企业档案保密与安全管理研究

蔡雅君
中国节能环保集团有限公司，北京 100082

摘要：随着信息技术的飞速发展和大数据时代的到来，企业档案管理的复杂性和重要性显著提升。企业档案不仅是企业内部信息资源的载体，也是企业核心竞争力的重要组成部分。然而，在档案数字化和信息化的背景下，档案的安全性和保密性问题日益突出。本文围绕企业档案的保密与安全管理，分析当前企业在档案保密管理中存在的问题，探讨新时期企业档案管理的策略及创新路径，为构建高效、安全的档案管理体系提供理论支持和实践参考。

关键词：企业档案；保密管理；安全管理；数字化；全过程管理

Research on Enterprise Archives Secrecy and Security Management

Cai,Yajun

China Energy Conservation & Environmental Protection Group (CECEP), Beijing, 100082, China

Abstract: With the rapid development of information technology and the arrival of the era of big data, the complexity and importance of enterprise file management have increased significantly. Enterprise archives are not only the carrier of internal information resources, but also an important part of the core competitiveness of enterprises. However, under the background of digitalization and informatization of archives, the security and confidentiality of archives are increasingly prominent. Focusing on the security and safety management of enterprise archives, this paper analyzes the problems existing in the current enterprise archives security management, discusses the strategies and innovative paths of enterprise archives management in the new period, and provides theoretical support and practical reference for building an efficient and safe archives management system.

Keywords: Enterprise files; Security management; Safety management; Digitization; Whole process management

DOI: 10.62639/sspis18.20250203

企业档案是企业经营活动的重要记录，涵盖了生产经营、技术研发、人力资源、财务管理等核心信息。这些档案不仅具有法律效力和参考价值，还与企业的核心利益息息相关。特别是在国家对保密工作的重视不断提升的背景下，档案的保密管理已然成为企业管理中的重要内容[1]。传统的档案管理模式由于信息化程度低、规章制度不完善，在新时期面临严峻挑战。因此，探索档案保密与安全管理的新模式，对于提升企业综合竞争力具有重要意义。

一、当前企业档案保密管理的现状与问题

（一）保密意识薄弱

在一些企业中，档案保密工作往往被视为次要任务，难以进入战略管理的核心范畴。领导层对此的轻视，使保密工作逐渐被边缘化，仅流于形式和合规化处理，未被融入整体安全管理框架。员工更是因缺乏教育和培训，难以真正意识到档案泄密可能带来的严重后果[2]。认知上的空白会在业务增长和效率优先的压力下愈加突出，导致企业常用牺牲档案管理精细化的方式换取即时收益。管理层和员工的疏忽，使档案保密成为一条随时可能断裂的薄弱链条，不但让企业在面对突发风险时手足无措，还可能在长期的惯性疏忽中积累隐患。

（二）制度体系不健全

大部分企业虽已制定档案管理制度，但这些制度多流于表面，缺乏可操作性和实用性。尤其在针对档案敏感级别和不同使用场景的管理上，常未形成明确细则，操作多靠员工个人经验执行。监督和考核的不足，使制度的执行力度严重受限，进一步加大违规操作的可能性。归档、调阅和销毁环节的漏洞，则让管理工作常常流于形式化操作[3]。此外，制度缺少动态调整机制，无法应对业务环境的快速变化，导致员工在新情境下无章可循。管理规则如果缺乏实效性，难以真正提升档案保密工作的效率和权威性。

（三）信息化建设滞后

管数字化已成为大势所趋，部分企业的档案管理仍滞留在传统的纸质模式，未能充分发挥现代技术的优势。这种技术空白让档案在存储、传输和使用环节都暴露于较高的泄密风险中。档案常依赖单一物理介质存储，缺乏分级加密和电子签章等核心安全技术的支撑，而传输过程中未施以权限控制，导致敏感信息更易被外部威胁所侵害。面对日益严峻的网络安全环境，这种技术滞后不仅削弱企业对档案保密的控制力，还可能在竞争中让企业陷入被动境地，更进一步拉低档案管理的效率和可控性。

（稿件编号：IS-25-3-1011）

作者简介：蔡雅君（1985-），性别：女，民族：汉，籍贯：天津，学历：硕士研究生，职称：高级经济师，研究方向：档案管理、保密管理、公文管理。

（四）管理责任不明确

档案保密管理的成效与责任分工是否清晰有直接联系，但许多企业在这一方面存在明显缺失。分级责任体系的不完善，使各部门在档案管理中责任模糊，甚至出现“责任无人区”。这种情况下，多个部门协作往往缺乏沟通与协调，使问题难以追踪归因。更严重的是，监督和考核机制的空缺，意味着即使发生失误，也难以追究相关责任[4]。档案保密工作的有效性，在这种混乱的管理格局下大打折扣，泄密隐患随之加剧。只有明确分工、清晰责任链条，并形成管理闭环，才能让保密措施在实际执行中具备真正的保障力。

二、企业档案保密与安全管理的创新策略

（一）从理念渗透到行为塑造，全面构建全员保密意识

企业档案的保密与安全管理是一项系统性工作，其成效取决于全体员工的共同参与，而非某些岗位的独立承担。然而，现实中部分员工往往对档案保密的严肃性认识不足，甚至将其视为与自身职责无关的事务。要改变这种现状，企业需要着眼于培养全员的保密意识，让保密观念真正融入员工的工作习惯与价值判断之中。一方面，企业可以组织案例分析会，从典型的失泄密事件出发，以直观、生动的方式向员工展示档案泄密的危害性，让他们感受到保密的重要性。另一方面，针对不同岗位的保密需求，设计有针对性的培训课程[5]。技术研发部门的人员需要了解数据保护和涉密技术文件的管理要点，而人力资源部门的员工则需掌握员工档案信息的风险控制方法。此外，借助线上学习平台或企业内部网络，开设保密知识微课和互动问答模块，让员工随时随地巩固保密技能。为了增强培训的吸引力，还可以结合情景模拟和沉浸式体验，让员工在实景中了解档案泄密的潜在风险，从而在思想深处树立起档案保密的底线意识。

在强化理念的同时，企业还需要在日常管理中不断渗透保密意识。在新员工入职培训中，可以将保密教育列为必修模块，详细讲解档案保密的原则和具体做法。每年定期举办保密知识竞赛或主题活动，以寓教于乐的方式激发员工的学习兴趣，并让他们对保密要求形成深刻记忆。此外，为了让保密意识不局限于培训室，可以在企业的办公区域设置醒目的保密提示标语，或者通过内网定期推送保密动态和知识点。对涉密岗位的员工，企业可以建立动态提醒机制，在其处理敏感信息时，系统自动弹出保密提示，提醒注意操作合规性。总之，构建全员保密意识并非一朝一夕之功，而是一个从理念渗透到行为塑造的长期过程。只有让保密成为每位员工的本能反应，档案管理的防线才能更加稳固。

（二）从顶层设计到精细落地，不断完善制度与流程

档案保密管理的有效性离不开完善的制度保障，然而，许多企业的管理制度存在内容笼统、针对性不足的问题，导致在实际操作中难以发挥应有的作用。要从根本上改变这种状况，企业需要从顶层设计出发，制定科学、细化的规章制度，将档案保密管理融入企业的整体管理体系。在制度层面，可以建立分级分类的档案管理办法，根据档案的敏感程度，明确其归档、流转、使用和销毁的具体要求。同时，针对涉密档案的全生命周期，设计详细的操作流程，将其固化为标准化的作业规范。对于跨部门协作的档案管理环节，企业应通过设置责任分工清单和操作指引，确保流程的每一步都有人负责且有据可依。此外，在档案管理制度的制定过程中，可以邀请各部门的业务骨干参与讨论，以充分吸收一线人员的实操经验，使制度更贴合实际需求。

在制度完善之后，执行环节往往决定了管理效果的最终呈现。为此，企业需要建立动态调整和定期检查机制，以应对制度在实际运作中的偏差和业务环境的变化。企业可定期组织档案管理流程的专项审查，通过现场走访和文件核查发现问题并及时整改。同时，设置定期考核制度，考察员工对制度执行的熟悉度和规范性，并将考核结果纳入绩效评价体系，以增强制度执行的刚性约束力。针对制度的宣传与更新，企业可以借助数字化手段，设立档案管理在线系统，及时推送最新的管理要求，并在关键节点对员工进行操作提醒。此外，为提高制度执行的透明度，还可引入第三方机构进行定期审计，以强化对档案管理工作的监督。这种从顶层设计到精细落地的制度建设方式，不仅能提升管理效率，还能在企业内部形成统一的保密文化氛围，推动档案保密管理朝着更高水平发展。

（三）技术赋能档案管理，推进数字化建设进程

数字化已经成为档案保密管理的必然趋势，其在提升效率的同时，也为安全性赋予了新的可能。然而，不少企业在推进数字化管理时，往往因缺乏整体规划或技术保障而停留在浅层次的电子化阶段，这使得数字化的优势未能充分显现。为了从根本上提升数字化管理水平，企业需要从系统建设和技术引入两个维度开展行动。首先，建立高效、可靠的档案管理信息系统是数字化管理的核心。该系统应具备档案归档、存储、查询、流转、销毁的全功能支持，并针对涉密档案设置多级权限控制。企业可以引入加密技术对档案数据进行分级存储，从而在最大程度上减少敏感信息的暴露面。其次，技术创新为档案管理提供了新的突破口，区块链技术以其去中心化和不可篡改的特性，为档案使用过程的全程记录提供了技术保障。这种透明且可追溯的管理方式不仅增强了档案管理的可信度，还能在档案使用出现问题时快速定位责任主体。此外，人工智能技术也可用于智能分类和敏感信息的自动检测，大幅度降低人工管理的工作量和误操作风险。在推进数字化的过程中，企业还需注重与现有系统的兼容性，

避免因技术割裂而影响管理效率。

然而，数字化管理的成功实施并非仅依赖技术手段。配套措施的完善是其顺利运行的前提条件。企业需要定期组织技术维护和系统更新，以防范因软件漏洞或老化硬件引发的安全问题。同时，在技术层面加强风险评估，确保数据加密、备份和容灾机制的完备性。为了提升员工对数字化系统的适应能力，企业还应设立专项培训，使员工能够熟练操作管理系统并掌握基本的技术维护技能。另一方面，针对档案管理信息系统的建设，企业可选择引入外部咨询机构，在系统架构、技术应用和实施策略等方面提供专业支持。通过技术驱动与制度支撑的双轮驱动，数字化管理才能真正成为提升档案保密管理水平的强有力工具。

（四）落实全过程管理，构筑档案保密的系统化防线

档案管理的有效性不仅依赖于某一环节的优化，更需要贯穿其生成、存储、使用、流转和销毁等全生命周期的全过程管理。然而，实践中很多企业在档案管理的不同阶段存在脱节现象，如生成阶段对敏感信息的识别不足，使用阶段权限控制不严，销毁阶段未采用安全可靠的方法。这种零散化管理方式显然无法匹配新时期对档案保密的高要求。因此，企业应从系统化角度出发，将全过程管理贯穿于档案管理的每一个环节。首先，在档案生成阶段，企业应建立分类分级机制，对档案的敏感程度进行精确识别并予以标注。存储阶段需严格执行分级存储策略，对于涉密档案设置独立的存储介质或网络环境，避免与普通档案混存。此外，在档案的流转和使用环节，应强化权限管理，采用动态监控技术实时追踪档案流转路径和使用记录，确保档案的安全性得到动态保护。

全过程管理的难点往往集中在销毁阶段，很多企业对此环节重视程度不足，导致泄密风险隐患显著增加。针对档案销毁环节，企业应优先采用专业化手段，对纸质档案进行粉碎处理并掺入其他废料，或对电子档案实施磁盘物理销毁和彻底数据擦除。这些措施能够有效降低信息复原的可能性。此外，销毁过程应严格按照事先制定的标准化流程进行，包括销毁审批、过程监督、结果核查等步骤，所有环节应留存记录以便后续审计。为了使全过程管理更加高效，企业可以引入自动化管理系统，将档案的全生命周期数据集成到一个平台上实现一体化管理，从而减少人为操作带来的疏漏。同时，定期组织档案管理的专项审查，对每个环节进行全面检查和优化，以动态调整管理策略并适应业务环境的变化。全过程管理的关键在于系统思维的落地，通过细致、全面的管理措施构建一条环环相扣的保密链条，才能真正使档案安全管理实现闭环，进而为企业发展保驾护航。

（五）强化涉密人员与载体管理，人机协同构建安全屏障

涉密档案的管理高度依赖人员的职业素养与载体的物理安全，这两者的协同管理直接影响档案保密工作的成效。在人员管理方面，涉密岗位的特性决定了选任过程必须严谨细致，企业应当制定涉密人员的筛选标准，从政治觉悟、职业道德到履职能力进行全面考察，避免不适合的人员进入关键岗位。背景审查可以细化为阶段性核查，包括入职前的详尽背景调查和定期的履职状况评估，以实时掌握人员的风险变化。同时，建立动态的考核制度，让涉密人员对其保密责任始终保持清醒认知。企业需要定期组织涉密人员参与保密知识测试或案例讨论，在日常工作中通过情景模拟检验其应对突发事件的能力。对涉密行为的失误应采取惩戒和教育并重的方式，从制度上加以纠正，并从心理层面强化涉密人员对失泄密后果的认知。

在载体管理方面，企业需要强化从存储环境到使用流程的全方位保护。档案库房应设置在远离公共区域的独立空间，并配备监控系统、身份识别门禁等安全措施，防止未经授权的人员进入。对于数字化涉密载体，企业可以部署分级防火墙和数据加密技术，以提高档案存储与传输过程中的安全性。此外，涉密载体的全生命周期管理应涵盖备案、流转、回收和销毁等环节，逐步建立一套闭环式的监督机制。在使用涉密载体时，必须严格限制使用范围，归还后及时核对内容完整性，并对操作记录进行保存以备审查。对于存储介质的报废处理，应采用物理销毁或彻底抹除技术，避免因废弃设备的恢复性操作造成泄密隐患。通过在人机协同管理中细化措施，企业可显著提升涉密档案管理的安全等级。

三、结语

企业档案保密与安全管理不仅是企业内部管理的重要组成部分，更是提升企业核心竞争力的基础保障。在大数据时代，档案管理需要从传统模式向信息化、智能化转型，构建全方位的保密与安全管理体系。通过完善制度、强化技术应用、提升员工意识，企业能够有效规避档案管理中的风险，确保信息资源的安全与可控，为企业的可持续发展提供坚实支撑。

参考文献：

[1] 杜悠．大数据背景下如何加强企业档案信息化保密管理[J]．兰台内外，2024，(26)：10-12.
[2] 冯雪．发电企业优化档案开发利用与保密工作的实践路径[J]．办公室业务，2024，(14)：89-91.
[3] 陈艳艳，何秋英．档案保密技术防范问题与对策研究——以广州地铁集团为例[J]．兰台内外，2019，(22)：73-74.
[4] 张丽．大数据时代下加强企业档案信息化保密管理的有效策略[J]．中国管理信息化，2021，24（14）：172-173.
[5] 吕春燕．试析企业档案管理保密工作的重要性及相关对策[J]．办公室业务，2020，(03)：106+108.