 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i11.33765

Security risk analysis and prevention of classified document digitization

Wenhe Zhang

Beijing Feihang Jiesun Technology Co., Ltd., Beijing, 100074, China

Abstract

In the digital transformation of China's classified archives, the shift from traditional paper-based formats to electronic, networked, and systematic systems has fundamentally restructured the processes of document creation, circulation, storage, and utilization. While digitization has significantly enhanced management efficiency and accessibility, it has also exposed multiple security vulnerabilities. This paper examines the practical implementation of digital transformation in China's classified archives, first highlighting the critical importance of security risk prevention. It then analyzes four major security risks inherent in the digitalization process through four key dimensions, and proposes four professional, actionable countermeasures to address these challenges.

Keywords

confidential archives; digital construction; security risks; prevention; important value; measures

保密档案数字化建设的安全风险分析及防范

张雯鹤

北京飞航捷迅科技有限公司，中国·北京 100074

摘　要

在我国保密档案数字化建设过程中，随着传统纸质载体向电子化、网络化、系统化转型，档案的生成、流转、存储与利用环节被深度重构。数字化虽提升了档案管理效率和利用便捷性，但亦暴露出诸多安全风险点。本文从我国保密档案数字化建设的现实场景出发，首先探析保密档案数字化建设中安全风险防范的重要价值，其次从四大维度剖析数字化过程中存在的主要安全风险，再针对上述风险提出四项专业化、可操作的防范措施。

关键词

保密档案；数字化建设；安全风险；防范；重要价值；措施

1 引言

保密档案是国家、组织或个人的重要信息资源，它具有非常高的价值和敏感性，保密档案数字化建设随着数字化技术的广泛应用已成为提高档案管理效率、实现资源共享的重要方式。档案数字化是指计算机技术将模拟信号转化为数字信号的过程，其中纸质档案数字化就是用扫描仪等数码设备对纸质档案进行数字化加工并将它转化为磁盘等载体的过程。然而从实践来看，现阶段保密档案数字化建设进程仍面临着一定的安全风险，因而如何进行有效防范是一项值得深入探究的课题。

【作者简介】张雯鹤（1976–），女，蒙古族，中国内蒙古赤峰人，本科，高级工程师，从事人力资源，保密管理，国家安全研究。

2 保密档案数字化建设安全风险防范的重要价值

随着我国档案事业迈入数字化治理的新时代，保密档案从传统的纸质形态转向数字化、网络化和集成化的发展阶段，在此基础上保密档案的安全风险防范就显得尤为必要[1]。一方面，从业务管理层面来看，电子类档案管理有关办法要求电子档案全生命周期均应遵循网络安全法、数据安全法、个人信息保护法以及保密法等国家法律法规。另一方面，从技术层面来说，保密档案数字化建设包括资料的扫描、转换、存储、检索等各个工作步骤，同时也涉及相关的存储介质、网络传输、云服务等众多方面，在这种情况下只有技术保障措施到位才能有效地防范各环节所存在的风险。此外，从组织管理层面来说，保密档案数字化建设是一个跨部门、跨系统、跨程序的过程，在没有严格的标准化、规范化操作与统一的责任落实及安全审计保障下容易出现管理空白、责任不清的情况，继而导致数字化保密档案面临不法使用、泄漏等风险。最后，从利用价值维度看，保密档案一旦数字化，其

检索速度、资源整合及服务能力显著提升，但若未同步实施风险防范，则易于构成信息暴露或误用。因此，构建基于风险识别、制度控制、技术防护与人员管理的防范体系，在我国保密档案数字化建设中具有不可替代的重要地位。

3 保密档案数字化建设的安全风险分析

3.1 生成阶段的载体转换与电子化加工风险

保密档案数字化建设的生成阶段在纸质载体向电子化转换过程中存在较高安全风险。档案在预处理、拆卷、扫描、元数据录入及格式转换等环节，若缺乏物理隔离与访问控制，极易被非法复制、拍照或截屏并通过外部网络传播。加工设备若接入互联网或外设端口未封闭，则可能遭受恶意软件入侵，导致档案内容被篡改或泄漏[2]。同时，生成阶段产生的大量临时文件和备份数据若缺乏统一编号与复原核对机制，易引发卷内页顺序错乱、密级标识遗漏或原件遗失等问题。若加工人员未经保密审查或培训不到位，亦可能出现误操作、私自导出数据、违规携带外部介质等行为，从而使生成阶段成为档案数字化安全体系中最易被忽视的风险环节。

3.2 流转环节的登记与归集脱控风险

数字化保密档案在生成后需流转至归档整理、利用审批、存储接收等环节。若流转过程中未进行准确登记、未区分涉密级别、未对档案移交人员、时间、接收系统、审查流程进行记录，则可能出现档案“失控”、人为拍照流传、未经授权访问等问题。例如，某省档案局服务人员于扫描现场将标注“机密”档案带出现场后拍照分享到微信群，因流转环节未严格登记、未核复档案拆封复原、未监控人员行为，造成泄密。在数字化状态下，流转频次增加、访问权限扩大、系统接口增多，若缺乏流程管控、权限分级、日志审计，则此类风险尤为突出。

3.3 存储阶段的物理、网络及数据安全风险

数字化后的保密档案主要以电子形式存储，其安全威胁包括但不限于物理介质损坏、存储环境恶化、网络攻击、恶意软件入侵、传输过程拦截及数据篡改。结合实践来看，数字化保密档案存储介质会受到温度、湿度、磁力场、振动等因素的影响，该局面下一旦环境监控不当，容易造成数据破坏或者丢失。而通过外部网络连接、远程访问或是云平台等进行保密档案数据存取的行为也存在着安全隐患点，这些地方容易成为黑客、病毒、漏洞发起攻击的目标，从而导致保密档案被非法访问、篡改或者窃取！

3.4 利用阶段的内部管理与共享机制风险

保密档案数字化提升了检索、共享与利用的效率，但同时也带来了内部访问控制失效、共享范围扩大导致失控、敏感信息与非涉密数据错配、开源信息融合可能生成新敏感信息等风险。近年来，开源信息成为国家秘密泄密的新源头，若保密档案与公共数据、社交媒体数据交融共享，则可能被情报机构通过数据挖掘提取敏感信息[3]。此外，组织内部若未建立严格的权限分级、审查流程、责任追踪及审计机制，则档案利用阶段仍存在人为越权、拍照传播、系统截屏等违法行为。

4 保密档案数字化建设安全风险的防范措施

4.1 针对生成阶段载体转换与电子化加工的控制

为强化生成阶段安全控制，应建立系统化、可追溯的管理机制。首先，纸质档案进入数字化加工前应设立物理隔离的受控区域，禁止与办公网络、无线网络连接，并实行门禁卡、视频监控、进出登记制度。其次，在设备与网络管理方面，扫描设备、工作站及存储服务器须运行于专网或脱网环境，禁用互联网接入，对 USB、蓝牙、光驱等端口进行物理封闭与周期性检测。所有设备使用前须经档案与保密部门联合核验固件、系统补丁及防病毒状态。第三，应对拆卷、扫描、图像处理、元数据录入、文件格式转换、复原归档等环节制定标准化操作规程，每环节设定责任人与审核签字，电子档案生成后应立即比对原件的内容、页码、密级标识与签章图像，形成核对日志并归档。第四，在人员控制方面，所有加工人员须通过涉密审查、签订保密协议并经培训合格方可上岗，加工现场严禁携带手机、摄录设备及移动介质，实行交接班与设备清点制度。对外包机构须签订包含保密责任、违约处罚及审计权的合同，并接受定期或不定期现场核查。最后，应建立日志监控与审计机制，扫描系统自动记录操作人员、时间、设备编号与数据存放路径，档案与保密部门定期抽查并对异常操作启动应急响应和整改程序，从而实现生成阶段全过程的可控与追溯。

4.2 针对流转环节登记与归集脱控的流程规范

为防范保密档案数字化建设中流转环节的登记与归集脱控，应构建闭环管理流程。首先，建立统一的数字档案流转登记体系，明确档案从生成、接收、整理、归档、利用全过程的责任部门、责任人、接收时间、系统平台及签字确认信息，所有移交操作须经审批节点、密级确认节点、身份验证节点及权限校验节点后方可执行，并通过电子审批系统实现流程可追溯。其次，实施分级授权与访问控制机制，依据档案密级、岗位职责及使用目的设定权限范围，系统自动记录每次查阅、下载、转发等操作的主体、时间、设备及 IP 信息，并定期生成权限异常审计报告由保密管理部门复核，确保访问行为全程留痕。再次，在档案移交至档案管理部门或业务系统环节，应采用端到端加密传输与密级标识技术，移交前生成唯一编号并在源、目标系统同步登记，接收环节执行编号核对、签收确认与日志入库，移动介质移交须附封条、清单、签名确认并实施双人核对[4]。最后，建立异常事件快速响应机制，对发现的档案缺失、越权访问、未登记移交、日志异常等情况，立即启动事件调查程序，暂停相关系统访问、保存电子证据、通报保密主管部门，并在安全责任

档案中记录处置流程及追责结果，形成事件全程闭环可追溯体系。

4.3 针对存储阶段物理、网络及数据安全的综合防护

针对数字化保密档案存储阶段，核心在于构建起多层次的、物理上和逻辑上分开的安全体系。档案管理部门应该有自己的独立的保密档案存储设备和专网环境（禁止连接外部互联网），同时配备恒温恒湿、磁场、震感检测的机房，并有门禁、视频监控、消防、环境监测等全套的安全防护措施。运用“磁带＋磁盘阵列＋光盘”的异构备份方式来保证数字化保密档案存储的多介质冗余和容灾能力。数据环节上采取强加密、访问控制和完整性校验方式，对扫描文件以及元数据使用加密算法并生成哈希值校验完整性，同时定期进行快照对比和冗余校验，并且还应建立异地灾备与周期性恢复演练机制。网络安全环节则做好防火墙、入侵检测以及漏洞扫描等系统部署，同时辅以日志分析、补丁管理做足常规安全防范工作，采取最小权限、会话超时、双因子认证等访问控制措施降低保密档案被非法访问或篡改的风险。此外，档案管理部门还需跟踪存储介质老化、迁移过程以及格式化更新的过程，以保证该过程中不造成保密档案数据无损、签名一致以及日志完整。另外，档案管理部门还应实行数字化保密档案安全审计、应急响应体系，在线监控网络的访问行为、设备状态的管理制度。一旦发现非法数字化保密档案被入侵、异常导出、介质损坏等情况立即启动应急程序，即隔离系统、保存日志、修复漏洞，并形成本次处置报告归于责任追溯档案，保证存储备份整个阶段的安全可控。

4.4 针对利用阶段内部管理与共享机制的权限控制

在数字化保密档案进入利用阶段后，应强化访问权限控制、共享范围管理、挖掘隐蔽风险的数据融合防范、用户行为审计等。首先，应建立访客与用户实名制制度，并结合岗位职责设定访问级别。系统应实施细粒度访问控制模型（如基于角色的访问控制 RBAC、基于属性的访问控制 ABAC），确保只有在履职需要、经审批授权的用户才得以访问特定密级档案。其次，应对档案共享机制进行严格审批与监管。任何跨部门、跨系统、跨地域的档案调用必须预审密级、用途、审批人、借阅期限、回收机制；共享时应采用水印防复制、防截屏、防拍照技术，并对共享数据实施访问记录、导出控制、电子痕迹。第三，应对开源信息与敏感档案的数据融合风险进行动态评估 [5]。鉴于开源信息可能与涉密档案结合形成新敏感情报，档案管理部门应建立情报监测机制，追踪开源数据走向、检测可能的新敏感关联，在档案共享前开展“关联敏感性评估”，判断是否存在由非涉密数据反推涉密信息风险。最后，对用户行为实施持续审计与异常预警。系统应自动记录用户访问、下载、导出、修改、拍照屏幕、远程访问、异常时段登录等操作日志，并利用大数据分析、行为模型、异常检测算法识别潜在越权、拍屏、传播等风险，触发预警机制并启动人工调查。

5 结语

在我国保密档案数字化建设向纵深推进的过程中，安全风险防范体系的构建不仅关系到档案本身的完整性、可控性与安全性，也关系到国家秘密与信息资产的守护。通过从生成、流转、存储、利用四个环节切入，配合技术防护、流程管控、人员责任与审计机制的协同运行，能够有效提升保密档案数字化建设的安全保障水平。未来，档案管理机关需持续完善制度规范、强化技术保障、健全人才队伍、提升整体态势感知与应急处置能力，从而为保密档案数字化提供坚实的安全基石。

参考文献

[1] 张雪军.档案数字化工作中的安全风险和防范措施[J].科技视界,2024,14(12):55-59.

[2] 金在莹.对档案数字化的质量控制与安全保密方法的研究[J].活力,2023(9):109-111.

[3] 苏云川.数字化档案的安全保密管理及信息安全分析[J].计算机产品与流通,2023(10).

[4] 顾金玲.档案数字化过程中的保密技术选择与实施策略[J].兰台世界,2024(11).

[5] 李明丽,石郦冰,金明鑫,等.科研保密单位纸质档案数字化加工分析[J].兰台世界,2024(6).