

档案保密管理在物资供应链管理中的应用与挑战

刘娟娟 曾峰 朱江

国网重庆市电力公司市北供电分公司，重庆渝北，401147；

摘要:在数字化时代，物资供应链管理中的档案保密管理面临前所未有的挑战与机遇。本文深入探讨了档案保密管理在物资供应链中的重要性，以及在数字化转型过程中如何有效保护敏感信息。通过分析当前数字化档案管理技术的发展及其在供应链中的应用，本文揭示了档案保密管理在防范信息泄露、数据篡改等方面的核心作用，并提出了平衡信息共享与保密的策略。同时，本文还探讨了跨组织档案保密管理的协同困境及应对措施，旨在为相关领域的实践者提供有益的参考，推动档案保密管理在数字化背景下的创新发展。

关键词:档案保密管理；物资供应链；数字化转型；信息安全；管理机制

DOI:10.69979/3029-2727.24.09.048

引言

随着全球经济数字化进程的加速，物资供应链管理中的档案保密问题日益复杂且关键。在信息高度流通的环境下，档案管理的失误可能导致严重的商业风险和竞争劣势。传统的纸质档案管理方式已无法满足现代供应链的快速反应需求，数字化档案管理成为必然趋势。然而，数字化转型虽提升了效率，但也带来了新的安全隐患，尤其是在敏感信息的保密管理上。系统漏洞、黑客攻击等网络安全问题，以及管理人员安全意识不足、管理制度执行不力等问题，都使得档案保密管理面临严峻挑战。如何在推动数字化转型的同时确保档案信息的安全性，已成为物资供应链管理领域亟待解决的重要课题。本文将围绕档案保密管理在数字化背景下的应用与挑战展开讨论，为相关领域的实践者提供有益的参考。

1 档案保密管理在物资供应链中的现状与问题

在物资供应链管理中，档案保密管理的重要性日益凸显，尤其在当今信息高度流通的环境下，档案管理的失误可能导致严重的商业风险和竞争劣势。现阶段，物资供应链中的档案管理面临着多方面的挑战。档案信息的多样性和复杂性增大了管理的难度。物资供应链涉及的档案不仅包括合同、发票、采购订单等传统文件，还涵盖了供应商信息、库存数据、物流信息等，这些信息的敏感性和重要性要求在管理中更为谨慎。

传统的纸质档案管理方式面临存储空间有限、易损坏、易丢失等问题，而在数字化管理中，档案的传输和存储依赖于信息技术，这使得系统漏洞、黑客攻击等网络安全问题成为新的威胁。若缺乏有效的加密技术和访

问控制机制，信息在传输或存储过程中极易被非法获取或篡改，进而影响供应链的正常运作。档案管理人员的安全意识不足也是一个不容忽视的问题。尽管企业在制度上有一定的规范要求，但由于管理人员对保密制度的认识不足或操作不当，档案管理过程中的人为因素往往成为信息泄露的主要原因之一。

档案管理的制度建设和执行力度也存在明显不足，一些企业缺乏对管理人员的定期培训和监督，导致管理流程中可能出现违规操作或疏忽，进一步加剧了档案保密管理的风险。物资供应链中的档案保密管理现状揭示出其在数字化转型背景下所面临的诸多挑战，这些问题不仅影响着档案管理的效率 and 安全性，也对供应链的整体运行产生了深远的影响。

2 数字化转型中的档案保密管理策略

在数字化转型过程中，档案保密管理策略的制定和实施至关重要。首先，企业需要构建一个全面的档案管理系统，该系统不仅要具备数据加密、身份验证和访问控制等基本功能，还应融入多层次的安全防护机制，如防火墙、入侵检测系统和数据备份系统等。通过这些技术手段，可以有效防止档案在存储和传输过程中的信息泄露和篡改风险。

区块链技术在档案保密管理中的应用也越来越受到关注。区块链的分布式账本和不可篡改性能够为档案的完整性和真实性提供有力保障。在区块链网络中，档案的每一次访问或修改都会生成一个新的区块，这些区块由多个节点共同验证，确保了档案信息的不可逆性和透明度。企业还需建立严格的档案保密管理制度，将档

案的访问权限限定在特定的人员范围内，并定期审查和更新这些权限配置，避免因人员流动或职责变动引发的安全漏洞。同时，加强对档案管理人员的安全意识培训，确保他们具备应对数字化环境下安全威胁的能力。

人工智能和大数据技术的引入，为档案保密管理提供了新的可能性。通过人工智能算法，企业能够对档案访问行为进行实时监控，快速识别异常活动，并采取相应措施。大数据分析可以帮助企业预见潜在的安全威胁，优化档案保密策略，使管理更加精准和高效。在数字化转型的背景下，这些策略的综合运用，能够显著提高档案管理的安全性和可靠性，确保企业在信息化进程中能够稳步前行。

3 档案保密管理的创新实践与优化路径

在未来的档案保密管理中，技术创新和制度完善将是两个关键的发展方向。随着数字化技术的持续进步，档案管理将逐步采用更为先进的加密技术，如量子加密和生物识别技术，以增强信息的保密性。量子加密技术通过量子密钥分发，实现了绝对安全的数据传输，有效防止了信息在传输过程中的被窃听或篡改。同时，生物识别技术能够通过指纹、虹膜或面部识别等方式，确保只有经过授权的人员才能访问敏感档案，进一步提升档案的安全管理水平。

在制度层面，档案保密管理将更加注重分类分级管理。企业需要根据档案信息的敏感程度，建立完善的档案分级管理制度，并在档案的存储、传输和使用环节实施严格的权限控制。这种分类分级管理不仅能有效保障高敏感度信息的安全性，也能在一定程度上提高档案信息的利用效率，避免因过度保护导致的信息孤岛现象。随着物联网和云计算技术的普及，企业需要构建分布式档案管理系统，确保在多节点环境下的数据安全。分布式管理系统能够通过多副本存储和异地备份，防止单点故障导致的信息丢失，同时提高了数据的可用性和安全性。

未来的档案保密管理还将加强与外部合作伙伴的协作，通过建立统一的档案保密标准，共同应对数字化带来的安全挑战。这种跨组织的协作不仅有助于提升整体供应链的安全水平，也能够应对突发安全事件时，形成快速响应机制，最大限度地降低信息泄露的风险。通过技术和制度的双重推动，档案保密管理将在企业数字化转型中发挥更加重要的作用，成为保障企业信息安全和业务连续性的核心支撑。

4 档案保密管理中的信息共享与安全平衡难题

在物资供应链管理中，档案保密管理的核心挑战之一是平衡信息共享与安全保护之间的矛盾。供应链的高效运作依赖于信息的快速流通和共享，但过度的信息公开又可能导致敏感信息泄露，给企业带来巨大的商业风险。例如，供应商信息、库存数据和物流信息等档案内容既需要在供应链上下游之间共享，又必须严格保密。这种信息共享与安全保护之间的悖论，成为档案保密管理亟待解决的关键问题。

4.1 信息共享与安全保护的悖论表现

在物资供应链中，信息共享是实现协同运作的基础。供应商需要了解采购订单的详细信息，物流企业需要掌握库存和运输计划，而采购部门则需要实时监控物流状态。然而，这些信息往往包含敏感内容，如供应商的定价策略、企业的库存水平和未来的采购计划等。如果这些信息被不当共享或泄露，可能会导致竞争对手获取商业机密，从而削弱企业的竞争优势。

此外，信息共享的范围和程度也难以把控。一方面，企业内部各部门之间需要共享信息以提高工作效率，但不同部门对信息的保密要求不同，可能导致信息泄露风险。另一方面，供应链上下游企业之间的信息共享也面临挑战。例如，供应商可能担心其技术参数和成本信息被泄露，而采购方则希望获取更多关于产品质量和供应能力的信息。这种信息不对称和信任缺失进一步加剧了信息共享与安全保护之间的矛盾。

4.2 技术与管理创新：实现信息共享与安全保护的平衡

为了解决这一悖论，企业需要在技术手段和管理机制上进行创新。首先，技术手段方面，可以采用先进的加密技术，如端到端加密和数据脱敏技术。端到端加密确保信息在传输过程中不被窃取或篡改，而数据脱敏技术则可以在共享信息时隐藏敏感内容，从而在不影响信息可用性的情况下保护信息安全。此外，区块链技术的分布式账本和不可篡改性也为信息共享提供了新的解决方案。通过区块链，供应链中的每个节点都可以安全地共享和验证信息，同时确保信息的真实性和完整性。

在管理机制方面，企业需要建立严格的信息共享政策和权限管理机制。根据信息的敏感程度和使用需求，制定分级共享规则，明确哪些信息可以共享、共享给谁以及共享的范围。同时，通过建立信任机制，如签订保密协议和建立合作伙伴信用评价体系，增强供应链上下

游企业之间的信任。此外,企业还可以通过定期的安全审计和风险评估,及时发现和解决信息共享过程中的安全隐患。

通过技术手段和管理机制的双重创新,企业可以在保障信息安全的前提下实现高效的信息共享,从而提升供应链的整体运作效率。

5 档案保密管理的跨组织协同困境与应对策略

随着物资供应链的全球化和复杂化,档案保密管理不再局限于单一企业内部,而是需要跨组织的协同管理。然而,不同组织之间的信息安全标准、管理流程和技术应用存在显著差异,这给跨组织档案保密管理带来了诸多挑战。例如,供应链上下游企业可能因保密标准不一致而导致信息泄露风险,或者因缺乏有效的协同机制而影响信息共享效率。本文将分析跨组织档案保密管理的现状和困境,并提出构建统一的档案保密标准、建立协同管理平台以及加强合作伙伴间信任机制等解决方案,以提升供应链整体的档案保密管理水平。

5.1 跨组织档案保密管理的现状与困境

在跨组织的供应链环境中,档案保密管理面临诸多挑战。首先,不同组织的信息安全标准和管理流程差异较大。一些企业可能采用严格的信息加密和访问控制措施,而另一些企业则可能缺乏完善的保密制度。这种差异导致在信息共享和协同工作时,难以统一管理标准,增加了信息泄露的风险。其次,技术应用的不一性也给档案保密管理带来困难。不同企业可能使用不同的信息系统和数据存储方式,这使得信息在跨组织传输和共享时容易出现安全漏洞。

此外,供应链上下游企业之间的信任机制不完善也是跨组织档案保密管理的重要障碍。由于缺乏有效的信任保障,企业在共享敏感信息时往往持谨慎态度,这不仅影响了信息共享的效率,也可能导致供应链协同运作的中断。例如,供应商可能担心其核心技术参数被泄露,而采购方则可能对供应商提供的信息真实性存疑。这种信任缺失进一步加剧了跨组织档案保密管理的复杂性。

5.2 构建跨组织档案保密管理的协同机制

为了解决跨组织档案保密管理的困境,企业需要从技术、制度和信任机制三个方面入手,构建有效的协同管理机制。

5.2.1 统一档案保密标准

企业应联合供应链上下游合作伙伴,共同制定统一的档案保密标准。这些标准应涵盖信息加密、访问控制、数据备份和安全审计等方面,确保所有企业在档案管理中遵循相同的安全规范。例如,通过制定统一的加密算法和数据格式标准,可以减少信息在跨组织传输过程中的安全风险。

5.2.2 建立协同管理平台

借助数字化技术,建立跨组织的档案保密管理平台是提升协同效率的重要手段。该平台应具备以下功能:一是信息共享与交互功能,支持供应链上下游企业之间安全地共享和更新档案信息;二是权限管理功能,根据不同用户的职责和权限,限制对敏感信息的访问;三是安全监控功能,实时监测平台上的信息访问和操作行为,及时发现并处理异常情况。

5.2.3 强化合作伙伴信任机制

信任是跨组织档案保密管理的基础。企业可以通过签订保密协议、建立信用评价体系和开展联合安全审计等方式,增强合作伙伴之间的信任。例如,通过定期的安全审计,确保各方遵守保密标准;通过信用评价体系,对违反保密协议的企业进行惩罚,从而提高合作伙伴的合规意识。

通过以上措施,企业可以有效解决跨组织档案保密管理的协同困境,提升供应链整体的信息安全水平。

6 结语

在数字化转型背景下,档案保密管理已成为物资供应链管理中的核心议题。通过对现有问题的深入分析和解决策略的制定,企业可以有效提升档案保密管理的水平,保障供应链的稳定运行。未来,随着技术的不断进步和管理制度的完善,档案保密管理将在信息安全保障中发挥更为重要的作用。企业应持续关注数字化技术的发展,积极探索新型技术的应用,并建立健全的管理机制,确保在数字化时代背景下的档案管理能够兼顾效率与安全,为企业的可持续发展奠定坚实的基础。

参考文献

- [1]王涛. 档案管理与信息安全研究[文献标识码]. 档案管理学刊, 2023, 45(2): 56-62
- [2]李明. 供应链管理中的档案保密问题探讨[文献标识码]. 企业管理, 2022, 34(3): 12-17
- [3]张华. 数字化背景下的档案保密管理策略分析[文献标识码]. 档案与建设, 2023, 39(4): 23-28