 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i1.23198

Research on the security guarantee and system construction in the digital management of archives information

Haijun Huo

Dongsheng District, Ordos City, Inner Mongolia, Ordos, Inner Mongolia, 017000, China

Abstract

The digital management of archival information has become the core trend of modern archival management, but the subsequent data security problems are becoming increasingly prominent. Starting from the current situation of digital management of archival information, this paper analyzes the security risks faced in the process of information storage, transmission and use, including technical loopholes, external attacks and human operation error. Based on the needs of security guarantee, the construction principles and implementation strategies of the digital archives management system are put forward, covering data encryption, access control, backup and recovery, and multi-level security management mechanism. Through the construction of a comprehensive security guarantee system, it can effectively prevent security threats, improve the reliability and sustainability of archives management, and provide theoretical and practical support for the realization of the modernization of archives management.

Keywords

file digitization; information security; management system; data encryption; risk prevention and control

档案信息数字化管理中的安全保障与体系构建研究

霍海军

内蒙古鄂尔多斯市东胜区就业局，中国·内蒙古 鄂尔多斯 017000

摘　要

档案信息数字化管理已成为现代档案管理的核心趋势，但随之而来的数据安全问题也日益突出。本文从档案信息数字化管理的现状出发，分析其在信息存储、传输与使用过程中面临的安全风险，包括技术漏洞、外部攻击和人为操作失误等。基于安全保障需求，提出档案数字化管理体系的构建原则和实施策略，涵盖数据加密、访问控制、备份恢复与多层次安全管理机制等方面。通过构建综合性的安全保障体系，能够有效防范安全威胁，提升档案管理的可靠性与可持续性，为实现档案管理现代化提供理论与实践支持。

关键词

档案数字化；信息安全；管理体系；数据加密；风险防控

1 引言

随着信息技术的快速发展，档案管理逐步向数字化方向转型。档案信息的数字化管理不仅提升了档案的存储、查阅和利用效率，还为档案资源的共享与开发提供了广阔空间。然而，这一转型也带来了前所未有的信息安全挑战。档案信息的数字化存储和在线传输，使其更易受到网络攻击、数据泄露及人为误操作的威胁。一旦发生安全事故，不仅会造成数据丢失或损坏，还可能影响档案的真实性与完整性，进而引发严重的社会和法律后果。

目前，档案信息数字化管理在安全保障方面仍存在诸多不足，例如缺乏系统化的管理机制、安全技术应用水平不足以及风险评估意识薄弱等。针对这些问题，本文旨在从风险防控的角度，研究档案信息数字化管理中的安全保障策略与管理体系构建方法，为相关领域的实践提供指导。

【作者简介】霍海军（1979–），男，中国内蒙古鄂尔多斯人，硕士，从事档案管理研究。

2 档案信息数字化管理的安全风险分析

2.1 数据存储中的风险

档案信息数字化管理首先面临的是数据存储安全问题。数字化档案通常存储于数据库或云平台中，这些存储介质在技术层面上可能存在漏洞。例如，数据库系统的权限设置不当可能导致非法访问，而云平台由于依赖于第三方服务，其安全性也难以完全掌控。此外，硬件设备的故障和老化也是数据存储中的潜在风险，特别是在备份机制不完善的情况下，一旦出现问题可能导致重要档案信息的永久丢失。

2.2 信息传输中的风险

档案信息的数字化管理往往需要通过网络实现档案的传输与共享。在传输过程中，档案信息可能面临窃听、篡改和中间人攻击等风险[1]。例如，未经加密的数据传输可能

被恶意第三方截取，从而导致档案信息的泄露。此外，网络环境中的不稳定性，如数据丢包和延迟，也可能对传输的完整性和时效性产生负面影响。

2.3 使用与管理中的风险

档案信息在数字化使用与管理过程中，人为操作失误和权限控制不当是主要风险来源。例如，管理员在操作系统时可能因疏忽删除重要档案，而未经严格权限控制的系统可能被无关人员访问，导致档案信息的泄露或滥用。同时，内部人员的恶意操作，例如私自复制或篡改档案，也构成了不可忽视的安全威胁。

3 档案信息数字化管理中的安全保障原则

3.1 以预防为主的风险管理原则

档案信息数字化管理的安全保障需要以风险预防为核心，通过全面的风险识别与评估，提前采取措施避免潜在威胁。这一原则的核心在于将安全防护前置化，在威胁发生之前就采取有效的预防措施[2]。例如，在数据存储方面，应优先选择高可靠性的存储介质，如具有容错功能的冗余阵列磁盘（RAID）和分布式存储架构，并结合加密存储技术提升数据的安全性。此外，为了防止硬件设备的老化和故障带来的风险，应建立定期检查和维护机制，包括磁盘的性能检测、温湿度环境的监控和备份设备的运行测试等。这些措施能够在硬件故障发生前及时发现隐患，从而有效降低因硬件问题导致数据丢失的可能性。

在信息传输过程中，风险预防的重点在于保护数据的保密性、完整性和真实性。例如，可采用端到端加密协议（如 TLS）对传输数据进行保护，确保数据在网络传输中不被截取或篡改。同时，还应结合数字签名技术对数据的完整性进行验证，防止恶意篡改或中间人攻击。

3.2 技术与管理相结合的综合保障原则

安全保障不仅依赖于先进的技术手段，还需要建立科学完善的管理体系，实现技术与管理的深度融合。技术手段为档案信息的安全提供了基础支持。例如，数据加密能够有效防止未经授权的访问和数据泄露，访问控制机制可以限制用户权限，而防火墙技术能够拦截恶意攻击和非法入侵。然而，这些技术的有效运行需要管理体系的配合才能发挥最大效用。

管理体系的建立需要从制度化、流程化和规范化入手。通过制定严格的规章制度，例如分级授权机制，可以明确不同岗位、不同用户的权限范围。对于档案管理系统中的敏感信息，可设置更高等级的权限访问要求，并对用户的操作行为进行详细记录和监控。

3.3 动态调整与持续优化原则

档案信息安全的威胁是动态变化的，因此安全保障体系需要具备持续调整与优化的能力。网络攻击手段和安全漏洞的演化速度极快，仅依赖一成不变的防护措施可能无法满足档案信息管理的安全需求。在这一背景下，动态调整和持续优化成为安全体系的关键。

在技术层面，面对不断演化的网络攻击手段，应定期更新安全软件和防护设备，确保其能够应对新型威胁。例如，安装具有主动威胁检测功能的防病毒软件，并通过实时更新病毒库提高对未知攻击的识别能力[3]。此外，还应结合漏洞扫描工具定期检查系统的潜在安全漏洞，针对发现的薄弱环节及时安装补丁或升级设备。动态调整还应包括安全策略的调整，例如根据网络流量和用户行为分析，优化防火墙规则和入侵监测机制。

4 档案信息数字化管理安全保障体系的构建

4.1 数据加密与存储安全策略

数据加密是保障档案信息在存储和传输过程中不受攻击的重要技术手段。数字化档案在存储阶段面临非法访问、数据泄露等风险，而加密技术的应用可以有效降低这些风险。对于存储的档案信息，可以结合对称加密与非对称加密技术构建安全框架。对称加密具有加密速度快、适用于大数据量处理的优势，例如采用 AES（高级加密标准）对大规模档案数据进行加密；非对称加密则可通过 RSA 算法保护数据传输中的密钥交换，进一步提高安全性。两者结合使用，可实现档案数据的高效保护。

为进一步提高数据存储的安全性，应在物理和逻辑两个层面采取多重措施。例如，设置多个地理位置的备份存储点，采用分布式存储技术，将数据分片存储在多个服务器中，以避免单点故障造成的数据丢失或服务中断。此外，可部署冗余阵列磁盘（RAID）系统，通过实时同步多块磁盘的数据，提升存储的容错能力。在存储环境的物理安全方面，应采取访问控制、视频监控等措施，确保服务器机房的安全性。通过这些技术手段与管理措施的结合，能够有效提升档案信息存储的可靠性和抗风险能力。

4.2 访问控制与权限管理机制

访问控制与权限管理是数字化档案信息安全体系中的重要组成部分，其目标是通过对用户权限的精细化管理，确保档案信息仅被授权人员访问、修改和操作。具体而言，可以采用基于角色的访问控制（RBAC）模型，将档案管理系统的用户权限划分为不同等级，例如普通用户只能查看档案，管理员则拥有档案上传、删除和修改的权限。在系统开发中，还可根据实际需求引入基于属性的访问控制（ABAC）技术，通过条件筛选的方式实现更灵活的权限管理。

在权限管理机制的设计中，生物识别技术的引入进一步提升了系统的安全性。例如，指纹识别、人脸识别和虹膜识别等技术可用于身份验证，确保档案信息的访问仅限于合法用户。结合双因子认证（2FA），通过密码和生物特征的联合验证，能够有效防止非法访问。此外，权限变更和审核机制是权限管理的重要环节。系统应具备自动记录和监控用

户权限变更的功能，确保权限分配的透明性和可追溯性。在权限审核中，可设置定期的权限清理流程，移除不再需要访问权限的用户，从而减少潜在的安全隐患。

4.3 安全监测与应急响应系统

实时的安全监测对于快速发现安全威胁至关重要。在档案管理系统中，可部署入侵检测系统（IDS）和安全信息与事件管理系统（SIEM），对系统访问日志、网络流量和用户行为进行全天候的监控和分析。这些系统利用预设规则和机器学习算法，可以实时检测异常访问、频繁失败的登录尝试以及其他潜在的攻击行为。一旦发现异常，系统可自动发出警报，并采取防护措施，例如阻断攻击来源或锁定受影响的账户。

应急响应系统是处理安全事件的重要保障。通过制定详细的应急响应计划，可以在安全事件发生后迅速采取措施，将损失降到最低。例如，当系统检测到数据泄露时，应首先隔离受影响的服务器，防止威胁扩散；其次，通过恢复备份数据和修复漏洞，确保系统尽快恢复正常运行。此外，应急响应计划还需明确事件后的调查和总结流程，通过追溯攻击路径和分析问题根源，为系统优化提供依据。通过将监测与响应有机结合，可以形成闭环的安全保障体系，为档案信息的数字化管理提供持续性的防护。

5 档案信息数字化管理的优化建议

5.1 引入先进技术提升系统安全性

在当前信息技术快速发展的背景下，引入前沿技术能够显著提升档案管理系统的安全性与可靠性。例如，区块链技术作为一种去中心化的数据存储技术，可用于记录档案的操作流程和权限变更等关键信息，从而确保数据的不可篡改性与高透明性。通过在档案管理系统中构建区块链网络，可以实现档案操作记录的分布式存储和自动化校验，极大提高档案信息的可信度和可追溯性[4]。

人工智能技术在安全威胁的预测和识别方面同样具有重要作用。例如，通过深度学习算法对系统日志和用户行为进行模式分析，可以及时发现异常行为并提前预警。结合自然语言处理技术，AI 还能帮助管理人员从海量日志中提取关键信息，提高安全事件分析的效率。此外，可结合物联网（IoT）技术部署智能传感器，实现对物理环境的实时监测，如温湿度、烟雾浓度等，为档案的物理安全提供进一步保障。

5.2 强化安全意识与制度建设

技术的有效应用离不开管理制度的支持。在档案信息数字化管理中，高校和企事业单位应建立一套完善的安全管理制度，从根本上规范人员的操作行为。例如，可制定档案数据访问和操作的细则，明确不同角色的责任范围与权限限制。此外，定期的安全培训和教育是增强档案管理人员安全意识的有效手段。通过组织培训班和案例分析，帮助人员了解常见的安全威胁和应对措施，并在日常操作中养成良好的安全习惯。

审计与监督机制是确保制度有效实施的关键。管理单位应定期对系统的安全状态进行全面检查，包括权限分配是否合理、防火墙和加密软件是否正常运行等。此外，还应对档案操作记录进行随机抽查，以发现潜在的违规行为。对违规者应采取严格的追责措施，通过建立奖惩机制强化制度的执行力。通过技术与管理的紧密结合，可以构建起更加稳健的档案信息安全保障体系。

6 结语

档案信息数字化管理的安全保障是实现档案管理现代化的重要前提。针对当前存在的安全风险，本文从技术和管理两个层面提出了构建综合安全保障体系的策略，包括数据加密、权限控制、安全监测与应急响应等措施。通过引入区块链、人工智能等新兴技术，并结合完善的管理制度，能够有效提升档案管理系统的安全性与可持续性。未来，随着信息技术的进一步发展，档案管理的安全保障体系应不断优化与完善，以应对复杂多变的安全威胁，为档案资源的高效利用和保护提供更加坚实的技术与管理支持。

参考文献

[1] 王宇飞,尚震.药品生产线档案管理智能化解决方案研究[J].流程工业,2024,(12):50-53.

[2] 看卓措.数字化助力提升高校档案品牌建设[J].中国品牌与防伪,2024,(12):87-89.

[3] 姜歌.数字化档案管理在事业单位中的应用分析[J].办公自动化,2024,29(24):62-64.

[4] 罗伟华.信息时代下的教育局文书档案管理优化路径[J].办公自动化,2024,29(24):75-77.