电子档案安全管理与风险防范措施探究

龚 翼

湖北典策档案科技发展有限公司 湖北 武汉 430000

摘 要：数字化转型背景下，电子档案成了档案管理工作的核心载体，能否保障其全生命周期安全，是档案事业高质量发展的关键。本文从电子档案数字化、多元化的特征出发，把档案生成、存储、传输、销毁各阶段的风险梳理了一遍，从制度建设、技术防控、人员素养、应急管理四个角度分析了风险成因。结合行业管理实际，有针对性地构建了一套全流程、立体化的风险防范体系，目的是化解数字化档案管理的安全隐患，筑牢档案数据的安全防线，给单位电子档案的规范化安全管理做个实践参考。

关键词：电子档案；安全管理；风险防范措施

引言

数字技术普及，传统纸质档案管理模式慢慢向数字化、智能化转，电子档案因为传输快、存着方便、能反复用这些好处，被各行各业广泛采用。但数字化也让电子档案的安全风险更隐蔽、更容易扩散，统档案管理模式已难以适应新的安全防控需求。眼下数据泄露、档案损毁、信息篡改这些问题频频出现，严重影响了档案管理工作的正常开展。针对这些情况，本文深入探究电子档案的安全风险与防控策略，希望能帮着完善数字化档案安全管理体系。

1 电子档案安全管理相关理论概述

1.1 电子档案的核心内涵与特征

（1）电子档案的定义：电子档案是数字化时代档案体系的核心载体，靠各种数字终端和网络设备来完成生成、传输、存储这一整套流程。它既保留了传统档案原始的记录性和法律凭证效力，又有完整的溯源路径和复用价值，属于标准化的数字化档案资源。档案的形态也不再限于传统的文本格式，还包括图像影像、音视频资料、数据库信息等多种数据形式，覆盖了各类数字化记录场景。（2）电子档案的核心特征：跟传统纸质档案比起来，电子档案用数字化媒介当存储载体，有批量复制、高速传输、集中存储这些明显优势。归档前的文件形成阶段，可以根据业务需要修改或调整；但一旦正式归档，就要靠技术和管理双重手段保证内容不能改，这样既照顾到现代化档案管理对灵活性的要求，也兼顾了严肃性。但也正因为数字化这个属性，电子档案的安全隐患跟传统档案不一样，风险更隐蔽、更容易扩散，一旦出了安全问题，很容易引发大范围、持续性的档案安全事故[1]。

1.2 电子档案安全管理的核心内容

（1）实体与载体安全管理：盯着电子档案的存储硬件做防护，重点保证存储设备、服务器、存储介质这些硬件的物理安全。通过常态化管护，把设备损毁、遗失、人为破坏这些实体风险防住，给档案存储的硬件安全把好关。（2）数据内容安全管理：以档案数据本身为核心，严格保证电子档案内容的真实性、完整性和有效性。靠技术和管理双重手段，把数据篡改、伪造、丢失、外泄这些问题堵住，保住档案的凭证价值和使用价值。（3）运行环境安全管理：对档案管理系统、网络运行环境以及日常操作流程，实施规范化的安全管控，覆盖电子档案从生成到销毁的整个过程，保证各环节合规、稳定、安全地跑下来。

2 电子档案全生命周期安全风险识别

2.1 档案生成与归档阶段风险

（1）生成环节风险：电子档案刚生成的时候，各种安全隐患很容易跟着数据采集和录入冒出来。人工录入出错、原始资料内容不全这些问题，会直接导致初始电子数据失真、内容不完整。同时，数字化生成设备突然故障、运行异常，也会破坏数据生成的完整性。另外，不排除有人故意篡改原始数据，那就会从源头上损害电子档案的真实性和原始性，引发基础性的安全风险[2]。（2）归档环节风险：档案归档是规范管理的关键一步，如果归档操作流程没有标准化约束，不对档案内容的真实性、完整性做全面审核，很容易出现漏归、错归。同时，有些档案管理人员工作不够规范，归档完了没有及时做数据备份，一旦数据出问题，就没法回溯复

原，造成档案资源流失。

2.2 档案存储与运维阶段风险

（1）硬件设备风险：电子档案得靠硬件载体来存，服务器、硬盘这些核心设备用久了容易老化、损坏，突然断电、设备出故障也会影响数据安全。另外，自然灾害、人为破坏这些外部因素，会直接毁掉存储载体，造成档案数据永久丢失。（2）软件系统风险：档案管理系统要是有程序漏洞、防护缺陷这些隐患，就容易遭到网络病毒入侵、黑客非法攻击。同时，系统升级或者日常运维的时候，如果操作不当、方案不合理，会导致后台数据错乱、缺失，破坏档案数据的稳定性和完整性[3]。（3）存储环境风险：网络和数据防护体系不完善会带来不少安全隐患，内外网混用、网络防护机制缺失，会大大降低网络安全等级。再加上档案数据加密标准不够，系统容易出现非法访问、越权操作这些问题，严重威胁档案存储安全。

2.3 档案传输与利用阶段风险

（1）传输环节风险：电子档案在跨设备、跨网络传来传去的时候，如果传输通道没有加密防护，数据很容易被第三方拦截、偷走或篡改，让档案信息泄露出去，把档案数据的保密性给破坏了。（2）利用环节风险：档案权限分配乱、管得不严，就会让岗位权限交叉、重复，不相干的人也能违规查看、下载、复制档案资料。同时，档案对外借阅、公开使用缺少规范的审批流程，挺随意的，信息泄露的风险就更大了。

2.4 档案销毁与报废阶段风险

（1）销毁不彻底风险：现在多数档案销毁只是简单删一删、清一下表层数据，没真正把底层存储数据清干净。被删掉的档案还能用技术手段恢复回来，信息泄露的风险不小。（2）报废管理风险：存档案的硬件设备在报废或流转之前，要是没把设备里留存的档案数据彻底清掉，残留信息就会跟着设备流出去，引发隐性的档案安全事故。

3 电子档案安全管理风险成因分析

3.1 管理制度体系不完善

（1）制度建设滞后：数字化档案一直在往前推，可管理制度更新跟不上，还在沿用传统纸质档案那套，很难适应电子档案数字化、网络化的管理。特别是电子档案单套制推行后，制度上有空白，跨部门协同安全管理机制也缺位。对元数据采集、格式兼容这些生成环节没有硬性约束，碰上 AI 生成内容真实性验证这种新型风险，就更没招了。（2）执行监管缺位：有些单位虽然建了基础制度，但执行起来走过场，没有常态化的监督检查和追责机制。再加上档案部门在单位里本来就不太受重视，专业人才流失严重，日常操作中的违规行为没人管，安全隐患一直攒着。

3.2 技术防控能力不足

（1）防护技术老旧：基层单位大多还靠防火墙、杀毒软件这些老办法，数据动态加密、漏洞智能检测、行为溯源、入侵预警等现代化技术跟不上。安全投入不够，技术更新慢，不同系统之间成了数据孤岛。存储阶段里，长期保存的格式失效风险、云存储的第三方依赖风险，也没怎么管到位。（2）技术运维薄弱：多数单位没有专属运维团队，系统的检修、升级很难常态化，潜在的漏洞没法及时补上。碰上网络攻击或数据异常，应急防控能力弱，而且对 AI 深度伪造篡改、个人信息泄露（违反《个人信息保护法》）这些利用阶段的风险，也缺少技术应对手段[4]。

3.3 人员安全素养参差不齐

（1）安全意识薄弱：从业人员对数字化存储、传输里的安全风险认识不够，私自拷数据、随便传、乱授权这些操作经常出现。档案部门本来就边缘化，人还留不住，现有人员常常把利用阶段的数据泄露风险和 AI 伪造篡改威胁不当回事，人为隐患比较突出。（2）专业能力不足：多数人没受过系统培训，对风险防控流程、安全操作规范、突发事件怎么处置，都掌握得不够。尤其是在个人信息保护合规、深度伪造识别、云存储数据彻底删除这些新领域，专业能力缺口不小，很难应对复杂的安全问题。

3.4 责任落实与应急机制缺失

（1）岗位职责模糊：多数单位没有按电子档案全流程把岗位权责细化，安全管理边界不清，也缺少对应的追责体系。一旦发生数据篡改、泄露这些事故，就容易互相推诿。而且对于云存储数据销毁阶段到底有没有彻底删掉，也说不清谁负责。（2）应急体系空白：单位普遍没针对数据篡改、泄露、丢失以及 AI 伪造等突发情况制定专项预案，缺少分级响应机制和数据恢复的时间要求。碰上安全事件，手里没有标准化的处置流程，没法快速止损、恢复，结果损失越拖越大。

4 电子档案安全管理与风险防范优化措施

4.1 健全规范化安全管理制度体系

（1）单位要结合行业标准和业务场景，围绕归档、存储、传输、利用到销毁的整个生命周期，把操作规范和安全管控细则细化到位，补齐传统制度在数字化场景

里的短板，让管理有据可依。（2）设个专门的安全监督岗，搭一个常态化全覆盖的排查机制，定期检查加随机抽查操作流程、系统状态、数据流转情况。靠标准化审核和动态监管，及时把违规行为纠正过来。（3）按岗位把电子档案安全权责清单细化出来，把管理、操作、审核各岗位的职责定清楚，签安全责任承诺书，再配上奖惩追责机制，形成闭环管理。

4.2 升级全方位技术防控体系

（1）强化数据安全防护：对核心数据用加密、脱敏这些现代化技术，让存储和传输全程都加密。建好常态化备份和异地容灾机制，把设备故障、系统异常这些风险防住。同时引入区块链技术，让电子档案没法篡改、全程可追溯；对高涉密档案可以试试量子加密技术，保证传输安全。（2）优化系统与网络安全：定期做漏洞扫描、隐患修复，优化防火墙和入侵检测，把内外网物理或逻辑隔离落实到位。积极用上 AI 技术：一方面应对 AI 深度伪造对档案真实性的篡改威胁，另一方面用 AI 做异常行为检测、漏洞自动扫描和智能风险预警，把主动防御能力提上去[5]。（3）搭建智能溯源监控系统：引入操作日志记录和行为溯源技术，对查阅、下载、修改、传输这些操作实时监控。再结合数字孪生技术搭虚拟备份和灾备体系，做到违规行为提前预警、全程可查、责任可追，保证电子档案操作的规范性和安全性。

4.3 强化从业人员专业素养建设

（1）开展常态化安全培训：结合电子档案管理的风险特点，定期组织数据安全、网络防护、AI 伪造识别、应急处置这些专项培训，帮从业人员更新专业知识，强化安全意识，规范日常操作，从人员层面切实减少安全隐患。（2）搭建专业人才队伍：多引进数字化档案管理、网络安全运维以及 AI 技术方面的专业人才，组建专职化的档案管理和技术运维团队，把现有人员的技术短板补上，把单位在电子档案风险识别、技术运维、突发问题处理等方面的专业能力提上来。（3）建立考核评价机制：把电子档案安全管理成效、合规操作情况、风险防控落实效果这些都放进员工绩效考核里，用考核推动从业人员重视档案安全，主动规范操作流程、把防控职责压实，把人员管理的基础夯实[6]。

4.4 完善应急处置与长效保障机制

（1）针对数据泄露、丢失、系统瘫痪、恶意篡改以及 AI 深度伪造这些常见突发情况，制定标准化的专项处置预案，把责任人员、处置流程、整改时限都定清楚。建立数据泄露事件的分级响应机制，并且规定核心数据恢复时间不超过 4 小时、重要数据不超过 24 小时，给突发事件处置提供清晰的制度支撑。（2）定期组织档案安全应急实战演练，让工作人员把风险处置流程和补救方法练熟，积累应急处置经验，提升团队协同能力，尽量降低安全事故造成的损失和影响。（3）盯着数字化技术迭代的节奏和网络安全风险的变化，动态调整管理制度、防护技术和防控方案，持续优化电子档案安全防控体系，做到常态化、长效化、智能化的安全风险防控。

结束语

电子档案安全管理是一项系统性、长期性的工作，贯穿档案从生到死的全过程，直接关系到档案资源的完整性、真实性和保密性。本文把电子档案各环节的安全风险都捋了一遍，从管理、技术、人员、应急机制几个层面剖析了核心问题，并给出了适配数字化场景的优化防控策略。往后还得紧跟技术迭代和风险变化，不断把防控体系完善起来，全方位提升电子档案安全管理水平，推动数字化档案管理工作合规、安全、长效地走下去。

参考文献

[1] 张萌. 电子档案管理中的安全风险及防范策略 [J]. 兰台内外,2023,5(27):23-25.

[2] 李娜. 电子档案管理的安全风险与防范措施 [J]. 黑龙江档案,2022,23(6):188-190.

[3] 安芳. 数字时代构建会计电子档案管理体系研究 [J]. 潍坊学院学报,2022,22(2):102-104.

[4] 滕增强. 单套制电子档案管理风险和策略探析 [J]. 黑龙江档案,2022,10(1):72-74.

[5] 刘越男. 电子档案单套制的法律与技术保障 [J]. 档案学通讯,2022(01):4-12.

[6] 张宁. 区块链技术在电子档案管理中的应用研究 [J]. 档案学研究,2021(03):112-118.