展电子档案安全保存和可靠利用提供统一、可操作的技术与管理依据。

3.编制思路和原则

3.1.编制思路

本文件在编制思路上坚持以电子档案全生命周期管理为主线，围绕电子档案形成、归档、保存、迁移、备份与恢复等关键环节，构建“制度保障与技术支撑并重”的管理框架。内容组织强调从源头控制入手，明确归档数据质量、元数据完整性和格式规范性要求，在此基础上对长期保存环境建设、存储介质管理、格式管理与迁移策略、完整性校验与版本控制、访问利用与权限管理等内容进行系

统梳理。同时，将异地备份作为电子档案安全保障体系的重要组成部分，重点规范备份架构设计、备份频率与方式、数据同步与一致性校验、恢复演练与应急处置流程，使长期保存与异地备份相互支撑、协同运行，避免仅重视“备而不用”或“存而不管”的管理偏差。

3.2.编制原则

本文件的编制遵循安全性与可靠性优先原则，强调通过多副本保存、介质与环境监控、完整性校验和定期恢复验证等措施，降低电子档案在长期保存过程中发生不可逆损毁的风险；遵循真实性与可追溯性原则，要求电子档案在保存和迁移过程中保持内容、结构与上下文信息不被破坏，相关操作留痕可审计，确保档案法律凭证属性；遵循规范性与可实施性原则，将管理要求转化为明确的流程、责任和技术措施，便于不同规模和类型单位结合实际条件执行；遵循统筹性与经济性原则，在保障安全的前提下，合理配置本地保存与异地备份资源，避免重复建设和资源浪费；同时遵循可持续发展原则，充分考虑信息技术演进和业务变化对电子档案保存方式的影响，为制度更新和技术升级预留空间。

4.编制过程

本标准修订讨论会均采用线上征集专家意见的形式，线上会议共计 2 次，会议期间广泛听取专家意见，并形成意见汇总表。

5.内容修订说明

本次修订主要围绕增强电子档案长期保存体系的稳定性与异地备份管理的实效性进行了完善。修订中进一步明确了电子档案长期保存与异地备份的职责分工和管理边界，强化了数据质量控制、元数据管理和格式迁移要求，提升长期保存体系对技术变化的适应能力；对异地备份的架构模式、数据同步策略和恢复验证要求进行了细化，强调备份数据可用性验证和定期演练，避免备份流于形式；同时，对安全管理与风险防控内容进行了补充完善，加强了对权限控制、日志审计、介质管理和突发事件应对的要求，使电子档案长期保存与异地备份管理由“被动防护”向“主动保障”转变，进一步提升本文件在实际档案管理工作中的指导性和可执行性。

ICS 01.140.20
CCS A 14

T/WEA

团　　体　　标　　准

T/WEA XXXX—2026

电子档案长期保存与异地备份管理指引

Guideline for management of long-term preservation and off-site backup of electronic archives

（征求意见稿）

2026－XX－XX 发布　　2026－XX－XX 实施

中国智慧工程研究会　　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专利的责任。

本文件由中国智慧工程研究会提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

随着信息技术的广泛应用，电子文件已成为各类组织业务活动和管理过程中的主要信息载体，电子档案数量持续增长，类型日益多样。与传统纸质档案相比，电子档案在形成方式、存储介质、利用方式和保存环境等方面具有显著差异，其长期保存面临的技术风险、管理风险和安全风险更加复杂。如何在确保真实性、完整性、可用性和安全性的前提下，实现电子档案的长期可靠保存，已成为档案管理工作中的重要课题。

电子档案长期保存过程中，受制于软硬件环境快速演进、存储介质老化、文件格式淘汰、系统平台升级以及人为操作等多种因素，若缺乏系统化管理措施，易出现数据损坏、内容不可读、关联关系丢失或证据效力削弱等问题。同时，单一存储环境在面对自然灾害、设备故障、网络攻击和突发事件时，难以有效保障电子档案的持续可用性，建立异地备份与容灾机制已成为提升档案安全保障能力的重要手段。

近年来，国家和行业层面不断强化对电子档案管理、数据安全和信息化治理的要求，推动电子档案从“可存储”向“可长期保存、可依法利用、可安全恢复”转变。在实际工作中，不同单位在电子档案长期保存策略、备份架构、管理流程、技术手段和责任分工等方面差异较大，部分单位仍存在备份策略不清晰、异地备份形式化、恢复验证不足、管理职责不明确等问题，制约了电子档案管理水平的整体提升。

在此背景下，有必要对电子档案长期保存与异地备份管理活动进行系统规范，明确保存对象、保存要求、备份策略、技术路径、管理流程及安全控制要点，形成可操作、可检查、可持续改进的管理指引。本文件在总结电子档案管理实践经验的基础上，结合信息技术发展现状，从管理与技术相结合的角度，对电子档案长期保存与异地备份的实施要求作出规定，旨在为各类组织开展相关工作提供统一参考依据，提升电子档案安全保障能力和长期利用价值。

电子档案长期保存与异地备份管理指引

1 范围

本文件规定了电子档案长期保存与异地备份管理的总体原则、保存对象与长期保存要求、异地备份策略与实施要求、备份与恢复管理流程、安全控制与审计及运行维护与检查评价等内容。

本文件适用于各类组织对电子档案开展长期保存管理及异地备份建设、运行与持续改进活动。

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 29194—2012 电子文件管理系统通用功能要求

GB/T 35273 信息安全技术　个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子档案 electronic records

由计算机等电子设备形成、办理、传输和存储，具有凭证、查考和保存价值并归档保存的信息记录及其相关元数据。

3.2

长期保存 long-term preservation

为确保电子档案在规定保存期限内持续保持真实性、完整性、可用性和安全性而采取的管理与技术措施的集合。

3.3

异地备份 off-site backup

将电子档案数据及其必要的元数据、配置与校验信息复制并存放在不同地理位置的备份介质或系统中，以降低单点故障与区域性灾害风险的备份方式。

3.4

备份策略 backup strategy

针对备份对象、备份频率、备份方式、备份保留周期、备份介质与存放位置、恢复目标等作出的规则与安排。

3.5

恢复验证 restore verification

对备份数据进行恢复演练或抽样恢复检查，以验证备份数据可恢复、可读取、可用且满足完整性与一致性要求的活动。

3.6

完整性校验 integrity verification

通过校验码、哈希值或等效技术手段，对电子档案数据在存储、传输、备份与恢复过程中的一致性和未被非授权篡改的特性进行验证的过程。

3.7

保存格式 preservation format

用于长期保存的文件格式或封装格式，具有规范公开、可长期解析、兼容性较强等特征，并与相应元数据共同支持长期可用。

4 总体原则

4.1 合规与职责明确原则

电子档案长期保存与异地备份管理应符合国家有关档案管理、数据安全与网络安全等要求，应明确归口管理部门、系统运维部门及业务部门的职责分工，形成覆盖归档、保存、备份、恢复、审计与改进的责任体系。关键岗位职责应可追溯，关键操作应留痕。

4.2 真实性与完整性保障原则

长期保存应以维护电子档案真实性与完整性为核心，应建立从形成归档到保存利用全过程的控制链条，应通过元数据管理、版本控制、完整性校验、操作审计与权限控制等手段，确保电子档案内容、结构和关联关系不被非授权更改，且变更过程可追溯。

4.3 可用性与可读性持续原则

长期保存应保证电子档案在保存期限内可检索、可读取、可理解和可利用，应关注软硬件环境演进与文件格式淘汰风险，应建立格式管理、迁移转换、兼容性验证与必要的技术文档留存机制，避免“数据在但不可用”。

4.4 风险分散与业务连续原则

异地备份应以风险分散为导向，应降低单点故障、区域性灾害、恶意攻击与人为误操作对电子档案安全的影响。备份体系应与业务连续性要求相衔接，应明确恢复目标与恢复流程，并通过定期恢复验证保证可恢复。

4.5 分级分类与最小授权原则

电子档案应实施分级分类管理，应根据档案敏感程度、重要程度与保密要求配置差异化的存储保护、访问控制、备份频率与留存策略。权限管理应执行最小授权原则，敏感档案访问与导出应实行审批控制并形成审计记录。

4.6 标准化与可审计原则

长期保存与备份管理应建立标准化流程、标准化数据要素与标准化操作规程，应形成可检查、可审计的记录证据。备份策略、校验规则、恢复演练与异常处置等应制度化，相关记录应纳入档案或运维记录管理范围并按规定保存。

4.7 持续改进原则

应定期评估长期保存与异地备份体系的有效性，应根据风险变化、技术演进、业务需求与审计发现持续优化保存策略、备份策略与控制措施，形成闭环改进机制。

5 保存对象与长期保存要求

5.1 保存对象范围

长期保存对象应包括电子档案内容数据及其必要的元数据、关联数据与支撑数据。保存对象至少应覆盖：归档电子文件、电子案卷/目录数据、元数据、权限与访问控制相关信息、校验信息、格式与版本信息、必要的系统配置与解析说明等。

对具有法律凭证价值或重要业务支撑价值的电子档案，应明确其长期保存范围与保存责任边界，并应纳入重点保护对象。

5.2 长期保存基本要求

电子档案长期保存应满足真实性、完整性、可用性与安全性要求。

电子档案应保持内容不被非授权修改；确需更正、补充或转换的，应保留原件或原始版本，并应记录变更原因、变更人、时间、方法与影响范围。

电子档案应保持结构与关联关系完整，应确保文件与元数据、目录、案卷关系、附件关系、版本关系等可正确关联与还原。

电子档案应具备持续可读性，应建立保存格式管理与迁移机制，对可能出现解析风险的格式应提前评估并采取转换或封装措施。

电子档案应具备可追溯性，应对归档、入库、校验、备份、恢复、迁移、利用与导出等关键操作进行审计记录。

5.3 保存要素要求

长期保存应至少保存以下要素：

a）内容数据：文件本体及其附件、图像/音视频等相关对象；

b）元数据：形成者、形成时间、业务来源、版本信息、保管期限、密级/敏感级别、关联关系、校验信息等；

c）证据链要素：签章/签名信息（如适用）、审批流记录、操作日志摘要或引用信息；

d）技术要素：文件格式标识、编码信息、必要的解析说明与渲染依赖信息（如适用）。

5.4 保存格式与迁移要求

应建立保存格式管理机制，应识别“长期可解析”的保存格式或封装格式，并规定优先使用的保存格式清单与转换规则。

对不利于长期解析或存在淘汰风险的格式，应进行风险评估并制定迁移计划；迁移应保持内容语义不变或可解释，迁移前后应进行一致性校验与抽样核验，并保留迁移记录。

迁移过程中生成的新版本应具备版本关系标识，并应保留迁移工具、参数与校验结果等证据。

5.5 电子档案保存

电子档案长期保存对象及其关键保存要素宜形成清单管理，示例见表1。

表1 电子档案长期保存对象与保存要素

保存对象	关键保存要素	主要控制要求
档案内容数据（文件本体及附件）	文件标识、格式、大小、生成时间、校验码	入库前完整性校验、保存版本可追溯、访问与导出受控
元数据与目录数据	形成信息、业务来源、保管期限、分类号、关联关系	元数据项完整、目录与案卷关系一致、变更留痕
校验信息	哈希值/校验码、校验算法、校验时间	定期复核、校验失败触发告警与处置
权限与访问控制信息	角色、授权范围、审批记录	最小授权、敏感访问需审批、权限变更审计
证据链信息（如签章/流程记录）	签章信息、审批流、操作日志摘要	不可抵赖、关键操作全程留痕、与档案对象关联
格式与解析支撑信息	格式版本、编码、渲染依赖、转换工具记录	建立格式清单、迁移记录完整、可重现或可解释

6 异地备份策略与实施要求

6.1 总体要求

异地备份应覆盖电子档案长期保存所必需的数据对象，应与长期保存要求一致，确保备份数据可恢复、可读取、可用且可追溯。

异地备份策略应根据档案重要程度、敏感程度、业务连续性要求与风险评估结果确定，并应形成制度化文件；策略调整应执行变更控制并留存记录。

6.2 备份范围与备份对象

异地备份范围至少应包括：电子档案内容数据、元数据与目录数据、校验信息、必要的配置数据与系统支撑数据；采用电子档案管理系统的，宜同时备份关键配置、索引与日志等支撑信息，以保障恢复后可检索与可追溯。

对重要档案、关键业务档案或具有凭证价值的档案，宜提高备份频率并实施更严格的完整性校验与恢复验证；对涉密或受限档案，应在合规前提下实施异地备份，并采取加密、隔离与访问审批等强化措施。

6.3 备份方式与存放要求

异地备份方式可采用在线复制、周期性增量备份、周期性全量备份或其组合。备份体系宜采用“本地多副本+异地副本”的分层保护模式，并应避免单一介质或单一站点风险。

异地备份存放地点应与主存储地点保持有效的地理隔离，且应满足环境、安防与运维管理要求。异地备份介质或存储系统应采取访问控制措施，防止未授权访问、删除或篡改。

异地备份数据的传输应采取保护措施，涉及敏感数据的传输宜采用加密通道；备份数据存储宜采用加密或等效保护措施，并应对密钥管理作出规定。

6.4 备份保留与版本管理

应规定备份保留周期与副本数量，应满足业务追溯、审计与灾后恢复需求。备份保留应结合“全量+增量/差异”的组合策略，避免保留策略不当导致恢复点不足或存储资源浪费。

备份应支持版本管理，应标识备份时间、备份范围、备份类型与备份版本；对跨周期保留的备份，应确保索引与校验信息可用于快速定位与一致性验证。

6.5 完整性校验与一致性控制

备份前、备份后及恢复后应实施完整性校验或等效验证措施。校验宜采用哈希校验等方法，并应记录校验算法、校验时间、校验对象与校验结果。

当校验失败或发现不一致时，应启动异常处置流程，查明原因并采取补救措施；必要时应重新备份并对受影响范围进行核查。

异地备份应与主存储保持一致性控制，避免出现“目录可查但文件缺失”“文件存在但元数据丢失”等不一致情形。

6.6 异地备份策略配置要点

异地备份策略的关键参数宜形成统一配置要点，示例见表2。

表2 异地备份策略配置要点

配置项	说明	建议控制要点
备份对象范围	内容数据、元数据、校验信息、配置与索引等	对象边界明确；支撑数据纳入； 避免仅备文件不备元数据
备份频率	全量/增量/实时复制的周期设置	重要档案提高频率；结合业务峰谷安排； 明确“最迟可接受备份点”
保留周期与副本数	备份保留时间、历史版本数量	满足审计与追溯；与存储容量匹配； 防止过短导致无法回溯
存放位置与隔离	异地站点、介质类型、逻辑/物理隔离	地理隔离有效；权限隔离； 防止同城同机房“伪异地”
传输与存储保护	通道加密、数据加密、密钥管理	敏感数据强制加密；密钥分级管理；访问可审计
校验与告警	校验方法、校验频次、告警规则	备份后自动校验；失败告警；形成处置闭环
恢复目标	恢复时间目标、恢复点目标	与业务连续性匹配；定期复核并更新
恢复验证频次	演练周期、抽检比例、验证方法	定期演练+抽样恢复；验证可读可检索可追溯

7 备份与恢复管理流程

7.1 一般要求

备份与恢复管理应形成闭环流程，应明确备份触发机制、备份执行要求、完整性校验、备份入库与保留、恢复申请与审批、恢复实施、恢复后验证、异常处置与记录归档等环节要求。

备份与恢复过程应全程留痕，应确保备份任务可追溯、恢复操作可审计、恢复结果可验证；对关键档案或敏感档案的恢复与导出应实施审批控制。

7.2 备份执行与记录

备份应按既定策略自动或半自动执行，确需人工触发的，应记录触发原因与责任人。

每次备份应形成备份记录，记录至少应包含备份时间、备份类型（全量/增量/差异/复制）、备份范围、备份对象数量与容量、目标站点、执行结果、异常信息及处置情况。

备份执行应避免影响电子档案系统的正常业务运行，必要时应采用分时段、分批次或限流策略。

7.3 校验、入库与保留

备份完成后应进行完整性校验或等效验证，校验应覆盖关键对象，至少应覆盖备份包索引、目录/元数据与文件本体的关联一致性。

校验通过后方可入库并纳入保留管理；校验不通过的备份不应作为有效恢复源，应启动异常处置流程。

备份入库应支持快速定位与检索，至少应支持按时间、范围、备份类型与版本号检索；备份保留到期处置应执行审批并留存记录。

7.4 恢复申请、审批与实施

恢复应建立申请与审批机制，应明确恢复原因、恢复范围、恢复点、目标环境与责任人。对敏感档案恢复、批量恢复或跨环境恢复，应执行更严格审批与风险评估。

恢复实施应遵循既定恢复流程，应在恢复前确认恢复源有效、校验信息齐全；恢复过程中应记录关键操作、参数与异常信息。

恢复完成后应进行恢复后验证，验证至少应包括：文件可读取、元数据可检索、关联关系可还原、关键校验一致性通过；必要时应进行抽样业务复核。

7.5 恢复验证与演练

应定期开展恢复验证或演练，演练应覆盖典型档案类型、关键业务档案与关键系统支撑数据。

恢复验证宜形成计划并留存记录，记录至少应包含演练范围、演练步骤、验证方法、验证结果、问题清单与整改措施。

恢复验证未通过或发现恢复链条存在缺陷的，应及时整改并复验，重大问题未闭环前不应降低备份频率或缩短保留周期。

7.6 异常处置与报告

发生备份失败、校验失败、备份数据损坏、恢复失败或疑似被篡改等情形时，应启动异常处置流程，及时隔离风险并开展原因分析。

异常处置应形成报告，报告应至少包含事件描述、影响范围、原因分析、处置过程、恢复措施、整改措施及防范建议；对重大事件应纳入安全事件或运维事件管理并进行复盘。

7.7 备份与恢复流程示意

备份与恢复管理流程示意如图1所示。

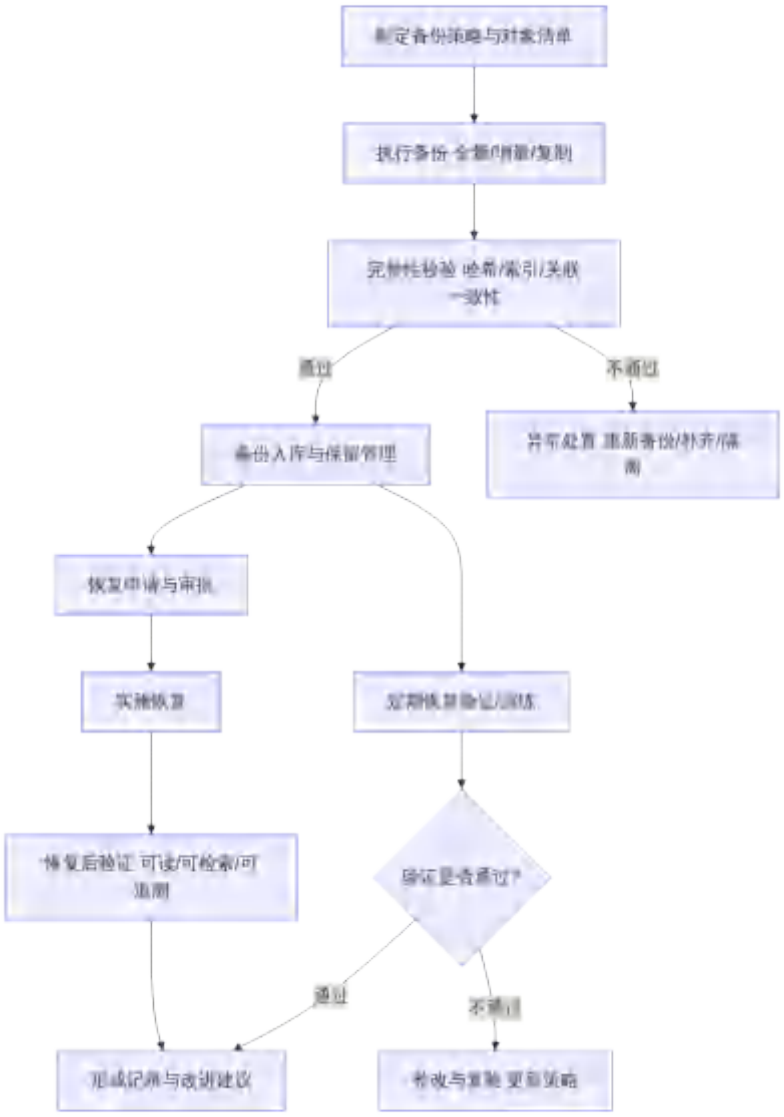

图1　备份与恢复管理流程示意图

8　安全控制与审计

8.1　总体要求

电子档案长期保存与异地备份安全控制应覆盖数据全生命周期，应对存储、传输、访问、备份、恢复与导出等关键环节实施安全措施，并应与组织的信息安全管理要求一致。

应对电子档案进行分级分类管理，并依据分级分类结果配置差异化的访问控制、加密保护、备份频率、保留周期与审计强度。

8.2　权限控制与访问审批

应建立基于角色的权限控制机制并执行最小授权原则。电子档案的浏览、检索、下载、导出、恢复与删除等操作应按权限控制，敏感档案访问与导出应实行审批。

权限变更应执行审批并留存记录，应定期开展权限核查与清理；对高权限账号和特权操作应加强审计与复核。

8.3 传输与存储安全

异地备份数据传输应采取保护措施，涉及敏感数据传输宜采用加密通道。备份数据存储宜采用加密或等效保护措施，并应明确密钥的生成、保管、轮换与销毁要求。

存储系统应具备访问隔离能力，备份存储与生产系统宜进行逻辑隔离或物理隔离，防止勒索软件、恶意删除等风险在同域传播。

备份介质（如磁带、移动硬盘等）应建立介质管理制度，至少应包括编号、登记、领用归还、出入库审批、环境要求与报废销毁记录。

8.4 日志审计与留痕

应对关键操作进行日志审计，审计范围至少应包括：用户登录与认证失败、权限变更、档案访问与导出、备份执行、校验结果、恢复申请与实施、恢复后验证、策略变更与异常事件处置等。

审计日志应包含操作者身份、时间、对象、操作类型、来源信息与结果状态等要素；对关键操作宜记录前后变化信息或引用信息。

审计日志应采取防篡改措施或等效控制，日志访问应受控，非授权人员不应查看或导出审计日志；日志留存期限应满足追溯与审计要求。

8.5 导出与共享控制

电子档案导出应实行审批控制，应明确导出目的、导出范围、导出格式、保密要求与责任人。

涉及个人信息、商业秘密或受限信息的数据导出，应采取脱敏、加密、水印或等效措施，并应记录导出全过程。

对外共享或跨系统交换应明确共享边界与责任，宜采用受控接口方式并记录共享日志；不宜以不受控介质方式大规模分发电子档案数据。

8.6 异地站点安全与环境保障

异地备份站点应满足物理安全与环境保障要求，应具备门禁管理、视频监控、消防与温湿度控制等措施，并应限定人员进入权限。

异地站点的运维操作应纳入统一运维管理，应记录运维行为并满足审计要求；远程运维应通过安全通道进行并进行强认证。

9 运行维护与检查评价

9.1 运行维护总体要求

应建立电子档案长期保存与异地备份运行维护机制，应明确运维职责、运维流程、响应要求与考核方式，并形成可追溯的运维记录。

运行维护应保障备份任务稳定执行、校验有效、恢复可用，应对容量、性能与异常事件实施持续监控，并根据风险变化与技术演进及时调整策略。

9.2 监控与告警

应建立监控与告警机制，监控内容至少应包括：备份任务状态、校验任务状态、存储容量、传输链路、站点可用性、异常访问与异常导出等。

备份失败、校验失败、容量不足、恢复验证失败、异常高频访问等事件应触发告警并进入处置流程；告警处置应形成闭环记录。

9.3 变更管理

备份策略、保留周期、站点配置、加密策略、校验算法、权限模型、系统版本与关键组件升级等变更应执行变更管理，应进行影响评估、审批、实施、验证与回退控制，并留存变更记录。

对可能影响档案可读性、可检索性或可追溯性的变更，应进行专项验证并形成验证证据。

9.4 定期检查与评价

应定期开展检查评价，检查内容至少应包括：备份覆盖率、备份成功率、校验通过率、恢复验证通过率、权限合规性、日志完整性、介质管理合规性与站点安全状态等。

检查评价应形成报告，报告应包含指标统计、问题清单、整改措施与改进建议；整改应闭环并复核。

9.5 持续改进

应基于监控数据、演练结果、审计发现与问题整改情况，持续优化长期保存与异地备份策略。

宜建立经验库与问题库，定期复盘重大故障与安全事件，形成制度或技术改进措施，并在同类业务场景中推广应用。