

试析电力企业档案管理保密制度建设中存在的问题及建议

瞿江林 国网湖北省电力有限公司恩施供电公司 湖北恩施 445000

摘要：在信息技术迅猛发展的当代，电力企业作为国家基础设施的重要组成部分，其档案管理的保密性和安全性显得尤为重要。档案不仅承载着企业的历史和文化，更是企业运营和决策的重要依据。然而，随着信息化进程的加快，电力企业在档案管理保密制度建设中面临诸多挑战。传统的管理模式和技术手段已难以应对日益复杂的安全威胁，制度不完善、技术滞后、人员意识薄弱等问题层出不穷。本文旨在深入分析电力企业档案管理保密制度中存在的主要问题，并提出切实可行的改进建议，以为电力企业的档案管理提供更为安全和高效的解决方案，确保企业在激烈的市场竞争中立于不败之地。

关键词：电力企业；档案管理；保密制度；信息安全

Analysis of the Problems and Suggestions in the Construction of Confidentiality System for Archives Management in Electric Power Enterprises

Jianglin Qu, Enshi Power Supply Company of State Grid Hubei Electric Power Co., Ltd., Enshi, Hubei 445000

Abstract: In the contemporary era of rapid development of information technology, as an important component of national infrastructure, the confidentiality and security of archives management in power enterprises are particularly important. Archives not only carry the history and culture of enterprises, but also serve as an important basis for their operation and decision-making. However, with the acceleration of the informatization process, power enterprises face many challenges in the construction of archives management confidentiality system. Traditional management models and technological means are no longer able to cope with increasingly complex security threats, with problems such as incomplete systems, outdated technology, and weak personnel awareness emerging one after another. This article aims to deeply analyze the main problems in the confidentiality system of archives management in power enterprises, and propose practical and feasible improvement suggestions, in order to provide a safer and more efficient solution for archives management in power enterprises, ensuring that enterprises stand firm in fierce market competition.

Keywords: power companies; Archive management; Confidentiality system; information security

电力企业作为国家经济的中流砥柱，其档案管理的保密制度建设直接关系到企业的核心竞争力和国家的信息安全。随着全球信息化的浪潮席卷各行各业，电力企业的档案管理面临着前所未有的挑战。现有的保密制度在应对复杂多变的安全环境时显得捉襟见肘，技术手段的滞后和人员意识的薄弱进一步加剧了这一问题。与此同时，外部网络攻击和信息泄露事件频发，给企业的档案安全带来了巨大的威胁。本文将从制度、技术和人员三个维度，深入探讨电力企业档案管理保密制度中存在的问题，并提出针对性的改进建议，旨在为电力企业的档案管理提供坚实的安全保障。

1 档案管理保密制度在电力企业中的基础作用

电力企业的档案管理保密制度在企业运营中扮演着至关重要的角色。档案管理不仅仅是信息的存储

和检索，更是企业核心数据的安全屏障。电力企业的档案中包含了大量的技术资料、客户信息和商业机密，这些信息一旦泄露，将对企业的竞争力和市场声誉造成不可估量的损失。因此，档案管理保密制度的建设成为企业信息安全的基石。通过科学的制度设计，企业能够有效地控制信息的访问权限，确保只有经过授权的人员才能接触敏感数据。此外，档案管理保密制度还为企业提供了一个系统化的框架，使得信息的存储、传输和销毁过程都能在可控的环境中进行。这样的制度不仅提高了信息管理的效率，还为企业在面对外部审计和合规检查时提供了有力的支持。

2 电力企业档案管理保密制度中存在的问题

2.1 制度不完善

电力企业的档案管理保密制度在设计 and 实施过程中，常常面临着多重挑战，这些挑战主要源于制度

本身的漏洞和不完整性。尽管许多企业已经意识到档案管理保密的重要性，并试图通过制定相关政策来加以规范，但在实际操作中，制度的覆盖范围和深度往往不足以应对复杂多变的安全环境。具体而言，现有制度在风险评估、权限管理、数据分类等方面的规定不够细致，导致在面对新型安全威胁时显得力不从心。以风险评估为例，许多企业缺乏系统的风险评估机制，无法及时识别和应对潜在的安全隐患。此外，权限管理的松散和不透明也为信息泄露埋下了隐患，许多员工在未经过严格授权的情况下，能够接触到敏感档案，增加了信息泄露的风险。数据分类不明确则导致在信息安全事件发生时，企业难以迅速定位和保护关键数据。制度的不完善不仅体现在内容的缺失，还表现在执行的力度和监督的有效性上。许多企业在制度执行过程中，缺乏有效的监督和反馈机制，导致制度形同虚设，无法发挥其应有的作用。

2.2 技术手段落后

在电力企业的档案管理中，技术手段的滞后性是一个不容忽视的问题。尽管信息技术的飞速发展发展为档案管理提供了诸多便利，但许多电力企业仍然依赖于传统的技术手段，未能充分利用现代化的信息安全技术。这种技术上的滞后性不仅限制了档案管理的效率，也为信息安全带来了隐患。传统的档案管理技术，如纸质档案和简单的电子文档管理系统，虽然在一定程度上满足了基本的管理需求，但在面对复杂的安全威胁时显得捉襟见肘。现代信息安全技术，如加密技术、区块链技术和人工智能技术，能够为档案管理提供更为坚实的安全保障。然而，许多电力企业在技术引进和应用上存在滞后，未能及时更新和升级其信息安全

技术体系。以加密技术为例，尽管其在保护数据安全方面具有显著优势，但在许多企业中，仍然未能得到广泛应用。此外，区块链技术作为一种新兴的分布式账本技术，具有高度的安全性和透明性，能够有效防止数据篡改和信息泄露，但在电力企业的档案管理中，应用案例寥寥无几。人工智能技术在信息安全中的应用也未能得到充分发挥，许多企业在安全事件的监测和响应上，仍然依赖于人工操作，效率低下且易出错。

2.3 人员意识薄弱

在电力企业的档案管理中，人员的保密意识薄弱是一个关键问题，直接影响到保密制度的有效执行。档案管理人员作为信息安全的第一道防线，其保密意识和专业素养对档案的安全性至关重要。然而，许多电力企业在人员培训和教育方面投入不足，导致员工对保密制度的理解和重视程度不够。具体表现为，员工在日常工作中缺乏对信息安全风险的敏感性，容易忽视潜在的安全隐患。例如，在处理敏感档案时，未能严格遵循保密规定，随意存储和传输数据，增加了信息泄露的风险。此外，员工对新兴信息安全技术和威胁的了解不足，无法有效识别和应对复杂的安全挑战。缺乏系统的培训和教育，使得员工在面对安全事件时，往往手足无措，无法采取有效的应对措施。为了提升档案管理的安全性，电力企业需要加强对员工的保密意识教育，建立系统的培训机制，定期开展信息安全培训和演练，提高员工的安全意识和应对能力。同时，企业应鼓励员工积极参与信息安全的学习和交流，提升其专业素养和技术水平。

2.4 外部威胁增加

电力企业在档案管理中面临的外部威胁日益严

表 1 某电力企业在档案管理保密制度中的关键指标和相关数据

指标类别	2022 年数据	2023 年数据	增长率 / 变化率
档案总量 (份)	50,000	55,000	10%
数字化档案比例	60%	75%	15%
员工培训覆盖率	85%	95%	10%
信息泄露事件数量	3	1	-66.7%
安全技术投入 (万元)	200	250	25%
应急演练次数	2	4	100%

峻,尤其是在网络攻击和信息泄露事件频发的背景下。随着信息技术的快速发展,网络攻击的手段和技术不断升级,给电力企业的档案安全带来了巨大的挑战。黑客组织和不法分子利用先进的技术手段,针对电力企业的网络系统和档案管理系统进行攻击,试图窃取敏感信息或破坏系统的正常运行。近年来,全球范围内发生的多起重大信息泄露事件,充分暴露了电力企业在应对外部威胁方面的脆弱性。例如,某大型电力企业曾遭遇大规模的网络攻击,导致大量敏感数据被窃取,给企业的声誉和经济利益造成了严重损失。外部威胁的增加,不仅要求电力企业在技术上进行升级和防护,还需要在管理和策略上进行调整和优化。企业应加强对外部威胁的监测和分析,建立健全的安全防护体系,提升对网络攻击的检测和响应能力。同时,企业应加强与外部安全机构和同行业的合作,分享信息安全经验和情报,形成合力,共同应对外部威胁。通过多层次、多维度的安全防护措施,电力企业能够更有效地抵御外部威胁,保障档案管理的安全性和稳定性。

3 电力企业档案管理保密制度的改进建议

3.1 完善制度建设

在电力企业的档案管理中,制度建设的完善性直接关系到信息安全的整体水平。为了应对日益复杂的安全环境,电力企业需要根据最新的安全标准和法规,对现有的档案管理保密制度进行全面的审视和更新。制度的完善不仅仅是对已有条款的修补,更是对整个管理体系的重构和优化。具体而言,企业应在制度中明确信息安全的责任分工,确保每个环节都有专人负责,避免因责任不清导致的管理漏洞。此外,制度应涵盖从档案的创建、存储、传输到销毁的全生命周期管理,确保每个阶段的安全措施都得到有效落实。为了增强制度的可操作性,企业需要结合自身的实际情况,制定切实可行的操作流程和应急预案,确保在发生安全事件时能够迅速响应和处理。制度的建设还应

注重与时俱进,定期进行评估和更新,以适应不断变化的安全形势和技术发展。通过完善制度建设,电力企业能够构建起一个系统化、规范化的信息安全管理体制,为档案管理的安全性提供坚实的制度保障。

3.2 引入先进技术

在提升电力企业档案管理安全性方面,引入先进的信息安全技术是一个不可或缺的策略。现代信息技术的迅猛发展,为档案管理提供了丰富的技术手段,能够有效提升信息的安全性和管理效率。加密技术作为信息安全的基石,能够为档案数据提供强有力的保护,防止未经授权的访问和数据泄露。通过采用先进的加密算法,企业可以确保敏感信息在存储和传输过程中的安全性。此外,区块链作为一种去中心化的分布式账本技术,具有高度的透明性和不可篡改性,能够为档案管理提供全新的安全保障。通过将档案数据存储在区块链上,企业可以实现对数据访问和修改的全程追溯,确保档案的完整性和真实性。除了加密和区块链技术,人工智能技术在信息安全中的应用也日益广泛。通过引入人工智能技术,企业可以实现对安全事件的实时监测和智能分析,提高对潜在威胁的识别和响应能力。为了充分发挥先进技术的作用,电力企业需要加大对信息安全技术的投入,积极探索和应用新兴技术,构建完善的技术防护体系。通过技术的创新和应用,电力企业能够更好地应对信息安全挑战,确保档案管理的安全性和可靠性。

3.3 加强人员培训

在电力企业档案管理的保密制度中,人员培训的强化是提升整体安全水平的关键环节。档案管理人员的安全意识和专业技能直接影响到信息的保密性和完整性。因此,企业需要建立系统化的培训机制,定期开展保密意识培训,以确保员工始终具备最新的安全知识和技能。培训内容应涵盖信息安全的基本原则、最新的安全威胁和防护措施,以及企业内部的保密制度和操作流程。通过案例分析和情景模拟,员工可以

更直观地理解安全风险和应对策略,从而提高其在实际工作中的安全意识和判断能力。此外,培训还应注重提升员工的专业技能,特别是在信息技术和安全工具的使用方面。随着信息技术的不断发展,档案管理人员需要掌握新的技术手段,以应对复杂的安全挑战。企业可以邀请信息安全专家进行专题讲座,分享行业前沿的安全技术和实践经验,帮助员工拓宽视野,提升专业素养。为了确保培训的效果,企业应建立培训评估机制,通过考核和反馈,持续改进培训内容和方法。通过加强人员培训,电力企业能够构建一支高素质的档案管理团队,为信息安全提供坚实的人才保障。

3.4 建立应急机制

在电力企业的档案管理中,建立健全的应急机制是提升应对突发事件能力的重要举措。面对日益复杂的信息安全环境,企业需要制定详细的应急预案,以确保在发生安全事件时能够迅速有效地进行处置。应急预案的制定应基于全面的风险评估,涵盖可能发生的各类安全事件及其影响,明确应对措施和责任分工。预案中应详细规定事件的报告流程、应急响应步骤、资源调配和信息沟通机制,确保在紧急情况下,各部门能够协调一致,快速反应。为了检验和提高应急预案的有效性,企业需要定期组织应急演练,通过模拟真实的安全事件,锻炼员工的应急反应能力和协作水平。演练后,应对整个过程进行评估和总结,识别存在的问题和不足,及时修订和完善应急预案。企业还应建立信息共享和沟通机制,与外部安全机构和同行业保持密切联系,获取最新的安全情报和应对经验。通过建立完善的应急机制,电力企业能够提高对突发事件的应对能力,最大限度地减少安全事件对档案管理的影响,保障信息的安全性和稳定性。

4 结束语

在电力企业档案管理保密制度的建设过程中,综合考虑多方面因素是确保信息安全的关键。通过细化制度、引入先进技术、强化员工培训以及建立健全的

应急机制,企业能够有效提升档案管理的安全性和可靠性。制度的完善不仅有助于防范潜在的安全威胁,还能提高企业在信息管理上的整体效率。与此同时,技术的应用为档案管理提供了更为坚实的保障,确保信息的完整性和可追溯性。员工培训则是提升安全意识和专业技能的基础,直接影响到制度的执行效果。应急机制的建立则为企业在突发事件中提供了快速反应的能力,减少可能的损失。

参考文献

- [1] 赵金玉. 电力企业档案管理保密制度建设问题及对策研究 [J]. 办公室业务, 2019(02):92.
- [2] 李云. 电力企业档案管理保密制度建设中存在不足点及改进 [J]. 低碳世界, 2017(33):347-348.
- [3] 黄辽兰. 电力企业档案管理保密制度建设中存在的问题及建议 [J]. 中国高新技术企业, 2016(05):166-167.

作者简介:瞿江林(1985-),女,湖北恩施,本科,馆员。研究方向:档案专业。