 DOI: https://doi.org/10.12345/daglyqyfzyj.v4i2.36995

Research on the Construction of Personnel Archives Safety Management System in Public Institutions under the Background of Digitalization

BaYan

Xinjiang Bayingolin Mongol Autonomous Prefecture Health School, Bayingolin, Xinjiang, 841000, China

Abstract

Digital transformation has exposed public institution personnel archives management to multifaceted risks including outsourcing mismanagement, operational tracelessness, and favoritism interference. This study transcends the traditional “technology-first” paradigm by constructing a three-dimensional collaborative security management framework integrating technology, institutional mechanisms, and personnel, grounded in institutional logic theory and street bureaucrat theory. Addressing resource scarcity in grassroots archives, the research proposes innovative strategies: on-site supervision through “physical isolation + full-process accompaniment,” compliance communication via “digital trace reverse governance,” and the role construction of “institutional entrepreneurs.” These form a practical “digital flexibility-hardness” governance mechanism. The study demonstrates that archives administrators can transform institutional constraints into organizational safeguards through algorithmic-mediated discourse and ritualized procedural justice. This enables a transition from passive gatekeepers to proactive governance while maintaining safety baselines, providing a micro-level operational framework for modernizing archival security governance in public institutions.

Keywords

Public institutions; Personnel file security; Street bureaucrats; Institutional logic; Trace governance; Institutional entrepreneurs

数字化背景下事业单位人事档案安全管理体系建设研究

巴彦

新疆巴音郭楞蒙古自治州卫生学校，中国·新疆 巴音郭楞蒙古自治州 841000

摘　要

数字化转型使事业单位人事档案管理面临外包失控、操作无痕、人情干扰等复合型风险。本文突破"技术至上"的传统范式，基于制度逻辑理论与街头官僚理论，构建"技术-制度-人员"三维协同的安全管理体系。针对基层档案室资源匮乏现状，提出"物理隔离+全程陪同"的现场监管、"数字痕迹反向治理"的合规沟通、"制度企业家"角色建构等创新策略，形成可落地的"数字化柔性强硬"治理机制。研究表明，档案管理员可通过算法中介化话语与仪式化程序正义，将制度约束转化为组织庇护，在坚守安全底线的同时实现从被动守门人到主动治理者的身份跃迁，为事业单位档案安全治理现代化提供微观操作框架。

关键词

事业单位；人事档案安全；街头官僚；制度逻辑；痕迹治理；制度企业家

1 引言

随着事业单位人事档案数字化工作的全面推进，档案室从传统的＂实体保管＂向＂双套制管理＂（纸质＋数字）转型。与专业的信息技术部门不同，事业单位档案室通常隶属于办公室或人事部门，档案管理员往往面临＂技术支撑弱、安全责任重、管理手段少＂的现实困境。

本文回归档案管理实务，聚焦能够掌控、必须执行、即刻落地的安全管理措施，构建一套不依赖高端技术、强调人工监管与制度约束的安全管理体系，解决＂外包人员如何监督＂＂电子档案如何防篡改＂＂领导违规查档如何拒绝＂等具体痛点。

2 事业单位人事档案安全管理的现实困境与特殊性

2.1 基层档案室的安全管理痛点

2.1.1 数字化加工环节的失控风险

历史档案数字化多通过外包完成，但基层档案室普遍缺乏对外包人员的管控手段。外包人员通常来自社会公司，未经政审即可接触含身份证号、家庭住址、政治评价等敏感信息的原始档案。实际操作中，档案管理员因缺乏监管经验，

【作者简介】巴彦（1976—），女，中国新疆焉耆人，本科，档案副研究馆员，从事档案系列研究。

往往"只监工进度、不监管安全"，导致手机偷拍、私自复印、数据外带等隐患难以发现。

2.1.2 电子档案操作的不可追溯性

纸质档案的查阅需物理接触，痕迹明显；而电子档案的复制、截屏、转发可在数秒内完成且不留痕迹。部分单位虽有档案管理系统，但缺乏操作日志审计功能，档案管理员无法知晓谁在何时查看了哪些内容，更无法发现异常下载行为。

2.1.3 “人情查档”与合规操作的冲突

事业单位人际关系复杂，领导"打个招呼"就调阅档案、同事"帮个忙"就复印材料的情况屡见不鲜。档案管理员往往面临"坚持原则得罪人，放松要求担责任"的两难境地，缺乏明确的制度依据和拒绝话术。

2.1.4 技术防护手段的匮乏

多数基层档案室没有专业服务器，采用普通办公电脑存储电子档案；缺乏专业防火墙，内外网隔离不彻底；档案管理员缺乏信息安全培训，对弱密码、钓鱼邮件、U 盘病毒等基础风险缺乏识别能力。

2.2 事业单位人事档案的特殊安全要求

与企业档案不同，事业单位人事档案具有终身绑定性（涉及退休待遇核定）、政治敏感性（含入党、政审、处分材料）、跨年利用性（十年前的档案可能因提拔考察被调阅）三大特征。一旦发生泄露，不仅影响个人隐私，更可能干扰组织人事工作，甚至引发政治风险。因此，基层档案室的安全管理必须做到"零事故"，不能依赖事后补救，必须强化事前预防和事中监管。

3 基层档案管理员可执行的安全管理体系构建

针对档案管理员的工作场景，本文构建"技术基础防护-操作流程规范-职业素养建设"三维体系，所有措施均基于现有条件可立即实施。

3.1 技术维度：基础但有效的防护措施

3.1.1 数字化加工现场的"物理隔离＋全程陪同"管理

设立独立加工区：在档案室划定专门的数字化加工区域，与办公区物理隔离，安装防盗门和窗户遮光帘，禁止外包人员进入其他办公区域。

实施"安检进出"制度：外包人员进入加工区前，手机、背包统一存放于储物柜，严禁携带个人电子设备；离开时接受金属探测仪检查，防止携带纸质档案或存储介质外出。

档案管理员全程陪同：实行"人不离档、档不离眼"，外包人员操作期间，档案管理员必须在场监督，重点关注是否偷藏手机、是否私自夹带纸张。每半天轮换一次监督人员，避免疲劳疏漏。

专用设备封闭管理：数字化设备（扫描仪、电脑）拆除 USB 接口、光驱，禁用无线网络，仅保留有线内网连接。设备张贴封条，由档案管理员每日检查封条完整性[1]。

3.1.2 电子档案的"三隔离"存储策略

内外网隔离：电子档案存储电脑必须单机运行或仅连接内部局域网，严禁接入互联网。如需传输数据，使用一次性刻录光盘（CD-R/DVD-R）作为"摆渡"介质，刻录后立即标记日期并封存。

公私设备隔离：严禁在档案管理电脑上使用个人 U 盘、移动硬盘。配备专用红色标识的"档案专用 U 盘"，编号登记，专人专用，定期病毒查杀。

冷热数据隔离：建立"在线-近线-离线"三级存储。正在处理的档案（热数据）存于工作电脑；近期利用的档案（温数据）存于脱机硬盘，使用时才连接；历史档案（冷数据）刻录为光盘或存入硬盘后物理隔离存放，类似纸质档案的"库房"概念。

3.1.3 基础密码与访问控制

强密码策略：档案管理系统、电脑开机、压缩包均设置 8 位以上强密码（字母＋数字＋符号），每三个月更换一次，禁止生日、电话号码等弱密码。密码记录于纸质笔记本并锁入保险柜，严禁贴在电脑旁。

权限最小化：为不同岗位设置差异化权限。档案管理员拥有全部权限；人事干部仅开放查阅权，无下载、打印权限；分管领导设置"审批密码"，重要操作需输入二次密码确认。

操作日志手工备案：即便系统无自动审计功能，建立《电子档案操作登记簿》，手工记录每次查阅、下载、修改的时间、人员、事由、档案号，每月汇总比对，发现异常及时追溯[2]。

3.2 制度维度：可执行的操作流程规范

3.2.1 外包加工的"双人双岗"监管制度

岗前审查：查验外包公司资质、保密资质证书、人员身份信息，留存身份证复印件及无犯罪记录证明（可由外包公司统一提供，档案管理员核验原件）。

岗中监督：每批次档案加工必须有本单位正式职工在场。建立《数字化加工现场检查表》，每日勾选检查项：是否私带手机、是否规范着装（无口袋工作服）、是否按流程操作。

岗后销毁：加工完成后，监督外包人员彻底删除本地电脑中的临时文件，使用专业擦除软件覆写硬盘，防止数据恢复。销毁过程需档案管理员现场确认并签字。

3.2.2 档案利用的"痕迹管理"制度

分级审批：普通查阅需填写《电子档案查阅申请表》，经档案管理员审核；复印、拍照需部门负责人审批；批量导出（超过 5 份）需单位分管领导审批。

全程陪同查阅：外来人员（如政审人员）查阅电子档案时，档案管理员全程操作电脑，查阅者仅可观看屏幕，禁止触碰键盘鼠标。如需拍照，须使用档案室提供的专用设备，并在拍摄水印中嵌入查阅者单位信息。

定期核对：每月核对电子档案操作日志与审批单，发

现无单操作、超权限操作立即倒查。

3.2.3 应急预案与灾备管理

321 备份原则：至少 3 份数据，使用 2 种不同介质（硬盘 + 光盘），1 份异地存放。档案管理员每周将增量数据备份至移动硬盘，每月刻录一次光盘，每季度将一份备份介质存放于单位机要室或异地库房。

病毒防护：安装正版杀毒软件，每周全盘查杀；禁止在档案电脑安装无关软件（如游戏、视频播放器），关闭系统自动播放功能，防止 U 盘病毒自动运行。

应急响应：制定《档案数据泄露应急处置卡》，明确步骤：立即断网→报告领导→保护现场→核查范围→通知当事人。定期进行桌面推演，确保突发情况下不慌乱；[3]。

3.3 人员维度：制度执行者的策略性行动与合规话语建构

3.3.1 制度逻辑冲突下的合规沟通策略与权力博弈

在事业单位科层制语境下，档案安全制度逻辑（合规性逻辑）与行政效率逻辑（工具性逻辑）、人情关系逻辑（传统社会资本逻辑）之间存在结构性冲突。基于制度逻辑理论与街头官僚理论，构建档案管理员在数字化情境下的“制度弹性边界协商模型”，提出具有理论根基的实践策略。

3.3.2 数字化痕迹的反向治理：从“弱者的武器”到“合规性证据链”

传统纸质档案管理中，档案管理员面对领导越权查档要求时处于绝对权力弱势。数字化背景下，操作痕迹的可视化，重构了权力博弈格局。档案管理员可利用“数字痕迹的不可篡改性”作为制度性修辞资源，将个体合规诉求转化为“系统强制要求”的客观表述。

具体策略体现为“技术客观化话语策略”：

痕迹前置引用：在遭遇非程序性查档请求时，通过展示系统操作日志（如“当前登录 IP 已被记录”“此次查询将生成唯一追溯编码”），将合规要求从“个人拒绝”转译为“技术系统的强制性约束”。这种话语策略既维护了领导面子，又坚守了制度底线，体现了“数字化柔性强硬”的治理智慧。

算法中介化：利用档案管理系统的审批流引擎，将领导口头指令转化为必须通过的系统节点（如“系统设置批量导出需二级密码，该密码由保密办保管，非我个人所能控制”）。通过“算法权威”的中介，消解面对面拒绝带来的关系张力[4]。

3.3.3 职业伦理的建构性实践：从“守门人”到“制度企业家”

合规叙事的专业化建构：将档案安全从“繁琐的行政程序”重新框架为“组织记忆保全的核心能力”与“干部人事工作的风险防控枢纽”。通过向领导提交《档案安全风险评估报告》《违规查档的法律责任清单》等专业文本，将档案管理从后台支撑工作提升为具有战略价值的专业活动，从而获取“专家权力”。

预警性话语的生产：建立“风险预警 - 制度建议”的话语范式。当发现某部门频繁出现非规范查档请求时，不是简单拒绝，而是撰写《关于 XX 部门档案利用风险的提示函》，指出“近期该系统查询频次异常，建议加强该部门人员保密教育”。这种“预防性治理话语”将档案管理员定位为组织风险管理的顾问，而非单纯的保管员。

数字化时代的伦理边界：在算法治理日益渗透的背景下，档案管理员需捍卫“人工干预权”。当自动化系统出现误判，或大数据分析可能泄露敏感关联信息时，档案管理员应基于专业判断行使“否决权”，并通过“技术伦理审查建议书”等正式文本，将个体伦理判断转化为组织制度完善的提案[5]。

3.3.4 组织庇护机制的构建：制度性免责与职业安全

程序正义的仪式化：通过设计“双人双岗确认书”“痕迹留存告知书”等标准化文书，使合规操作具有“仪式化”特征。当发生安全事件时，这些文书构成“尽职免责”的制度性证据，保护档案管理员免于承担个体责任。

合规文化的仪式化传播：定期组织“档案安全制度学习会”，邀请单位主要领导出席并率先签署《合规查档承诺书》。通过“领导示范 - 制度内化”的路径，将档案安全从个体责任转化为组织共同价值，从根本上减少冲突性沟通场景的发生。

4 体系落地的实施建议

4.1 分阶段推进策略

第一阶段（1-2 个月）：物理环境整改。完成数字化加工区隔离、电脑 USB 封堵、密码更换、专用 U 盘配备等硬件整改，建立基础台账。

第二阶段（3-4 个月）：制度流程固化。将 " 双人双岗 "" 痕迹管理 " 等要求形成书面制度，经领导签发后执行，赋予档案管理员制度依据。

第三阶段（长期）：行为习惯养成。通过反复培训和演练，使安全操作成为肌肉记忆，形成 " 人人都是安全员 " 的文化氛围。

4.2 资源受限情况下的优先级排序

当经费、人员不足时，按以下优先级实施：

最高优先级：外包加工现场监管（风险最大）、内外网隔离（底线要求）。

次优先级：密码管理、操作登记、定期备份。

再次：监控设备、专业存储设备、灾备演练。

5 结语

事业单位人事档案安全管理本质上是制度逻辑冲突下的微观权力博弈。本文构建的三维体系表明，技术防护的效能取决于制度执行的刚性，制度执行的刚性又依赖于执行者的策略性行动能力。面向未来，随着算法治理的深入渗透，

档案安全将从 " 人防 " 向 " 技防 " 再向 " 智防 " 演进，但人的专业判断与伦理坚守始终是最后一道防线。档案管理者应持续培育 " 制度企业家 " 精神，在推动档案安全治理体系与治理能力现代化的进程中，实现专业价值与组织价值的双重提升。

参考文献

[1] 周耀林,赵跃.面向公众需求的档案资源建设与服务研究[M].武汉大学出版社:201706:598.

[2] 田淑华.电子档案信息安全管理研究[D].中北大学,2009.

[3] 周耀林,常大伟.我国档案大数据研究的现状分析与趋势探讨[J].档案学研究,2017,(03):34-40.DOI:10.16065/j.cnki.issn1002-1620.2017.03.006.

[4] 肖敏.大数据环境下档案利用服务体系建设研究[D].湘潭大学,2015.

[5] 高晨翔,牛力.国内“档案数据”研究述评[J].档案学研究,2020,(05):11-18.DOI:10.16065/j.cnki.issn1002-1620.2020.05.002.