档案管理的安全保密及信息化档案管理探讨

董　茁

潍坊市潍城区公路事业发展中心　山东　潍坊　261021

摘　要：数字化时代下，档案信息化建设成为行业发展必然趋势，同时也对档案安全保密管理提出全新挑战。本文立足档案全生命周期管理视角，阐释档案安全保密与信息化管理的核心内涵、特征及内在关联，剖析当前制度体系、技术防护、人才建设、流程规范等方面的突出问题，针对性提出制度完善、技术升级、人才培育、流程标准化等优化策略，旨在实现档案高效利用与安全保密的有机统一，推动新时代档案管理高质量发展。

关键词：档案管理；安全保密；信息化档案管理

引言：随着数字技术、网络技术的广泛普及，传统纸质档案管理模式逐步向数字化、智能化信息化档案管理转型，极大提升了档案管理与利用效率。但信息化转型过程中，电子档案易泄露、易篡改、风险多元化等问题凸显，安全保密管控压力持续增大。安全保密是档案管理的核心底线，信息化是档案管理升级的重要支撑，二者协同发展至关重要。基于此，本文结合当下档案管理现状，探析现存问题并提出优化路径，为档案信息化安全管控提供实践参考。

1 档案管理安全保密与信息化管理核心概述

1.1 档案安全保密管理核心内涵与要求

（1）档案安全保密的核心内涵：档案安全保密的核心在于确保实体档案与电子档案在管理全过程中的信息完整、真实、不泄露、不丢失。既要维护物理载体的安全可控，更要保障数据内容的准确可靠，切实维护档案作为原始凭证的法定效力与可信度，其贯穿档案从形成到销毁的整个生命周期[1]。（2）档案安全保密的基本准则：严格遵循全程保密、分级管控、权责对应、安全可控四项基本准则。全程保密强调保密措施贯穿档案流转各环节；分级管控要求依据密级差异实施针对性保护策略；权责对应确保各岗位保密职责清晰明确；安全可控要求技术与管理手段协同保障，四者相互支撑，构成完整的管理准则体系。（3）档案保密分级管理要求：依据国家保密法规，将档案划分为绝密、机密、秘密三个等级，分别制定差异化的存储环境、传输渠道、借阅审批及销毁程序等管控标准。高密级档案实行从严管控，低密级档案实行规范管理，形成层次分明、重点突出的分级保护格局。

1.2 信息化档案管理的概念与特征

（1）信息化档案管理的定义：信息化档案管理是以计算机技术、网络技术和数据库技术为核心驱动，实现档案从采集、存储、检索、利用到归档全流程数字化、网络化与智能化的新型管理模式，是档案工作适应时代发展的重要转型方向。（2）信息化档案管理的核心特征：主要表现为存储数字化、传输网络化、利用便捷化、管理智能化及风险多元化五大特征。数字化与网络化极大提升了档案流转效率，智能化赋能自动分类与语义检索，但也使档案面临网络攻击、系统故障等多元风险，对安全防护提出更高要求。

1.3 安全保密与信息化档案管理的关联性

（1）安全保密是信息化档案管理的核心底线。无论技术手段如何升级迭代，保障数字化档案资源的合规存续、合法利用与安全可控始终是不可逾越的根本前提，是信息化管理不可动摇的基石。（2）信息化建设为档案安全保密管理提供技术支撑。加密存储、权限控制、操作审计、态势感知等数字化手段，显著提升了保密管控的高效性与精准性，使安全管理从被动应对转向主动防御。（3）二者协同发展是新时代档案管理高质量发展的必然趋势。需将安全保密理念深度嵌入信息化系统架构设计之中，以技术驱动安全升级，以安全保障技术应用，在互动共进中实现档案资源高效利用与合规管控的有机统一。

2 现阶段档案安全保密及信息化管理存在的问题

2.1 档案安全保密管理制度体系不完善

（1）制度适配性不足。现行保密管理制度大多基于传统纸质档案管理模式制定，对电子档案易复制、易传播、难追溯等特性缺乏充分考量，难以有效覆盖电子档案生成、流转、存储及网络归档等新型管理场景。

制度更新明显滞后于信息化发展速度，导致数字化各环节缺乏明确的操作规范与约束依据，管理随意性较大。（2）权责划分不清晰。档案管理部门、保密工作机构与信息技术管理部门之间存在职能交叉与管理盲区并存的现象。各方在档案数据安全管控中的具体职责界定模糊，遇有涉及档案信息安全管理的综合性事务时，容易出现推诿扯皮，形成保密管控的薄弱环节与真空地带[2]。（3）监督考核机制缺失。常态化保密监督检查与绩效考核体系尚未全面建立，对档案管理各环节的安全合规情况缺乏定期评估与动态监测。违规操作行为难以及时发现和有效约束，问责追责缺乏明确制度依据与处理程序，管理执行力与约束力大打折扣。

2.2 信息化档案安全技术防护能力薄弱

（1）基础防护设施老旧。部分档案管理系统配备的防火墙、入侵检测、数据加密及灾备恢复等基础安全设施建设年代较早，技术性能已难以应对当前复杂网络安全形势。系统升级迭代滞后，安全漏洞修补不及时，易出现数据泄露、损毁或永久丢失等安全事故。（2）数据管控技术不足。针对电子档案的防篡改认证、数字摘要验证、操作行为溯源及敏感信息自动脱敏等关键技术手段应用不够充分，档案数据从生成到销毁的全生命周期过程管控能力较弱，完整性与真实性难以得到持续有效的技术保障。（3）网络安全风险突出。档案数据在网络传输、跨系统交换及云端存储过程中面临病毒攻击、非法访问、数据截获篡改等多元安全威胁。部分单位尚未建立完善的网络安全监测预警与应急处置机制，安全风险防控整体处于被动应对状态。

2.3 档案管理专业人才素养有待提升

（1）传统档案管理人员对信息化管理工具和数字档案系统的操作能力明显不足，难以胜任数字化采集加工、智能检索应用及系统日常运维等新型业务需求，技能结构转型进展缓慢，知识更新滞后。（2）部分从业人员保密安全意识较为薄弱，存在未授权传输档案数据、使用非专用设备处理涉密信息、违规复制或外发电子档案等风险行为，人为因素已成为档案安全的重要隐患来源。（3）兼具档案专业素养、保密法规知识及信息技术能力的复合型人才严重匮乏。人才引进渠道不畅、在职培养体系不健全，难以有效支撑档案信息化与安全保密协同发展的现实需要，人才结构性矛盾突出。

2.4 档案信息化建设规范化程度不足

（1）档案数字化标准不统一。不同部门、不同业务系统之间在归档格式、元数据规范、存储结构及命名规则等方面缺乏一致性的执行标准，导致档案数据异构问题突出，既不利于信息资源共享，也增加了统一安全管控的难度与运行成本。（2）电子档案业务流程不规范。电子档案的归档移交、借阅审批、鉴定销毁等关键业务流程尚未形成系统化、标准化的操作规范，部分环节存在流程缺失或执行偏差。流程漏洞客观存在，容易引发档案信息泄露、数据资产流失等保密安全问题。（3）信息化系统互操作性不足。各业务系统之间缺乏统一的数据接口与交换标准，档案信息在跨平台流转过程中容易出现格式转换失真与安全管控脱节现象，制约了档案资源的高效整合与协同管理。

3 安全保密视域下信息化档案管理优化策略

3.1 健全档案安全保密管理制度体系

（1）完善适配信息化场景的保密制度。立足电子档案全生命周期管理需求，系统梳理档案在生成、流转、存储、利用及销毁各关键节点的保密风险与控制要求，逐项细化具有可操作性的管理规范与技术标准。针对电子档案易复制、易传播、难追溯等特性，补充完善网络归档审批、远程利用授权、移动存储介质管控等新型场景的制度约束。对与信息化实践明显脱节的陈旧条款及时修订或废止，对制度尚未覆盖的空白领域加紧补齐规则短板，确保制度供给与业务发展保持同步协调。（2）明确各部门各岗位保密权责。依据现行保密法律法规与单位组织架构，科学界定档案管理部门、保密工作机构及信息技术部门的职能边界与协同关系，清晰划分各层级在档案数据安全管控中的具体职责。建立分级负责、层层传导、逐级落实的保密责任体系，将保密义务精确分解到每个单位、每个岗位和每名人员，形成分工明确、衔接顺畅、上下贯通的权责链条，杜绝推诿扯皮与管理盲区[3]。（3）构建常态化监督考核与追责机制。建立定期保密专项检查与随机动态抽查相结合的常态化监督制度，将保密工作绩效全面纳入年度考核评价指标体系，实行量化打分与等级评定。对检查发现的问题实行台账管理、限期整改与闭环销号，明确违规行为认定标准与分级处理程序，强化问责追责的刚性约束力，切实增强制度的执行效力与警示震慑作用。

3.2 强化信息化档案安全技术防护体系建设

（1）升级基础安全防护设施。加大档案信息化安全基础设施投入力度，优化档案管理系统整体技术架构，统筹部署高性能网络防火墙、入侵检测系统、强效数据加密模块及异地容灾备份体系。定期开展信息安全漏洞检测与防护能力综合评估，对发现的安全隐患及时整改加固，持续夯实档案信息系统的安全运行环境与数据保

障能力。（2）应用智能安全技术。积极引入电子档案溯源标记、数字摘要防篡改认证、操作行为审计追踪及敏感信息智能识别与自动脱敏等先进技术手段，实现对档案数据生成、修改、访问、迁移及销毁等操作行为的全链条动态管控。通过技术赋能有效保障档案内容的原始性、真实性与完整性，提升对内部违规操作与外部恶意攻击的双重防御能力。（3）搭建网络安全防护体系。围绕档案数据传输与云端存储两大核心环节，建立健全网络访问控制、数据加密传输、入侵检测预警及安全态势感知等综合防护机制。制定完善网络安全事件应急预案，定期组织实战化攻防演练，切实提高对病毒攻击、非法入侵、数据截获篡改等突发安全事件的主动防御能力与快速响应水平[4]。

3.3 打造高素质复合型档案管理人才队伍

（1）开展常态化专项培训。制定覆盖全员、分层实施的年度培训计划，围绕档案保密法规深度解读、数字档案系统操作实务、网络安全防护技能训练等核心内容，灵活采用专题讲座、案例研讨、上机实操与岗位练兵等多种形式，确保培训的系统性、针对性与实效性持续提升，切实提高从业人员信息化素养与保密业务能力。（2）强化从业人员安全保密意识。定期组织保密警示教育、典型泄密案例通报及失泄密风险深度剖析等活动，引导全员深刻认识档案安全的极端重要性与现实紧迫性。将保密纪律要求融入日常管理与绩效考核，对违规传输、随意复制、私自外带档案数据等高风险行为实行零容忍，坚决杜绝因人为疏忽或主观违规引发的安全事件。（3）完善人才引进与培养机制。拓宽复合型人才引进渠道，优先吸纳具备档案学、保密管理、信息技术等多学科专业背景的优秀人才。建立在职人员继续教育与职业发展支持体系，通过定向委培、岗位轮训、院校合作及学术交流等多元途径，持续优化人才知识结构与能力层次，充实后备力量储备，为档案信息化与安全保密协同发展提供坚实智力保障。

3.4 规范档案信息化全流程管理标准

（1）统一档案数字化归档与存储标准。深入调研各业务部门档案管理现状与需求，制定覆盖各类档案门类的数字化格式规范、元数据描述标准、存储目录结构与命名规则，推动不同部门、不同系统之间档案资源的统一化、一致性管理。通过标准化建设消除数据异构障碍，为档案信息资源共享共用与统一安全管控创造坚实前提。（2）优化电子档案全流程权限管控机制。针对电子档案借阅、利用与销毁等关键业务环节，建立基于用户角色的分级授权审批制度，严格遵循最小必要权限分配原则。健全利用行为审计日志体系，确保每一次访问操作留有完整记录、可追溯核查，定期开展权限合规性审查，及时清理冗余账号与过期权限，切实杜绝越权访问与信息外泄等安全隐患[5]。（3）建立档案信息化动态管理机制。紧密跟踪信息技术迭代更新与政策法规调整变化，建立管理标准与操作规程的动态修订与及时发布机制。定期对现有管控流程的合规性与运行有效性进行系统评估，结合评估结果与技术发展前沿，持续优化管理流程与控制措施，确保各项管理工作始终保持安全、规范、高效的运行状态。

结束语

综上所述，档案安全保密与信息化建设相辅相成、密不可分，是新时代档案管理工作的两大核心重点。当前档案信息化管理仍存在制度、技术、人才、规范等多重短板，制约档案管理提质增效。唯有立足安全底线，持续完善保密管理制度、升级安全防护技术、培育复合型人才、规范全流程管理标准，才能化解信息化转型中的安全风险，筑牢档案安全防线，充分发挥档案资源的凭证价值与利用价值，助力档案事业长效稳健发展。

参考文献

[1] 李冬杰. 加强档案管理的安全保密及信息化档案管理 [J]. 电子元器件与信息技术,2024,8(11):227-229.

[2] 杨智勇, 桑梦瑶, 李华莹. 档案工作数字化转型的驱动因素和推进路径探析 [J]. 档案学通讯,2024,11(05):22-30.

[3] 王璐. 大数据时代背景下档案数字化安全管理与隐私保护研究 [J]. 中国管理信息化,2025,28(16):203-205.

[4] 金波, 杨鹏. 数字档案馆安全风险演化机理与防控体系研究 [J]. 图书情报工作,2023,67(14):45-53.

[5] 刘嘉铭. 数字化时代电子档案保密管理研究 [J]. 中国管理信息化,2025,28(12):150-152.