

电子档案长期保存策略在保障信息安全方面的有效性分析

孙士武

合肥包河文广产业投资有限公司 安徽合肥

【摘要】在数字化浪潮下，电子档案日益成为信息存储关键形式。其长期保存策略聚焦存储介质、加密、备份与人员管控。存储介质优选汰劣保障物理稳定；加密筑牢防泄防改壁垒；备份应对灾难确保可恢复；人员管理规范规避内部风险。综合各策略效能，精准剖析对防范数据损毁、泄密等安全问题的成效，为档案管理现代化转型提供安全守护指南。

【关键词】电子档案；长期保存；信息安全；存储介质；加密技术

【收稿日期】2025 年 4 月 15 日

【出刊日期】2025 年 5 月 8 日

【DOI】10.12208/j.ssr.20250207

Analysis on the effectiveness of long-term preservation strategy of electronic archives in ensuring information security

Shiwu Sun

Hefei Baohe Culture and Broadcasting Industry Investment Co., Ltd., Hefei, Anhui

【Abstract】In the wave of digitalization, electronic archives are increasingly becoming a critical form of information storage. Long-term preservation strategies focus on storage media, encryption, backup, and personnel management. Selecting high-quality storage media ensures physical stability; encryption builds robust barriers against leaks and modifications; backups address disasters to ensure recoverability; and personnel management mitigates internal risks. By comprehensively evaluating the effectiveness of these strategies, we can precisely analyze their impact on preventing data destruction, leaks, and other security issues, providing a safety guide for the modern transformation of archive management.

【Keywords】Electronic archives; Long-term preservation; Information security; Storage media; Encryption technology

引言

在当今数字化时代，电子档案呈爆发式增长，其承载的海量信息成为社会运转、知识传承的关键依托。但电子档案面临存储介质老化损坏、黑客恶意攻击、数据意外丢失、内部人员违规操作等诸多风险，时刻威胁信息安全。如何确保电子档案长期可靠保存意义重大。本研究聚焦存储介质、加密技术、备份机制与人员管理策略，深入探究其在保障电子档案信息安全上的有效性，为档案管理实践筑牢根基。

1 存储介质稳固根基

在数字时代，电子档案的存储介质呈现出多样化的态势，每一种介质都有着独特的特性。硬盘作为日常工作中极为常用的存储设备，具备存取便捷、数据读写

速度快的显著优势，能够迅速响应各类数据调用需求。传统的机械硬盘内部构造精密，对震动极为敏感，稍有不慎遭受震动，就可能造成盘片划伤、磁头损坏等严重问题，进而引发数据丢失^[1]。固态硬盘虽凭借闪存技术在读写速度上更胜一筹，却难以逃脱闪存衰减的宿命，随着使用年限增长、读写次数增多，闪存颗粒的性能逐渐下降，数据存储的稳定性面临挑战。

磁带以其成本效益高、存储容量大的特性，在电子档案存储领域占据一席之地，并且能够实现离线存储，有效抵御外界网络干扰。但磁带的检索方式相对繁琐，检索效率较低，在需要快速获取特定档案时往往力不从心。长期保存过程中，磁带介质还容易出现劣化现象，如磁带变形、磁粉脱落等，影响数据的完整性与可读性。

*通讯作者：孙士武（1989-）男，汉族，安徽阜阳，本科，研究方向为档案管理。

光盘存储凭借其稳定的特性，在电子档案存储方面表现不俗，尤其是蓝光光盘，在存储容量上优势突出^[2]。光盘的存储质量高度依赖刻录环节，刻录质量不佳容易导致数据读取错误。光盘对环境因素较为敏感，高温、高湿、强光等环境条件，都可能加速光盘的老化磨损，致使数据读取困难重重。

为强化电子档案存储介质的安全保障，档案部门必须制定严谨细致的规划。定期检测工作至关重要，借助专业的硬盘检测工具，能够精准评估硬盘的健康状况，及时发现潜在故障隐患；运用高精度的光学检测设备，可排查光盘表面的细微划痕，确保光盘数据的完整性。一旦检测到数据存在隐患，需迅速启动数据迁移流程，将数据转移至安全可靠的存储介质中。构建冗余存储体系同样不可或缺，采取多版本、多介质、异地备份的策略，实现全方位的数据保护。在本地构建硬盘镜像，确保日常数据的快速访问与恢复；在异地建立磁带备份中心，利用磁带的大容量与离线特性，应对可能出现的本地大规模灾害或系统故障。此外，为存储介质打造适宜的存储环境也不容忽视，严格控制存储场所的温度、湿度，使其保持在适宜范围内，有效防止介质因温湿度问题产生变形、腐蚀等状况。做好防尘、防静电措施，避免灰尘积聚影响介质性能，杜绝静电对电子元件的损害，从物理底层为电子档案的安全存续夯实基础，最大程度削减因介质“伤病”引发的信息散失风险。

2 加密技术严守机密

加密技术宛如电子档案的“隐形铠甲”，时刻抵御着外界的恶意侵袭。在众多加密算法中，对称加密算法以其高效的运算速度脱颖而出，如广泛应用的 AES 算法，在加密与解密过程中，犹如闪电般迅速，能够对海量数据进行高效批量处理^[3]。在内部环境中，对称加密的密钥管理相对简易，便于操作与维护。对称加密存在一个致命弱点，即密钥分发环节。倘若密钥在分发过程中“裸奔”，缺乏有效的安全防护措施，一旦密钥泄露，电子档案的安全门户将瞬间洞开，不法分子可轻易获取并篡改档案内容。

非对称加密算法，如 RSA 算法，采用公私钥搭配的独特模式。公钥可以广泛公开，用于数据加密；私钥则由所有者妥善保管，绝不外传，用于解密与数字签名。这种模式使得数字签名具备验真防伪的强大功能，同时保障了安全密钥交换的顺畅进行。非对称加密算法在运算过程中需要处理复杂的数学运算，运算负荷较重，对于大文件的处理速度犹如蜗牛爬行，在一定程度上限制了其应用场景。

在实际的电子档案加密实战运用中，常常融合对称加密与非对称加密的优势，实现互补。首先借助非对称加密算法，安全护送对称加密所需的密钥，确保密钥传输过程的万无一失。利用对称加密算法的高效性，对档案正文内容展开加密处理，大幅提升加密效率^[4]。针对不同密级的电子档案，需精准施策，实施差异化加密策略。对于高密级档案，采用强度更高的加密算法，并延长密钥长度，以“重兵把守”的态势，全方位增强档案的安全性。加密体系并非一成不变，需紧跟科技发展潮流，密切关注量子计算等具有颠覆性技术的发展走向。量子计算的超强运算能力，可能对现有的加密算法构成巨大威胁，因此必须及时升级加密算法，持续保持加密技术的领先性与有效性，让窥探者、篡改者面对加密后的电子档案望而却步。

3 备份机制筑牢防线

备份堪称电子档案的“避风港”，不同类型的备份方式功效各有千秋。全量备份能够完整留存电子档案的全貌，在数据恢复时，操作极为便捷，只需简单还原即可获取全部数据。但全量备份犹如“数据饕餮”，对存储空间的需求极大，每一次全量备份都需要占用大量的磁盘空间。频繁进行全量备份操作，还会给系统带来沉重负担，严重影响系统的正常运行效率^[5]。增量备份则显得更为机灵，它仅捕捉电子档案在两次备份之间发生变化的点滴数据，相较于全量备份，具有节省存储空间、备份速度快的显著优势。增量备份在数据恢复时步骤相对繁杂，需要依赖之前的全量备份作为基础，按照备份顺序依次恢复增量数据，一旦其中某个增量备份出现问题，可能影响整个恢复过程。

档案管理者在制定备份策略时，应当展现出足够的智慧，依据电子档案的动态变化情况以及重要程度“量体裁衣”。对于关键核心档案，应定期进行全量备份，如同为档案进行全面“体检”，确保档案数据的完整性与准确性。在两次全量备份的间隙，则灵活运用增量备份或差异备份进行“查漏补缺”，及时捕捉档案数据的变化。备份的落脚点也应多元化，本地冗余备份能够实现即时可用，在日常系统故障或数据误删除等场景下，可迅速恢复数据，保障业务的连续性。本地备份在面对大规模自然灾害、区域性网络攻击等极端情况时，抗灾能力较弱^[6]。异地灾备中心则凭借其地理位置的优势，安全可靠，能够有效应对本地无法承受的灾难事件，但建设与维护异地灾备中心的成本高昂。云端存储以其灵活便捷的特性，近年来备受青睐，用户可根据实际需求灵活调整存储容量，随时随地进行数据

备份与恢复操作。但云端存储也存在隐私隐忧，数据存于第三方云端服务器，数据隐私安全面临一定风险。融合三者长处，构建混合备份生态，如本地冗余备份保障日常使用，异地灾备中心应对重大灾难，云端存储作为补充，提供灵活的扩展与异地存储能力，确保在极端情境下电子档案能够迅速“重生”，成为信息安全“压舱石”。

4 人员管理把控内核

人员作为电子档案安保的“神经中枢”，对电子档案安全的影响微妙而关键。权限分配环节一旦失衡，便会引发严重问题。若赋予人员的权限过大，无异于为违规操作大开“绿灯”，某些心怀不轨之人可能利用过高权限肆意篡改电子档案内容，甚至将机密档案泄露给外部不法分子，给单位或组织带来难以估量的损失^[7]。反之，若权限分配过小，相关工作人员在履行正常工作流程时，会因权限不足而处处受阻，导致工作效率低下，档案管理流程无法顺利推进。

安全认知不足同样是电子档案安全的一大隐患。部分人员安全意识淡薄，设置密码时过于简单随意，或者长期使用同一弱密码，极易被不法分子通过暴力破解手段获取账号权限。账号共享现象时有发生，不同人员共用一个账号登录档案管理系统，一旦该账号泄露，众多档案信息将面临风险。更有甚者，在面对网络钓鱼链接时，缺乏足够的警惕性，轻易点击链接，导致个人信息泄露，进而被不法分子利用，入侵档案管理系统，使系统防护的措施形同虚设。

强化人员管控，要精细“雕琢”权限架构。依据不同岗位的工作需求，精准适配相应权限，确保工作人员既能顺利开展工作，又不会拥有过高权限带来安全风险。权限并非一成不变，应根据人员岗位变动、工作内容调整等实际情况，进行动态调整^[8]。采用多因素身份核验手段，如密码、指纹识别、短信验证码等，严格把控人员访问档案管理系统的入口。建立健全操作日志记录机制，对关键岗位人员的每一次操作进行全程留痕，便于后续追溯与审计。定期开展安全培训工作，通过实战演练模拟网络攻击场景，让工作人员亲身体验安全的风险；结合实际案例剖析，深入讲解安全事件发生的原因、造成的危害以及防范措施，唤醒工作人员的安全防范本能。对关键岗位人员进行严格的背景审查，确保人员政治可靠、品行端正，从源头上降低安全

风险。以人员高素质、高自律为笔，书写档案安保华章，从管理“内里”为长期保存策略注入灵魂，保障信息安全无死角。

5 结语

面向未来，科技变革加速电子档案进化。存储介质向高耐久、智能化进阶，管理要精准适配；加密迎量子挑战，算法革新刻不容缓；备份借 AI 赋能，智能决策、高效恢复；人员管理依托数字化升级，精准防控、智慧引导。各方携手共进，电子档案信息安全保障将突破新高，持续为社会发展、知识传承保驾护航，让数字记忆永恒流传。

参考文献

- [1] 许靖皎.电子档案长期保存中的信息安全问题与对策研究[J].兰台内外,2025,(10):4-6.
- [2] 徐智林.电子档案长期保存标准与技术适配性[J].大众标准化,2025,(06):129-131.
- [3] 张瑞华,郑毅,高大伟.电子档案中电子印章“去技术化”的法律问题及解决路径[J].档案管理,2025,(02):24-28+33.
- [4] 谢永宪.电子档案长期保存的正确打开方式[J].山西档案,2025,(02):2.
- [5] 吴楠,李洁.地质调查电子会计档案管理研究[J].中国矿业,2024,33(S2):24-28.
- [6] 王苗.基于云计算的电子档案信息资源长期保存策略研究[J].兰台内外,2024,(29):28-30.
- [7] 李婧媛,蔡云.PIGZ 工具软件在省级电子气象档案归档与长期保存系统中的应用[J].山地气象学报,2024,48(03): 108-111.
- [8] 曹洪阳.电子档案“四性”要求及其检验路径探析[J].兰台内外,2023,(18):31-33.

版权声明：©2025 作者与开放获取期刊研究中心（OAJRC）所有。本文章按照知识共享署名许可条款发表。

<http://creativecommons.org/licenses/by/4.0/>



OPEN ACCESS