档案管理中的信息安全问题及应对策略研究

杨　丽
秦皇岛市交通运输综合行政执法支队　河北　秦皇岛　066000

摘　要：本文旨在研究档案管理中的信息安全问题及其应对策略。随着信息技术的迅猛发展，档案信息安全面临的挑战日益严峻，包括黑客攻击、病毒传播、数据泄露等。针对这些问题，本文深入分析了其原因，并提出了相应的应对策略。通过建立完善的安全管理制度、采用先进的技术手段、加强人员培训等措施，可以有效提高档案信息的安全性和可靠性，为组织的稳定运营提供有力保障。

关键词：档案管理；信息安全问题；应对策略

1 信息安全在档案管理中的重要性

信息安全在档案管理中的重要性不容忽视。随着信息技术的飞速发展，档案作为企业、组织、机构的重要信息资源，其安全性、保密性、完整性受到前所未有的挑战。信息安全不仅关乎档案的保存和管理，更直接影响到组织的运营和利益。确保档案信息安全是维护企业利益的关键。档案中往往包含着大量的商业机密、客户信息等敏感数据，一旦泄露或被篡改，将对企业的经济利益和声誉造成严重损害。因此，加强档案信息安全防护，能够有效地减少信息泄露风险，保护企业的核心利益。信息安全对于档案的长期保存也至关重要[1]。随着时间的推移，档案的保存环境、介质等都可能发生变化，导致档案损坏、丢失等问题。通过采取有效的信息安全措施，如数据备份、加密技术等，可以大大降低档案损坏或丢失的风险，确保档案的长期保存和利用。信息安全还关系到组织内部的决策和运营。档案作为决策的依据和参考，其真实性和可靠性对于组织的稳定运营至关重要。通过保障档案信息安全，可以确保决策者获得准确、完整的信息，进而做出科学、合理的决策。

2 档案管理中的信息安全问题分析

随着信息化程度的不断提高，档案信息不仅包括传统的纸质文件，还包括电子文件、数字档案等。这些档案信息在生成、传输、存储和利用等过程中，面临着多种安全威胁。首先，档案信息面临来自外部的攻击和威胁。黑客、恶意软件等攻击者利用各种手段，如网络钓鱼、恶意脚本、勒索软件等，对档案信息系统发起攻击，窃取、篡改或删除档案信息，导致信息泄露、损坏或丢失。此外，网络窃密和间谍活动也对档案信息安全构成严重威胁。其次，档案信息在内部管理过程中也存在安全隐患。同时，缺乏完善的安全管理制度和规范，也可能导致档案信息的安全风险增加。此外，档案信息的存储和传输过程中也存在安全问题。存储介质的不稳定、自然灾害等不可抗力因素可能导致档案信息的损坏或丢失。在传输过程中，如果没有采取加密等安全措施，档案信息可能遭受截获、窃取或篡改等安全威胁。

3 数据泄露风险

3.1 黑客攻击

数据泄露风险和黑客攻击是当今企业面临的主要信息安全威胁。随着信息技术的快速发展，企业的运营和决策越来越依赖于数据，因此数据的安全性对于企业的成功至关重要。数据泄露风险是指企业的敏感数据被非法获取或泄露的风险。这些敏感数据可能包括客户信息、员工个人信息、财务数据、商业机密等。黑客攻击是指黑客利用漏洞或恶意软件对企业网络和信息系统进行攻击，以窃取、篡改或删除数据和信息。黑客攻击可能来自内部人员、外部攻击者或组织，其目的可能是为了获取经济利益、破坏企业运营或进行间谍活动等。黑客攻击的手段多样，包括网络钓鱼、恶意脚本、勒索软件等，给企业带来巨大的安全风险。

3.2 病毒威胁

病毒威胁是当今企业面临的一种常见信息安全威胁。随着信息技术的广泛应用，病毒的传播速度和破坏力也在不断增强，给企业的正常运营和信息安全带来了严重威胁。病毒是一种恶意软件，能够在计算机系统内自我复制并传播，对计算机系统造成破坏或干扰。病毒可以通过电子邮件附件、网络下载、移动存储设备等多种途径传播，一旦感染病毒，轻则导致系统运行缓慢、数据损坏或丢失，重则导致整个系统瘫痪，甚至造成重要数据的泄露。病毒威胁对企业的影响是巨大的。病毒会导致企业的重要数据泄露或损坏，给企业带来不可估量的损失。病毒会导致企业网络和信息系统瘫痪，影响企业的正常运营和业务开展。病毒还会增加企业的维护

成本和时间成本，给企业带来不必要的经济负担[2]。

3.3 软硬件故障

软硬件故障是档案管理中常见的安全问题，它可能导致档案信息的损坏、丢失或无法访问，从而给组织带来严重的影响。软硬件故障可能由多种原因引起，例如硬件设备的老化、过载或损坏，软件系统的缺陷、漏洞或病毒感染，以及自然灾害、意外事故等不可抗力因素。这些故障可能导致档案信息无法正常读取、存储或传输，甚至导致整个档案管理系统的瘫痪。软硬件故障对档案管理的影响是多方面的。软硬件故障可能导致档案信息的损坏或丢失，从而影响档案的完整性和可用性。这可能对组织的运营和决策造成不利影响，甚至可能引发法律纠纷或责任问题。

3.4 管理问题

管理问题在档案管理中也是一个重要的安全问题，它可能导致档案信息的损坏、丢失或被非法访问，从而给组织带来严重的影响。管理问题可能由多种原因引起，例如管理制度不健全、管理流程不规范、管理人员缺乏经验或责任心不强等。这些问题可能导致档案信息的管理不善，例如档案的分类、存储、备份和利用等方面的不规范操作，从而引发安全漏洞和风险。管理问题对档案管理的影响是多方面的。管理问题可能导致档案信息的损坏或丢失，从而影响档案的完整性和可用性。这可能对组织的运营和决策造成不利影响，甚至可能引发法律纠纷或责任问题。管理问题还可能增加档案管理的成本和时间。由于管理流程不规范，组织可能需要投入更多的资源来纠正错误和弥补漏洞，例如重新整理档案、恢复丢失的数据等。这不仅增加了组织的运营成本，还可能影响档案的正常利用和服务。

4 档案管理中的信息安全应对策略

4.1 加密技术

通过对档案信息进行加密处理，可以确保未经授权的人员无法读取或篡改档案内容，从而防止敏感信息的泄露和损坏。加密技术采用特定的算法和密钥对档案信息进行加密，将其转换为无法识别的密文。只有持有正确密钥的人员才能够解密和访问档案内容。通过这种方式，即使档案信息在传输或存储过程中被截获或窃取，攻击者也无法轻易地获取其中的敏感信息。加密技术可以应用于档案信息的各个阶段。在档案的生成和传输阶段，可以采用端到端的加密方式，确保档案在传输过程中始终保持加密状态，防止途中被窃取或篡改。在档案的存储阶段，可以采用存储加密的方式，将档案信息加密后存储在介质中，防止未经授权的人员访问或篡改。还可以采用传输加密的方式，对档案信息在传输过程中的加密保护进行加强，提高档案信息的安全性。除了以上所述的加密技术，还可以采取其他安全措施来进一步加强档案管理中的信息安全。例如，建立完善的安全管理制度和规范，加强人员培训和教育，建立备份和恢复计划等。这些措施可以与加密技术相结合，形成多层次的安全防护体系，确保档案信息的安全性和完整性。

4.2 防火墙技术

防火墙是一种安全系统，用于阻止未经授权的访问和数据传输，从而保护网络和系统的安全。在档案管理中，防火墙技术可以用于保护档案服务器和网络设备，防止外部攻击和恶意软件的入侵。通过设置合理的防火墙规则，可以限制对档案服务器的访问权限，只允许经过授权的IP地址或用户进行访问。同时，防火墙还可以监控网络流量，对异常流量进行报警和阻断，防止病毒和恶意软件的传播[3]。除了防止外部攻击外，防火墙技术还可以用于防止内部人员未经授权的访问和数据泄露。通过设置相应的访问控制规则，可以限制内部人员对敏感档案的访问权限，确保只有经过授权的人员才能够访问相关档案。这样可以有效减少内部人员恶意或非恶意的数据泄露风险。

4.3 备份策略

在面对各种安全威胁和风险时，备份策略能够确保档案信息的可靠性和可用性，降低数据丢失的风险。备份策略的制定需要考虑多个方面，包括备份方式、备份频率、备份介质和存储方式等。备份方式可以分为全量备份和增量备份，根据档案的重要性和变化频率选择合适的备份方式。备份频率的设定也很关键，可以根据档案的重要性和变化频率来确定备份的周期。备份介质的选择也十分重要，可以选择可靠的存储设备，如硬盘、磁带等，确保备份数据的可靠存储。同时，还需要选择安全的存储环境，确保备份数据免受自然灾害和人为破坏的影响。在实施备份策略时，还需要注意备份数据的可用性和可恢复性。备份数据需要能够及时恢复，并且能够保证恢复的数据完整性和一致性。除了备份策略的制定和实施，组织还需要建立完善的数据恢复计划。数据恢复计划应该详细列出每一步的恢复步骤和操作指南，以便在数据丢失或损坏时能够快速恢复数据。

4.4 硬件保障

为了确保档案信息的可靠存储和顺利访问，组织需要提供稳定、可靠的硬件设备，并采取一系列的保障措施来确保硬件设备的正常运行和稳定性。首先，组织需要选择高品质的硬件设备，如可靠的存储设备、服务

器和网络设备等。这些设备需要具备高度的稳定性和可靠性，能够承受一定的工作压力和环境变化。同时，组织还需要根据实际需求选择合适的硬件配置，以满足档案信息的存储、处理和访问等需求。其次，组织需要建立完善的硬件维护和检修制度。定期对硬件设备进行检查、清洁、保养和维修，确保设备的正常运行和稳定性。对于关键的硬件设备，可以采取预防性维护措施，定期更换易损件和进行必要的升级改造，以减少设备故障的风险。此外，组织还需要建立硬件故障应急响应机制。一旦发生硬件故障，需要及时发现并采取措施进行修复，以减少故障对档案信息的影响。

4.5 管理措施

组织需要建立完善的安全管理制度和规范，明确档案信息的安全要求和操作规程。管理制度应包括档案的分类、存储、备份、访问控制等方面的规定，以确保档案信息的安全性和完整性。同时，组织还需要制定相应的安全操作规程，规范工作人员的操作行为，防止误操作或违规操作导致安全风险。通过开展安全培训、宣传活动等方式，提高工作人员对档案信息安全的认识和重视程度，增强其安全意识和责任心。同时，组织还需要定期进行安全检查和评估，及时发现和纠正管理问题，确保档案信息的安全管理得到有效执行。组织还需要建立有效的监督和考核机制。通过定期对档案信息的安全管理进行监督和检查，确保各项安全制度和规范得到执行和遵守。对于违反安全管理规定的行为，需要进行严肃处理和追责，以维护档案信息的安全性和可靠性。

5 档案管理中的信息安全评估和监管

5.1 评估档案信息安全风险

通过对档案信息安全进行全面评估，组织可以了解当前面临的安全风险和隐患，并采取相应的措施进行防范和应对。组织需要建立完善的信息安全评估体系。该体系应包括对档案信息面临的各种威胁、脆弱性和影响的全面分析，以便识别出潜在的安全风险。评估体系还需要考虑到档案信息的机密性、完整性和可用性需求，制定相应的评估标准和指标，以确保评估结果的准确性和可靠性。在评估档案信息安全风险时，组织需要采用多种方法和技术手段。这包括漏洞扫描、渗透测试、威胁模拟等，以便发现潜在的安全隐患和脆弱性。评估结果出来后，组织需要根据评估结果制定相应的安全措施和应对策略[4]。这包括加强安全防护、优化访问控制、完善备份和恢复计划等，以确保档案信息的安全性和可靠性。为了确保评估和监管工作的有效执行，组织需要建立完善的监督和考核机制。该机制应包括对评估和监管工作的定期检查、评估结果的问责和反馈等，以确保相关人员能够认真履行职责，提高档案信息的安全性。

5.2 制定档案信息安全标准和指南

通过制定统一的标准和指南，组织可以规范档案信息的安全管理，提高档案信息的安全性和可靠性。这包括分析档案信息的机密性、完整性和可用性需求，识别出潜在的安全风险和威胁，并根据实际情况制定相应的标准和指南。在制定档案信息安全标准和指南时，组织需要考虑多个方面。这包括档案信息的分类、存储、备份、传输和利用等方面的安全要求，以及安全管理制度、技术措施和人员培训等方面的规定。制定档案信息安全标准和指南后，组织需要将其落实到实际工作中。这包括加强档案信息的安全管理，优化安全技术措施，提高人员的安全意识和能力等。随着技术和威胁的不断变化，档案信息安全面临的挑战也在不断变化。因此，组织需要保持对安全标准和指南的持续关注和更新，以确保其始终能够反映当前的安全形势和要求。

结束语

总的来说，档案管理中的信息安全问题是一个复杂而重要的领域，需要组织给予足够的重视和投入。通过深入研究和实践探索，我们可以不断完善档案信息安全管理，为组织的稳定运营和发展提供有力保障。

参考文献

[1]张小红,李明霞,张宇红.档案管理中的信息安全问题及对策研究[J].信息学报,2021,40(3):89-95.

[2]陈志勇,杨雪明,李春平.档案管理中的信息安全问题及应对策略研究[J].数量经济技术经济研究,2021,38(1):56-63.

[3]王亚东,刘晓雷,王晓宇.档案管理中的信息安全问题及对策研究[J].科技创新导报,2021,18(2):76-80.

[4]张琳,孙文洁,李华.档案管理中的信息安全问题及应对策略研究[J].档案学通讯,2021,45(3):90-94.