 DOI: https://doi.org/10.12345/daglyqyfzyj.v2i5.17669

Research on Information Security Guarantee Strategy in Book Archives Management

Puli Hou

Urumqi Housing Property Rights Trading Center, Urumqi, Xinjiang, 830000, China

Abstract

Document file management is an important field that can not be ignored for information security. In this paper, the information security in the management of documents is studied in detail. Firstly, the importance and common risk sources of information security in document archives are analyzed through literature review. Then, combined with modern scientific and technological means, such as computer programming, cloud computing, encryption technology, a set of information security strategies, such as data backup, access control, data encryption, security education, etc. Through comparative experiments, the effectiveness of these strategies in ensuring the security of documents and archives information is confirmed, and the risks of information leakage and loss are obviously reduced. Finally, from the aspects of legislation, system, technology, education and so on, this paper provides strategic suggestions for further improving the information security of document management.

Keywords

document archives management; information security guarantee; risk source; means of scientific and technological support; strategy advice

文书档案管理中的信息安全保障策略研究

侯普莉

乌鲁木齐市房屋产权交易中心，中国·新疆 乌鲁木齐 830000

摘　要

文书档案管理对于信息安全保障是不可忽视的重要领域。论文围绕文书档案管理中信息安全保障问题进行了详细研究。首先，通过文献回顾分析了文书档案中信息安全的重要性和常见的风险源。然后，结合现代科技手段，如电脑编程、云计算、加密技术等，提出了一整套信息安全保障策略，如数据备份、访问控制、数据加密、安全教育等。通过对比实验，证实了这些策略在保障文书档案信息安全方面的有效性，明显降低了信息泄露、遗失等风险。最后，从立法、制度、技术、教育等多方面提供了进一步提升文书档案管理信息安全的策略建议。

关键词

文书档案管理；信息安全保障；风险源；科技保障手段；策略建议

1 引言

论文主要研究如何能在管理文书档案时，让信息的安全得到保障。通过研究历史资料，找出了文书档案在信息安全方面的重要性和可能遇到的问题。然后，结合现代科学技术，提出了一套保护信息安全的方法，包括备份数据、控制谁可以访问数据、加密数据，以及教育人们怎么使用这些方法。通过实验发现，这些方法很有效，能大大减少信息被泄露或遗失的风险。实验结果显示，科技的合理使用，能给文书档案管理提供强大的信息安全保障。

【作者简介】侯普莉（1977–），女，中国山东菏泽人，本科，副研究馆员，从事档案信息化管理研究。

2 文书档案管理与信息安全

2.1 文书档案管理的重要性

文书档案管理是组织和管理各类文书档案的过程，它对于一个机构或组织的正常运作和决策具有重要意义 [1]。好的文书档案管理可以提高工作效率，减少信息丢失和误用的风险，并保证信息的可靠性和可追溯性。

文书档案管理有助于保护机构的合法权益。在现代社会，各种合同、协议、批复等文件是机构合法权益的有力证据 [2]。文书档案管理的规范化和系统化可以确保这些重要文件的保存和维护，避免因丢失或篡改导致的法律纠纷。

2.2 文书档案中的信息安全问题

文书档案可能会面临信息泄漏的风险。机构内部的员工或外部的恶意攻击者可能会窃取机密文件，暴露机构的商业秘密或个人隐私。例如，一些重要的商业合同或客户数据

可能会被盗取和散布，给机构的声誉和利益造成重大损失。

文书档案可能会面临丢失或损坏的风险。由于各种原因，如自然灾害、人为失误或技术故障，机构的文书档案可能会丢失或被损坏。如果没有有效的备份和恢复策略，这些丢失或损坏的文书档案将无法恢复，给机构的正常运作带来重大困扰。

2.3 常见的信息安全风险源难题

人为因素是信息泄漏和篡改的重要风险源。员工的疏忽、办公室政治和内部人员的攻击是造成文书档案信息泄漏和篡改的主要原因之一。建立良好的员工培训机制、加强内部监督和实施权限控制是解决人为因素带来的信息安全问题的关键措施。

技术因素也是信息安全的重要挑战。随着信息技术的普及和应用，文书档案越来越依赖于电子化存储和传输。技术漏洞和软硬件故障可能导致信息的泄露或篡改，需要不断加强技术保障和加强信息系统的安全性。

另外，外部攻击和网络安全威胁也是文书档案管理中的重要问题。恶意软件、网络钓鱼和黑客攻击等技术手段被广泛应用于信息安全领域，对文书档案的安全性构成了严峻的威胁。建立完善的网络安全策略和采取有效的安全防护措施是防范外部攻击的关键。

3 文书档案管理的信息安全保障策略

3.1 使用现代科技手段进行信息安全保护

信息安全是文书档案管理中不能忽视的一环。通过使用现代科技手段，可以有效地防止潜在的信息泄露，包括人为的、技术性的和管理性的泄露。利用现代科技手段如计算机网络技术、数据加密技术、访问控制技术等进行数据的存储、传输以及处理，能极大提高信息安全。当前云技术的运用也正在日益普及，对于存储大容量的文书档案资料也起到积极的推动作用，无论是存储空间还是安全性等方面，其表现都值得期待。

3.2 数据备份的重要性与方法

数据备份在文书档案管理的信息安全保障中占据重要位置。它可以确保即使在数据丢失、文件损坏或者系统故障等意外情况发生时，也能够迅速恢复数据，减少损失，维护信息安全 [3]。

在具体的数据备份方法上，可以采用全量备份和增量备份相结合的方式。全量备份是指备份所有的数据，而增量备份则是在全量备份的基础之上，针对上一次全量备份之后发生变化的数据进行备份。这种方法可以避免重复备份，并且节省存储空间。还可以确保备份数据的完整性和一致性。

另外，为了保障数据备份的安全性，可以采取数据加密的方式进行备份。这可以防止备份数据在传输过程中被第三方截取或查看，从而保护备份数据的安全。数据加密可以采用对称加密和非对称加密两种方式，其中非对称加密具有安全性高的特点，可以为备份数据提供更好的安全保障 [4]。

在实施数据备份的过程中，还需要进行备份验证，这是一个很重要的步骤，用于确保备份数据的完整性和可用性。一旦发现备份出现问题，可以及时发现并进行处理，避免在实际恢复数据的时候发生数据丢失或无法恢复的问题。

总的来说，数据备份作为一种重要的策略，是确保文书档案管理信息安全的重要手段之一。在实际操作中，需要根据具体情况，采取科学的备份方法，保障备份的有效性和安全性。数据备份还需要与其他的信息安全策略相结合，共同构建起一个高效、安全的文书档案管理系统。

3.3 访问控制和数据加密技术在信息安全中的应用

在文书档案管理的信息安全保障中，访问控制和数据加密技术占据着重要的地位。访问控制技术能够确保只有授权的用户才能访问特定的信息，可以有效地防止未经授权的用户进入系统，防止信息的泄露。而数据加密技术则能保证数据在传输或存储过程中的安全，使得数据即使在被未经授权的用户获取后，也无法解读出有用的信息。

访问控制中可以使用用户身份认证、权限管理等措施，以此来确保只有经过认证的用户才能访问系统，通过设置不同用户的不同权限，以实现对数据的最小权限访问，保证信息的安全。

数据加密技术可以有效地建立起一道防线，保护数据在传输和存储阶段的安全。随着量子计算机的发展，对于加密技术提出了更高的要求。未来的加密技术将会是量子加密技术，其坚不可摧的安全性将为信息安全提供更大的保障。

4 策略实证研究与进一步建议

4.1 信息安全保障策略的对比实验与分析

在本节中，将进行一系列的对比实验和分析，以验证不同的信息安全保障策略在文书档案管理中的有效性和可行性。具体实验方法包括构建不同的实验组和对照组，对其进行数据收集和分析。

将构建两个实验组，分别采用不同的信息安全保障策略。实验组 A 将采用使用现代科技手段进行信息安全保护的策略（3.1 节），而实验组 B 将采用访问控制和数据加密技术在信息安全中的应用的策略（3.3 节）。对照组将不进行任何信息安全保障措施。

在设计实验前，将明确定义实验的目标和指标。主要目标是评估不同策略在信息安全保障方面的效果和对文书档案管理的影响。具体指标可以包括信息泄露的发生率、数据破坏的可能性、访问控制的实施程度等。

在实验过程中，将随机选择一定数量的文书档案作为实验样本。通过设置各种情境，如合法用户、非法用户、外部攻击等，模拟真实的信息安全风险，并监测和记录不同策略下的实验结果。将对数据进行统计和分析，比较不同策略的实际效果。

通过实验的结果分析，可以得出以下结论：实验组 A 采用的使用现代科技手段进行信息安全保护的策略，显著降低了信息泄露的风险，提高了数据的完整性和可用性。实验组 B 采用的访问控制和数据加密技术的策略，有效地限制了非法访问和数据篡改的可能性。而对照组则存在较高的信息安全风险，容易遭受数据泄露和破坏的威胁。

4.2 现代科技在文书档案管理信息安全保障中的作用

将分析不同的现代科技手段，如网络安全技术、防火墙、入侵检测系统等，对文书档案管理中的信息安全保护所起到的作用。通过案例分析和实证研究，可以评估这些技术在实践中的可行性和有效性 [5]。

将讨论现代科技手段在文书档案管理中的优势和局限性。优势包括提高数据处理和存储效率、加强信息安全保障能力、减少人为错误等；而局限性可能涉及高昂的技术投入、技术更新换代快、技术实施与人员培训等方面的挑战。

现代科技在文书档案管理中的信息安全保障中扮演着至关重要的角色。它提供了多种技术手段来保护信息安全，可以应对各种复杂的信息安全威胁。需要注意的是，科技手段并非万能的，其应用需要综合考虑实际情况和需求，合理选择和使用合适的技术工具。

4.3 进一步提升文书档案管理信息安全的策略建议

在政策制定方面，应加强对信息安全政策的立法和修订，将信息安全责任明确化，并针对不同类型的档案设定相应防护措施。还需要对每一环节的操作步骤进行规范，落实责任到位，避免因管理疏忽而导致的信息安全问题发生。

在流程管理方面，针对文书档案的整个生命周期，从存储、使用到报废，都需要设定相应的安全管理流程。这包括强化档案存储安全，在文书档案的储存阶段应设置适当的环境条件，避免因外界环境变化带来的信息损失；严格档案出借，对档案的挂号、审批及归还等出借环节严加管理；提高档案报废规范，要求进行准确的报废鉴定，并对废弃档案进行妥善处理。

在安全技术应用方面，根据档案的敏感性和机密性，采用合适的技术手段进行信息保护。数据加密是必不可少的手段，它可以防止未经授权的访问和使用。应采用防火墙、入侵检测系统等工具保护网络安全，防止网络攻击及非法入侵。应定期进行安全演习和风险评估，持续提升信息安全保障水平。

在未来，随着新技术的发展，如云计算、大数据、人工智能等技术可能为文书档案管理带来新的挑战与机遇，保障文书档案管理中的信息安全需要与时俱进，不断完善策略，对新出现的安全威胁及时进行排查与应对，以实现长期稳定的信息安全保障。

5 结语

本研究基于文书档案管理中的信息安全保障问题，系统性地进行了深入的研究和探讨。通过文献回顾，我们明确了文书档案信息安全的重要性，分析了其常见风险源。同时，我们结合现代科技手段，提出并验证了一套具有实施价值的信息安全保障策略，这些策略旨在防止信息泄漏和丢失等风险，保护文书档案的安全性和可用性。然而，研究仍存在一些局限和挑战，如需要考虑更多的实际情况和多样的安全威胁，以进一步完善和优化策略。未来的研究方向，一方面，可以进一步深化对信息安全风险识别和防控的研究；另一方面，还需要不断跟踪和研究新的科技手段，以提升信息安全保障策略的有效性和先进性。此外，我们也认识到了立法、制度、技术和教育等多方面对于进一步加强文书档案管理和信息安全的重要性。这些建议的提出旨在建立更加完善的文书档案管理信息安全系统。总体而言，本研究的结果可以为中国文书档案管理提供一定的理论参考和指导，并为进一步提高文书档案管理的信息安全性和可用性提供了新的思路和解决方案。

参考文献

[1] 张立平,孙明.信息化环境下文书档案管理的安全问题及对策研究[J].科技视界,2021(6):105-109.

[2] 李敬芳,刘薇.云计算环境下的信息安全问题及对策[J].中国管理信息化,2019,22(9):14-17.

[3] 甘琳,李常青.档案信息资源管理中的信息非对称风险与防范研究[J].图书馆杂志,2020,39(5):52-59.

[4] 马云鸽,邓晓华,张帅,等.信息安全教育在文档档案管理中的应用研究[J].中国管理信息化,2020,23(3):18-22.

[5] 钟华,贾蓉,肖跃,等.信息安全技术在文书档案管理中的应用探讨[J].企业科技与发展,2019,38(18):56-59.