

档案管理数字化转型中的数据安全保障策略

赵波

宁波知行物联科技有限公司 浙江 宁波 315000

摘要: 档案管理数字化转型中, 数据安全保障需多维度发力。技术上, 构建分层防御体系, 利用区块链存证溯源, 借助AI分析威胁情报; 管理上, 制定分级分类制度, 建立“三员分立”体系, 完善全生命周期管控流程; 法律上, 对比国内外法规, 构建合规框架, 明确跨境数据流动路径; 人员上, 强化安全意识培训, 培养复合型人才, 建立外包监管机制, 全方位筑牢档案数据安全防护线。

关键词: 档案管理; 数字化转型; 数据安全; 保障策略

引言: 在数字化浪潮席卷下, 档案管理正加速向数字化转型。这一转变极大提升了管理效率与资源利用价值, 却也使档案数据面临前所未有的安全挑战, 数据泄露、篡改、合规冲突等问题频发。数据作为档案核心资产, 其安全关乎个人隐私、机构运营乃至国家安全。在此背景下, 探索档案管理数字化转型中切实可行的数据安全保障策略, 成为保障档案事业可持续发展的关键所在。

1 档案管理数字化转型的现状与安全风险

1.1 数字化转型特征

(1) 电子档案占比提升与全生命周期管理: 随着数字化进程加快, 电子档案在档案总量中占比持续攀升, 逐步替代传统纸质档案成为主流。同时, 档案管理模式从分散式存储转向全生命周期管理, 覆盖档案收集、整理、归档、保管、利用等各环节, 实现从产生到销毁的全程数字化管控, 提升管理效率与精准度。(2) 云计算、大数据、AI技术的深度应用: 云计算为档案存储提供弹性空间, 降低硬件成本; 大数据技术可挖掘档案数据价值, 辅助决策; AI技术则赋能档案分类、检索, 如智能识别档案内容自动归类, 大幅缩短检索时间, 推动档案管理从“被动保管”向“主动服务”转型。(3) 跨机构、跨区域档案资源共享趋势: 打破传统档案管理的地域与部门壁垒, 通过搭建统一数字化平台, 实现跨机构(如政府部门间)、跨区域(如不同省市档案馆)的档案资源互联互通, 满足公众、企业等对档案查询的跨场景需求, 提升档案资源利用价值^[1]。

1.2 典型数据安全风险分析

(1) 技术层面: 数据泄露、篡改、丢失风险突出, 勒索软件攻击频发, 攻击者通过加密档案数据索要赎金, 导致档案无法正常访问; 同时, 系统漏洞、传输加密不足等问题, 也可能造成档案数据被非法获取或篡改, 破坏档案完整性。(2) 管理层面: 存在权限失控问

题, 部分人员超权限访问敏感档案; 操作留痕缺失, 难以追溯异常操作源头; 应急响应滞后, 面对安全事件时无法及时处置, 加剧数据安全风险。(3) 法律层面: 合规风险显著, 国内外数据监管法规(如GDPR、我国《档案法》)要求存在差异, 跨国、跨区域档案管理易出现合规冲突, 若未做好衔接, 可能面临法律处罚。(4) 社会层面: 公众对档案数据隐私的信任危机加剧, 近年来档案数据泄露事件频发, 导致公众对档案管理机构的数

2 数据安全保障的理论基础与技术框架

2.1 理论基础

(1) 信息安全三元论: 作为数据安全核心理论, 保密性通过加密等手段防止档案数据被未授权访问; 完整性确保档案在存储、传输中不被篡改, 维持原始状态; 可用性保障授权用户在需要时能正常获取、使用档案数据, 三者共同构成档案数据安全的基础防线。(2) 动态安全模型: 突破传统静态防护局限, P2DR模型以安全策略为指导, 通过防护措施(如防火墙)抵御风险, 借助检测技术(如入侵检测系统)实时监控异常, 再以快速响应机制处置安全事件, 形成动态闭环, 适配档案管理中持续变化的安全需求。(3) 零信任架构在档案管理中的适应性: 秉持“永不信任, 始终验证”理念, 打破传统网络边界信任模式。针对档案管理中跨机构共享、多用户访问场景, 零信任通过持续身份验证、最小权限分配, 避免内部越权与外部入侵风险, 适配档案数据多场景流转的安全需求。

2.2 关键技术体系

(1) 数据加密技术: 同态加密支持在加密状态下对档案数据运算, 保障数据处理时的安全性; 量子加密凭借量子不可克隆特性, 实现绝对安全的密钥传输, 为高敏感档案(如涉密档案)提供长期安全保障, 应用前景

广阔。(2)访问控制技术:基于属性的加密(ABE)可根据用户属性(如职位、权限等级)动态分配档案访问权限;区块链权限管理利用分布式账本记录权限变更,确保权限分配透明可追溯,强化档案访问管控。(3)数据脱敏技术:静态脱敏适用于非实时场景(如档案数据备份),对敏感信息永久替换;动态脱敏针对实时查询(如公众查档),按需隐藏敏感字段,实现场景化安全防护。(4)审计追踪技术:区块链不可篡改日志完整记录档案操作行为,防止日志被篡改;AI异常检测通过分析操作模式,实时识别异常行为(如批量下载档案),提升审计精准度。(5)灾备恢复技术:采用云灾备与本地备份协同策略,本地备份保障快速恢复核心档案,云灾备实现异地数据冗余存储,应对自然灾害、硬件故障等极端情况,确保档案数据不丢失^[2]。

3 档案管理数字化转型中的数据安全保障策略

3.1 技术防护策略

(1)构建分层防御体系:网络层部署下一代防火墙、入侵防御系统,阻断非法访问与恶意攻击;系统层通过操作系统加固、漏洞定期扫描,降低系统安全隐患;应用层实施代码审计、接口加密,防范SQL注入、跨站脚本等应用层攻击;数据层采用加密存储、脱敏处理,从源头保障档案数据安全,形成多层联动、纵深防御的技术屏障。(2)区块链技术在档案存证与溯源中的应用:利用区块链分布式账本与不可篡改特性,将档案的创建时间、修改记录、访问痕迹等关键信息上链存证,确保档案溯源的真实性与可靠性;针对电子档案易被篡改的问题,通过区块链哈希值校验,实时验证档案完整性,为档案确权、纠纷溯源提供技术支撑。(3)AI驱动的威胁情报分析与主动防御机制:依托AI算法对档案管理系统的访问日志、网络流量、操作行为进行实时分析,构建威胁情报模型,精准识别异常行为(如非授权批量下载、异常IP访问);同时,基于历史威胁数据进行预测,提前部署防御策略,变“被动响应”为“主动防御”,提升对未知安全威胁的应对能力。

3.2 管理保障策略

(1)制定数据安全分级分类管理制度:根据档案数据的敏感程度(如涉密档案、个人信息档案、普通公开档案)与重要性,划分安全等级(如一级至五级),针对不同等级制定差异化管控措施,例如涉密档案实施最高级别的加密存储与专人管控,普通公开档案则简化访问流程,实现“精准防护、分级管控”。(2)建立“三员分立”安全管理体系:明确三员职责边界,系统管理员负责系统运维与权限配置,安全审计员负责监督操

作行为与日志审计,安全保密员负责涉密档案的保密管理,形成“运维-监督-保密”相互制衡的管理机制,避免单一角色权限过大导致的安全风险。(3)完善档案数据全生命周期安全管控流程:在档案收集阶段,对源头数据进行安全校验与合规审查;存储阶段实施加密备份与容灾部署;利用阶段通过动态脱敏、权限管控限制数据使用范围;销毁阶段采用物理粉碎(纸质档案)、数据擦除(电子档案)等方式,确保档案数据全流程无安全漏洞^[3]。

3.3 法律合规策略

(1)国内外档案数据安全法规对比分析:梳理国内《档案法》《数据安全法》《个人信息保护法》与国际GDPR、ISO27001等法规标准的差异,重点分析数据收集、存储、跨境传输等环节的合规要求,例如GDPR对个人数据跨境的“充分性认定”与国内“安全评估”的衔接要点,为跨国、跨区域档案管理提供合规参考^[4]。

(2)构建符合等保2.0的档案系统安全框架:以网络安全等级保护2.0标准为依据,从物理环境、网络架构、数据安全、应急响应等方面,搭建档案管理系统的安全合规框架,例如满足等保2.0中“三级系统”的访问控制、日志审计、数据备份等要求,确保系统通过等保测评。

(3)跨境档案数据流动的合规路径设计:针对跨境档案数据(如跨国企业档案、国际合作项目档案),建立“事前评估-事中管控-事后追溯”的合规流程,事前开展数据出境安全评估与个人信息影响评估,事中采用加密传输、本地化存储等措施,事后留存数据流动日志,确保符合国内外数据跨境监管要求。

3.4 人员能力建设策略

(1)档案人员数据安全意识培训体系:制定分层培训计划,对普通档案人员开展数据安全基础知识(如密码管理、钓鱼邮件识别)培训,对管理人员开展安全策略与应急处置培训;采用案例教学、模拟演练等形式,定期组织培训考核,强化人员“数据安全无小事”的责任意识,减少因人为操作失误导致的安全风险。(2)复合型人才培养模式:联合高校、科研机构开设“档案学-信息安全”交叉学科课程,培养既掌握档案整理、编目等专业技能,又熟悉数据加密、网络安全等技术的复合型人才;同时,鼓励在职人员参加信息安全工程师、注册档案师等职业资格考试,提升专业能力,满足数字化转型对人才的多元化需求。(3)建立安全运维外包服务监管机制:对于外包的档案系统运维、数据备份等服务,明确外包服务商的安全责任与服务标准,签订保密协议与安全承诺书;建立定期审计与考核机制,对服务

商的操作日志、安全措施落实情况进行检查,防范因外包服务漏洞导致的档案数据泄露风险,确保外包服务全程可控、可监管^[5]。

4 档案管理数字化转型中数据安全保障的挑战与未来展望

4.1 当前实施障碍

(1) 技术成本与档案部门预算的矛盾: 数据安全保障需投入高额成本,如部署区块链存证系统、AI威胁检测平台、量子加密设备等,且后期需持续投入运维与升级费用。但多数档案部门(尤其是基层单位)预算有限,优先保障档案收集、整理等基础工作,导致安全技术落地困难,形成“需求高、投入低”的矛盾。(2) 传统档案工作模式的惯性阻力: 部分档案人员长期依赖纸质档案管理思维,对数字化安全操作(如权限申请、加密传输)存在抵触心理;传统“重保管、轻安全”的工作模式难以快速转变,例如仍存在手工记录操作日志、未及时更新安全策略等问题,阻碍数据安全保障措施的全面推行。(3) 跨领域标准不统一导致的协同困难: 档案管理涉及档案、信息安全、法律等多领域,但目前各领域标准衔接不足。例如档案行业的“档案分类标准”与信息安全领域的“数据分级标准”定义不一致,跨机构共享档案时需重复适配,降低协同效率,也增加安全漏洞风险。

4.2 未来发展趋势

(1) 隐私计算技术在档案共享中的应用: 通过联邦学习、安全多方计算等隐私计算技术,实现“数据可用不可见”一跨机构无需共享原始档案数据,即可联合开展数据分析(如历史档案统计研究),在保障数据隐私的同时,打破档案共享的安全壁垒,提升资源利用价值。(2) 基于元宇宙的沉浸式档案安全体验: 借助元宇宙技术构建虚拟档案管理场景,档案人员可通过数字分身开展沉浸式安全操作演练(如模拟应对勒索软件攻击、数据泄露应急处置),直观感受安全风险后果;同时,元宇宙中的档案展示可设置动态权限屏障,增强公众访问的安全性与互动性。(3) AI自主进化带来的安全伦理挑战: 随着AI技术自主学习能力提升,其在威胁检测、权限管控中的决策自主性增强,但也可能出现“误

判合法操作”“过度拦截正常访问”等问题;此外,AI算法的黑箱特性可能导致安全决策无法追溯,引发“算法公平性”“责任界定”等伦理争议,需建立配套伦理规范。

4.3 研究深化方向

(1) 量子计算对档案加密体系的冲击与应对: 量子计算的超强算力可能破解现有RSA、AES等加密算法,威胁档案数据安全。未来需深化“后量子密码”研究,开发适用于档案管理的抗量子加密算法(如格基密码、哈希签名),并提前布局现有加密体系的升级替代方案,构建量子时代的档案安全防线。(2) 档案数据主权与国际治理规则构建: 随着跨境档案数据流动增多,数据主权争议(如他国要求调取涉本国利益的历史档案数据)日益凸显。需深入研究档案数据主权的界定标准、跨境流动的权责划分,推动国际社会形成统一的档案数据安全治理规则,平衡数据安全与全球档案资源共享需求。

结束语

档案管理数字化转型是时代发展的必然趋势,数据安全保障则是其稳健前行的基石。本文从技术、管理、法律、人员等多维度提出了系列策略,旨在构建全方位、多层次的安全防护网。然而,数据安全保障是一项长期而复杂的系统工程,需持续关注技术发展动态,紧跟法规政策变化,不断优化保障措施。唯有如此,才能在数字化转型浪潮中,确保档案数据的安全、可靠与合规,为档案事业的长远发展保驾护航。

参考文献

- [1]袁锋平.人工智能技术在档案管理中的应用现状与发展趋势[J].办公室业务,2025,(16):86-88.
- [2]刘永凤.大数据时代档案数据安全治理探究[J].兰台内外,2025,(24):9-11.
- [3]倪晓敏.企业数字化转型视角下档案数据治理必要性与实施策略探究[J].机电兵船档案,2025,(04):110-112.
- [4]李文清.企业数字档案馆(室)建设中的档案数据治理问题探讨[J].兰台内外,2025,(14):17-19.
- [5]雷培玲.新时期档案资源数据治理体系建设研究[J].办公室业务,2025,(06):55-57.