数字档案资源安全管理策略研究

王芳
山西省儿童医院 山西省妇幼保健院，山西 太原 030013

DOI: 10.61369/SSSD.2025160010

摘　　要： 在信息化和数字化转型进程中，数字化技术在档案管理中得到进一步推广和应用，我国档案管理正从传统纸质档案，转向数字档案建设和管理阶段。数字档案资源具有存储容量大、价值密度高、隐私涉密性强等特点，但也面临着数据安全与个人隐私保护方面的安全威胁。本文结合档案数字化建设与发展进程，分析档案数字化过程中的安全隐患，并围绕技术防护、管理机制、人员管理、应急响应四个方面，提出数字档案资源的安全管理策略，为保障数字档案资源安全提供参考。

关 键 词： 数字档案资源；安全管理；策略

Research on Security Management Strategies of Digital Archive Resources

Wang Fang
Shanxi Children's Hospital, Shanxi Maternal and Child Health Care Hospital, Taiyuan, Shanxi 030013

Abstract: In the process of informatization and digital transformation, digital technology has been further promoted and applied in archive management. China's archive management is shifting from traditional paper-based archives to the stage of digital archive construction and management. Digital archive resources have the characteristics of large storage capacity, high value density, and strong privacy and confidentiality, but they also face security threats in terms of data security and personal privacy protection. Combined with the construction and development process of archive digitalization, this paper analyzes the security risks in the process of archive digitalization, and proposes security management strategies for digital archive resources from four aspects: technical protection, management mechanism, personnel management, and emergency response, so as to provide references for ensuring the security of digital archive resources.

Keywords: digital archive resources; security management; strategy

引言

在数字化时代，基于“加强共享开放的一体化数据资源体系建设”目标要求，档案数据共享资源向数字档案资源方向转化，数字档案资源呈海量化趋势，其安全性面临着新的挑战[1]。随着《密码法》《信息系统密码应用基本要求》等法律和标准的出台，对数字档案资源的网络安全也提出了更高要求。数字档案资源是记录机构历史、承载核心信息的重要资产，安全管理水平直接关系到信息真实性、可用性、保密性与完整性[2]。当前，网络攻击、技术迭代、人员操作失误等风险因素，给数字档案安全带来威胁[3]。由此，从技术、管理、人员、应急等多维度构建系统化管理策略，实现全生命周期安全防护势在必行。

一、技术防护：筑牢数字档案安全技术防线

技术是数字档案安全的核心支撑，需围绕“身份验证－数据加密－备份恢复－系统防护”构建闭环体系，抵御各类外部与内部风险。

（一）身份认证与权限管控：杜绝越权访问

1. 推行多因素认证（MFA）：档案管理系统访问采用“密码＋动态验证码＋生物识别”组合认证，对于核心岗位人员，管理员、审计员可额外增加硬件令牌，避免单一密码泄露引发安全问题[4]。

2. 实施最小权限原则：按“岗位－职责”对应关系分配权限，如“档案采集员”仅拥有数据录入权限，“审核员”仅拥有审核权限，禁止跨岗位、跨层级越权操作；每季度或每月定期清理冗余权限，注销“僵尸账号”。

3. 部署单点登录（SSO）系统：整合档案管理、存储、备份等多平台账号，实现“一次登录、多系统访问”，同时统一账号生命周期管理（创建/变更/注销），减少账号管理漏洞。

（二）全流程数据加密：保障数据不泄露、不篡改

1. 传输加密：采用 HTTPS、SSL/TLS1.3 协议加密档案数据传输过程，跨部门、跨地域传输时，额外使用专用加密通道，禁止明文传输。

2. 存储加密：涉密、敏感数据采用 AES-256、SM4 等高强度算法加密存储；服务器、硬盘、云存储等存储介质采用

BitLocker、LUKS 加密技术，开启全盘加密，防止介质丢失导致数据泄露。

3. 使用加密：档案查阅、下载时自动叠加动态水印，防止截图、复印二次泄露；涉密档案需在物理隔离终端操作，禁止连接互联网 [5]。

（三）备份与恢复：应对数据丢失风险

1. 制定分级备份策略：按档案重要性执行差异化备份，核心档案遵循“321 原则”（3个副本、2种介质、1个异地离线存储），重要档案采用“211 原则”（2个副本、1种介质、1个异地在线存储），普通档案采用本地双副本；备份频率根据更新频次设定。

2. 建立异地备份中心：异地备份点与本地机房距离不低于100公里，避开地震、洪水等自然灾害高发区；备份介质区分在线（云存储）与离线（磁带库、离线硬盘），离线介质存放在防火、防潮、防盗的专用库房。

3. 定期开展恢复测试：每季度对备份数据抽样恢复，验证数据完整性与恢复时效性；测试结果形成报告，发现备份失效立即优化策略。

（四）系统与数据完整性防护：确保系统稳定、数据可信

1. 完整性校验：对归档数据生成唯一哈希值，存储时同步保存哈希值，每次访问、修改后重新校验，哈希值不一致则触发告警；核心档案采用区块链技术存证，记录全生命周期修改日志，实现不可篡改溯源。

2. 系统可用性保障：部署双机热备、集群架构，核心服务器、网络设备配置备用节点，避免单点故障；采用负载均衡技术分散访问压力，防止查询高峰期系统过载；每月开展漏洞扫描，每半年进行渗透测试，高危漏洞24小时内修复。

3. 终端安全管控：档案终端安装企业级杀毒软件、EDR（终端检测与响应）系统，实时拦截恶意代码；禁止终端连接无线网络、使用个人存储介质，确需使用需审批并扫描病毒；开启终端硬盘加密，防止终端丢失泄露数据。

二、管理机制：完善数字档案安全制度保障

技术需依托制度落地，通过“分级分类－流程规范－监督审计”建立管理体系，将安全要求嵌入数字档案全生命周期。

（一）分级分类管理：实现精准防控

1. 档案分级：按“涉密等级＋重要程度”对数字档案分级，绝密核心档案需物理隔离存储，机密重要档案加密存储并限制访问，普通档案按权限开放查询；每年复核分级结果，根据档案价值变化调整等级 [6]。

2. 介质分类：将存储介质按“信任等级”分为三类，信任介质（内部专用服务器）存储核心档案，半信任介质（加密 U 盘）用于临时传输，非信任介质（外部设备）禁止接入档案系统；介质使用需登记领用 / 归还 / 销毁信息，全程留痕。

（二）全生命周期流程管控：堵住各环节漏洞

1. 采集阶段：明确数据采集标准，外部数据需签订保密协议，采集后先杀毒、再校验完整性，拒绝恶意或不完整数据。

2. 整理阶段：整理过程禁止擅自修改档案内容，修改需填写《档案修改申请表》，经部门负责人审批后执行，修改日志自动留存且不可删除。

3. 归档阶段：归档前执行“三审”，经过采集员自审、审核员复审、管理员终审，审核通过后生成唯一归档编号并加密存储，归档数据与原始数据比对一致后，删除临时存储的原始数据。

4. 利用阶段：建立分级审批流程，绝密档案需单位负责人审批，机密档案需部门负责人审批，普通档案需管理员审批；利用时记录“利用人、时间、用途、操作内容”，禁止超范围使用 [7]。

5. 销毁阶段：到期档案需经“鉴定－审批－执行”流程，鉴定由档案管理委员会负责，审批需单位负责人签字，执行时采用“物理粉碎（硬盘）＋多次覆写（数据）”，双人监督并留存销毁清单与现场视频。

（三）监督与审计：确保制度落地

1. 实时审计：部署安全审计系统，监控档案系统的登录、查询、修改、下载等所有操作行为，对非工作时间大量下载、跨权限访问的异常操作触发告警；审计日志保存期限不低于6个月，禁止删除、篡改。

2. 定期检查：每月开展日常检查（备份完整性、权限合理性），每季度开展专项检查（利用审批、介质管理），每年开展全面检查（覆盖技术、管理、人员）；检查结果形成报告，问题整改期限不超过15天。

3. 第三方评估：每两年聘请第三方机构开展等保测评（等保2.0二级 / 三级）、数据安全评估，对照国家法规与行业标准查找漏洞，评估结果向主管部门报备 [8]。

三、人员管理：降低人为操作风险

人员是安全管理的关键环节，需通过“培训赋能－意识培养－行为规范”提升人员安全素养，减少内部风险。

（一）分层分类安全培训：提升防护能力

1. 全员基础培训（每年1次）：内容包括安全制度（介质管理、利用规范）、基础技能（弱密码设置、钓鱼邮件识别）、违规后果（法律责任、绩效处罚）；培训后通过线上考试，不合格者补考通过方可上岗。

2. 关键岗位专项培训（每半年1次）：针对档案管理员、运维员、审计员，培训内容包括技术工具使用、风险识别、合规要求；培训后进行实操考核。

3. 动态更新培训：针对新技术（AI、区块链）、新风险（新型钓鱼攻击），及时开展临时培训，确保人员掌握最新防护方法；培训课件、签到表、考核成绩归档留存 [9]。

（二）安全意识培养：营造全员安全氛围

1. 定期发布安全警示：每月通过内部邮件、公告栏发布安全警示，分享典型案例（档案泄露事件）、风险点（弱密码、未加密传输）、防范措施，提醒人员关注风险。

2. 开展宣传活动：每年结合“国家网络安全宣传周”“档案法宣传日”，组织安全知识竞赛、模拟演练数据泄露处置，提升人

员参与度。

3. 建立奖惩机制：对发现安全漏洞、阻止安全事件的人员给予奖励，对违反制度的人员按情节处罚，通过奖惩强化安全责任。

（三）人员行为全周期管控：规范操作流程

1. 入职管理：新员工签订《数字档案安全保密协议》，明确保密义务与违约责任；开展入职安全培训与考核，按最小权限分配账号。

2. 在职管理：每年开展人员背景审查，重点核查关键岗位人员的信用记录；禁止账号转借、个人设备接入档案系统，确需使用需审批并安装安全软件。

3. 离职管理：员工离职时办理“权限回收－介质交还－数据清理”手续，即时注销账号，收回存储介质，清理个人设备中档案数据；离职后定期回访，确认保密义务履行情况。

四、应急响应：快速处置突发风险

针对突发安全事件（数据泄露、系统宕机、病毒攻击），需建立“预案－响应－复盘”机制，最大限度降低损失。

（一）制定分级应急预案：明确处置流程

1. 事件分级：按影响范围、损失程度分为四级，一级（特别重大）：核心档案大规模泄露 / 系统瘫痪超24小时；二级（重大）：重要档案泄露 / 系统瘫痪12-24小时；三级（较大）：普通档案泄露 / 系统瘫痪6-12小时；四级（一般）：单份档案篡改 / 系统中断≤6小时。

2. 分类预案编制：针对数据泄露、勒索病毒、自然灾害等场景，明确应急组织架构（总指挥、技术组、协调组）、处置流程（发现－上报－控制－恢复）、时间要求（一级事件30分钟内上报）、资源储备（备用服务器、第三方支援联系方式）。

3. 预案修订：每半年评审预案，结合新风险、技术变化、演练结果优化内容，修订记录归档。

（二）建立应急响应体系：确保快速处置

1. 组建应急队伍：固定成员包括档案管理员、运维员、法务人员，明确职责；与网络安全厂商、数据恢复公司签订支援协议，一级 / 二级事件外部团队2小时内到场。

2. 定期演练：每季度开展四级 / 三级事件演练，每半年开展二级事件演练，每年开展一级事件演练；演练后形成评估报告，优化流程与资源配置。

3. 快速响应：事件发现后，第一发现人立即上报，技术组1小时内采取临时措施（关闭泄露渠道、隔离受感染终端），按等级上报相关负责人（一级事件上报上级主管部门）[10]。

（三）事件复盘与优化：避免重复发生

1. 复盘分析：事件处置结束后1周内，召开复盘会议，分析原因（技术漏洞 / 管理缺陷 / 人员操作）、处置问题（响应延迟 / 资源不足）、损失评估（数据丢失量 / 系统中断时长）。

2. 改进措施：技术层面修复漏洞、升级工具，管理层面修订制度、加强监督，人员层面补充培训、调整权限；改进措施纳入制度与流程，形成标准化文件。

3. 成果分享：内部分享复盘成果，告知全员改进方向，提升整体风险防控能力。

五、结语

综上所述，数字档案资源安全管理是一项长期性、系统性的工程，而影响数字档案安全的因素贯穿于数字档案形成、保管、利用等全生命周期，与系统建设、存储设备、管理规范、人员意识等存在密切的关系。因此，在传统纸质档案向数字档案资源转化的过程中，无论是管理人员，还是技术人员，都应通力合作，重视安全风险的预测识别、系统预防和应急响应，通过构建“技术防护为核心、管理机制为保障、人员管控为基础、应急响应为支撑”的多维管理模式，实现数字档案全生命周期安全可控，保障内部信息资产安全，提高数字档案资源的安全性、完整性与可靠性，为机构高质量发展提供坚实资源支撑。

参考文献

[1] 沈虹霞 . 纸质档案向数字档案转型过程中的信息组织与检索优化 [J]. 造纸信息 , 2024, (12): 125-127.

[2] 刘睿 . 传统档案向数字化档案转型的路径分析 [J]. 兰台内外 , 2024, (32): 16-18.

[3] 刘澔 , 栾珺予 . 新医改背景下医院档案数字化管理的实践与探索 [J]. 黑龙江档案 , 2024, (05): 78-80.

[4] 宋香玉 . 数字化转型背景下档案管理的安全性与隐私保护策略研究 [J]. 中原文化与旅游 , 2024, (08): 61-63.

[5] 王静 , 楚莒 , 沈继涛 . 档案数字化保存与智慧应用 [J]. 河南科技 , 2024, 51 (17): 155-158.

[6] 陈红 . 智能化视域下数字档案管理的挑战与应对策略 [J]. 办公室业务 , 2024, (15): 163-165.

[7] 窦光利 . 关于网络环境下数字档案管理应用安全分析 [J]. 内蒙古科技与经济 , 2024, (12): 38-41.

[8] 张若瑜 . 数字档案管理中数据归档鉴定的方法与应用分析 [J]. 办公自动化 , 2024, 29 (12): 55-58.

[9] 赵雪飞 , 尹磊 . 人工智能与新兴技术在未来数字档案管理中的应用研究 [J]. 赤峰学院学报 (自然科学版), 2024, 40 (03): 56-59.

[10] 庞丽红 . 数字档案馆建设视域下档案管理工作研究 [J]. 档案记忆 , 2024, (01): 55-56.

