

数字化转型背景下国企档案安全管理制度建设探析

熊 燕

武汉市政工程设计研究院有限责任公司 湖北 武汉 430000

【摘要】：随着数字化转型的加速推进，国有企业面临着档案管理模式和安全保护要求的双重挑战。传统的档案管理模式已无法满足现代化企业在信息化、数字化管理过程中对档案安全和保密的需求。为此，数字化转型背景下的档案安全管理制度建设显得尤为重要，如何实现档案管理的数字化、安全性与高效性成为亟待解决的问题。构建健全的档案安全管理制度，适应数字化转型的需求，是保障企业档案信息安全、推动管理创新的关键。通过加强制度设计、技术支撑与人员管理等方面的结合，可以有效提升国企档案安全管理的整体水平，防范潜在风险，确保档案信息的长期安全。

【关键词】：数字化转型；国有企业；档案管理；安全管理；制度建设

DOI:10.12417/3041-0630.26.08.018

引言

在数字化转型的浪潮中，国有企业的管理体系正逐步迈向信息化和智能化。然而，随着信息技术的广泛应用，企业面临的档案安全管理问题愈加严峻。传统的纸质档案管理逐步转型为电子档案和数字化信息管理，这一变化给企业带来了便利的同时，也引发了对档案安全性、完整性和保密性的严峻考验。如何在数字化环境下保障档案管理的真实性，成为了国企在推动数字化转型过程中亟需解决的关键问题。探索建立适应新形势下的档案安全管理制度，不仅是提升管理效能的需求，更是确保企业信息安全、持续发展的必然选择。

1 数字化转型对档案管理的挑战

数字化转型带来了企业档案管理方式的深刻变革，同时也使档案管理面临更加复杂和多样化的挑战。传统的档案管理模式主要依赖于纸质文件的存储和人工管理，这种模式下，档案安全依赖于物理存储环境和人员管理。在数字化转型的推动下，档案逐渐进入电子化、信息化管理阶段，档案的保存和管理方式发生了根本性的变化^[1]。数字化档案虽然具有存储便捷、访问迅速等优点，但也暴露出了新的安全隐患。电子档案容易受到黑客攻击、病毒侵入以及系统故障等因素的影响，这些都极大地增加了档案信息泄露和丢失的风险。

随着信息技术的广泛应用，企业档案管理不仅需要应对日益复杂的技术环境，还必须考虑到不同技术手段所带来的安全隐患。数字化转型过程中，档案数据的多元化存储和共享使得信息的传递变得更加快捷，但也使得档案的保护工作变得更加困难。电子档案在跨部门、跨地域的共享与流转中，可能会遭遇未经授权的访问和篡改，导致档案的完整性和保密性受到威胁。由于数字化档案管理系统中涉及到多种软硬件设备和技术平台，管理过程中一旦出现漏洞，极有可能导致数据泄露或丢失，给企业带来巨大的损失。

数字化转型对档案管理带来的最大挑战之一，是如何在满足日常管理需求的同时，确保档案数据的长期安全性和可靠性。随着档案数量和种类的激增，传统的纸质档案安全防护措施已经无法适应现代化的管理需求。数字化档案管理系统的安全漏洞、技术不稳定性以及管理人员对信息安全的意识不足，都会加剧档案信息在转型过程中的安全风险。企业必须加强档案安全管理的技术保障与制度建设，以应对数字化转型所带来的各种挑战。

2 构建有效的档案安全管理制度

在数字化转型的过程中，构建一个科学且有效的档案安全管理制度显得尤为关键。传统的档案管理体制已无法适应现代信息化、数字化环境下的需求，企业必须在档案管理的各个层面上进行全面的制度重构。档案安全管理制度需要涵盖从档案的生成、存储到使用、销毁等各个环节，确保每一个环节都能够遵循严格的安全标准^[2]。电子档案和纸质档案管理模式的结合，要求企业必须建立一个多层次、全方位的档案安全管理体系，不仅要加强物理环境的保护，还要在技术上实现数据加密、身份认证、权限控制等安全措施。这种制度建设不仅要符合国家的相关法律法规，还需要根据企业的实际情况，量体裁衣，做到具体问题具体分析。

有效的档案安全管理制度还必须通过强化技术保障，确保档案数据的安全性和可靠性。数字化档案的存储和管理不再局限于纸质文件的封存，而是转向了信息化平台和云存储系统。这种转型要求企业不仅在硬件设施上进行投入，还要在软件系统上加强信息安全防护。档案管理系统需要具备高效的防护机制，例如采用高级加密技术对档案数据进行加密处理，以防止未经授权的访问与篡改。信息系统还需配备实时监控功能，能够及时发现并应对各种潜在的安全威胁。档案系统的备份与恢复机制同样至关重要，一旦发生系统崩溃或数据丢失，可依托完备的恢复方案，最大限度降低信息泄露与数据损毁造成的损

失。

制度建设成功与否，关键还在于企业人员的管理与培训。无论是数字化档案的管理人员，还是日常使用档案的各类职能部门人员，必须强化信息意识和操作规范。建立严格的岗位责任制，对档案安全管理人员进行专门培训，确保其掌握必要的安全技能和法律法规知识，以便及时应对各种突发事件。要加强跨部门之间的沟通协作，确保在档案管理过程中，能够形成合力，避免因人员失职或疏忽导致的档案信息泄露或丢失。在此基础上，企业应定期开展安全审计和风险评估，及时发现制度中的漏洞与不足，进行调整与优化，确保档案管理制度始终能够适应快速变化的数字化转型环境。

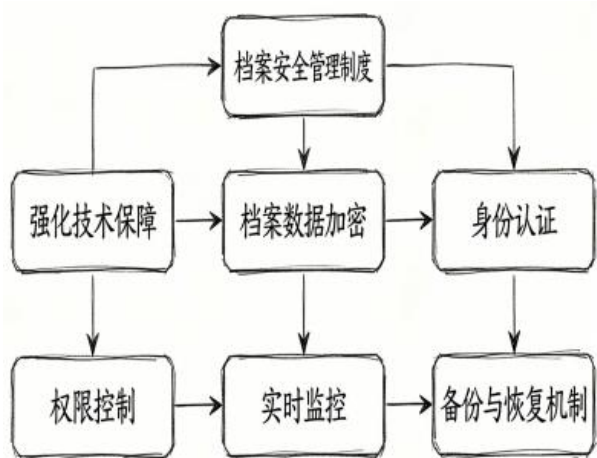


图1 档案安全管理制度架构图

3 提升档案管理安全的实践路径

提升档案管理安全的实践路径，必须着眼于技术创新与制度保障的有机结合。数字化转型要求企业在管理方式上实现突破，尤其是在档案安全管理上，必须通过技术手段提升档案的保护能力。档案数据加密技术作为一项基础性的安全措施，已成为保护档案信息的关键手段。企业应当采用先进的加密算法对档案数据进行处理，确保在存储、传输过程中的数据安全^[3]。

参考文献：

[1] 廖有永.数字化转型对国有企业价值的影响研究[J].现代商业,2025,(24):107-110.
 [2] 郭瑾.数字化转型背景下国有企业思想政治工作的创新路径[N].河南经济报,2025-12-23(010).
 [3] 韩宜,张记元.数字化转型如何赋能国有企业主业创新[J].新疆农垦经济,2025,(12):78-92.

身份认证和权限管理系统的建设，也至关重要。通过多重身份验证机制，确保只有授权人员才能访问敏感档案，并对文件的操作进行实时跟踪与审计，避免任何未授权的篡改或泄露事件发生。通过这一系列技术手段，企业可以有效防止黑客攻击和数据泄露风险，确保档案在数字化转型过程中不受威胁。

另一方面，提升档案管理安全的路径还需要优化管理流程与制度建设。数字化档案管理并非单纯依赖技术，它同样需要科学的管理制度作为支撑。为了有效保障档案安全，企业应当从制度层面上进行完善，建立健全的档案安全责任制。各部门之间必须建立协同机制，在档案的使用、存储和传递过程中，严格遵循安全管理规范。定期的安全审计与风险评估机制，可以有效发现潜在的漏洞和风险，及时进行整改，从而避免管理上的盲区。通过加强对档案管理的监督和控制，能够确保档案信息的保密性和完整性。

在提升档案管理安全的实践中，人员的安全意识和操作规范也起着至关重要的作用。企业需要对档案管理人员和相关职能部门进行定期的安全培训，提高其对数字化档案管理的认知和应对能力。只有当管理人员具备了扎实的专业知识和较强的安全意识，才能在日常操作中有效避免安全隐患。强化对企业内部人员的安全审查与行为规范管理，能够有效预防内部人员因疏忽或恶意操作导致的安全事件。通过制度保障、技术创新和人员培训的三方合力，企业可在数字化转型进程中牢牢守住档案安全底线，推动档案管理工作高质量可持续发展。

4 结语

数字化转型对国有企业档案管理提出了前所未有的挑战，同时也为提升档案管理的安全性提供了新的机遇。构建完善的档案安全管理制度、采用先进的技术手段，并加强人员培训和管理，已成为保障档案安全的关键措施。面对快速变化的信息化环境，只有不断优化管理模式，提升安全保障能力，才能确保档案信息的长期安全与可靠性，为企业的可持续发展提供有力支持。