数字化背景下档案数据安全管理体系研究

邓　滔

昭阳区财会人员教育培训和会计核算中心　云南　昭通　657000

摘　要：档案管理数字化转型使数据安全风险从实体损坏扩展至网络攻击、系统故障与供应链威胁，传统防护模式难以应对。本文以档案数据为对象，分析其安全形势与风险特征，从管理、技术、制度、人员四个维度构建安全管理体系。研究提出，档案数据安全应以分类分级为基础、以全生命周期为主线，通过四维协同形成覆盖采集、存储、传输、利用、共享、销毁各环节的管理闭环。该体系可为档案数据长期安全保存与合规利用提供系统性保障。

关键词：数字化；档案数据；安全管理；分类分级；全生命周期

引言：档案数据是国家基础性、战略性信息资源，其安全性关乎国家利益与公民权益。随着数字中国建设推进，档案管理从纸质载体向数字载体转变，数据易复制、易篡改、易泄露，网络攻击手段升级，存储介质寿命有限，安全边界日益模糊，传统实体防护模式已难以应对。当前研究多聚焦技术防护或制度规范单一维度，缺乏系统性体系构建。本文立足数字化背景，分析档案数据安全形势与风险特征，从管理、技术、制度、人员四个维度探讨安全管理体系的构建路径，旨在为档案数据安全保障提供系统化参考。

1 数字化背景下档案数据安全形势与风险特征

1.1 档案数据的内涵与安全要求

档案数据是指以数字形式生成、采集、存储和利用的具有档案价值的信息资源，包括原生数字档案和传统载体档案数字化副本。档案数据具有原始记录性、凭证价值性、长期保存性与不可再生性，其安全要求高于一般业务数据。档案数据安全不仅要求防止数据泄露、篡改与丢失，还要求保障数据的完整性、可用性与可追溯性，确保档案在法律、行政、历史研究等场景中持续发挥凭证作用。数字化条件下，档案数据的安全边界从实体库房扩展至网络空间，安全对象从载体扩展至内容，安全周期从保管阶段延伸至全生命周期。

1.2 数字化带来的安全风险变化

数字化转型使档案数据安全风险发生结构性变化。风险来源方面，从传统的物理损坏、自然灾害扩展至网络攻击、系统故障、人为误操作、供应链风险等。风险传播方面，数据一旦泄露或篡改，可在短时间内大范围扩散，影响面远超纸质档案。风险隐蔽方面，数字环境下的攻击与篡改往往不留明显痕迹，发现与追溯难度大。风险关联方面，档案数据常与业务系统、政务平台、云服务关联，安全边界模糊，一处失守可能引发连锁反应。风险持续性方面，存储介质寿命有限、格式迭代快、系统依赖性高，长期保存面临技术过时与介质失效的双重压力[1]。

1.3 档案数据安全面临的主要威胁

档案数据安全面临的主要威胁可归纳为四类。一是外部攻击威胁，包括黑客入侵、勒索软件、高级持续性威胁等，目标直指数据窃取、篡改或加密勒索。二是内部管理威胁，包括人员误操作、权限滥用、离职人员带走数据、外包人员管控不严等。三是技术系统威胁，包括存储介质故障、系统漏洞、网络中断、云服务商风险等。四是制度执行威胁，包括制度不健全、执行不到位、监督缺失、责任不清等。四类威胁相互交织，单一防护手段难以应对，需构建系统性安全管理体系。

2 档案数据安全管理体系构建

2.1 管理体系构建的总体思路

档案数据安全管理体系构建应遵循系统性、全生命周期、分类分级、动态调整四项原则。系统性要求覆盖管理、技术、制度、人员四个维度，形成协同防护；全生命周期要求覆盖数据采集、存储、传输、利用、共享、销毁各阶段，不留管理盲区；分类分级要求根据数据敏感程度与价值等级实施差异化保护，合理配置资源；动态调整要求根据技术发展与威胁变化持续优化体系，保持防护有效性。总体思路是以分类分级为基础，以全生命周期为主线，以管理、技术、制度、人员四维协同为支撑，构建覆盖全面、重点突出、动态可调的安全管理框架。

2.2 管理维度：分类分级与流程管控

管理维度是档案数据安全管理体系的基础。分类分级方面，应根据档案数据的来源、内容、价值、敏感程度划分等级，明确不同等级数据的保护要求、访问权限与审批流程。一般而言，可分为公开、内部、秘密、机密等级别，对应不同的存储、传输与利用管控措施。流程管控方面，应建立覆盖数据全生命周期的管理流程，明确各阶段的责任主体、操作规范与监督机制。采集阶段确保数据来源可靠、内容完整；存储阶段确保介质安全、备份可靠；传输阶段确保通道加密、身份认证；利用阶段确保权限受控、行为可溯；共享阶段确保范围明确、协议规范；销毁阶段确保彻底清除、不可恢复[2]。

2.3 技术维度：防护手段与系统保障

技术维度是档案数据安全管理体系的重要支撑。防护手段方面，应采用加密技术保护数据存储与传输安全，采用访问控制技术限制未授权访问，采用审计技术记录操作行为，采用备份与容灾技术保障数据可用性，采用防篡改技术保障数据完整性。系统保障方面，应加强档案管理系统的安全设计与运维，定期开展漏洞扫描与渗透测试，及时更新补丁，防范系统层面风险。对于采用云服务的档案数据，应明确服务商安全责任，签订安全协议，定期开展安全评估。技术防护应与时俱进，关注零信任架构、区块链存证、隐私计算等新技术在档案数据安全中的应用。

2.4 制度维度：规范体系与监督机制

制度维度是档案数据安全管理体系的规范保障。规范体系方面，应制定档案数据安全管理办法、分类分级指南、访问控制规程、备份恢复规程、应急响应预案等制度文件，明确安全目标、责任分工、操作流程与考核标准。监督机制方面，应建立定期检查与专项审计相结合的监督制度，对制度执行情况、技术防护效果、人员操作行为进行检查与评估，发现问题及时整改。同时应建立安全事件报告与处置机制，明确事件分级、报告流程、处置措施与责任追究，确保安全事件得到及时有效处理。制度体系应与国家法律法规、行业标准衔接，确保合规性。

2.5 人员维度：安全意识与能力建设

人员维度是档案数据安全管理体系的关键环节。安全意识方面，应通过培训、宣传、案例教育等方式，提高全员对档案数据安全重要性的认识，使其了解常见威胁与防范措施，形成自觉遵守安全规范的行为习惯。能力建设方面，应针对不同岗位开展差异化培训，管理人员侧重制度设计与监督能力，技术人员侧重防护技术与应急处置能力，操作人员侧重规范操作与风险识别能力。同时应建立人员安全考核与激励机制，将安全表现纳入绩效考核，对违规行为严肃处理。对于外包人员与访问人员，应加强准入管理与过程监督，防范内部威胁。

3 档案数据全生命周期安全管理

3.1 采集阶段安全管理

采集阶段是档案数据全生命周期的起点，安全管理重点在于确保数据来源可靠、内容完整、格式规范。对于原生数字档案，应明确采集范围与标准，确保数据生成系统符合安全要求，采集过程有记录、可追溯。对于传统载体数字化副本，应确保扫描设备与软件安全可靠，数字化过程有质量控制，图像与元数据对应准确。采集阶段还应做好数据校验，防止采集过程中出现数据丢失或损坏。同时应建立采集登记制度，记录数据来源、采集时间、采集人员、质量检查结果等信息，为后续管理提供依据。

3.2 存储阶段安全管理

存储阶段是档案数据安全管理的核心环节，重点在于保障数据的完整性、可用性与长期可读性。存储介质应选择可靠性高、寿命长的产品，定期检测介质状态，及时迁移数据。存储环境应具备防火、防水、防尘、防磁、温湿度控制等条件，确保介质安全。存储架构应采用冗余设计，重要数据应异地备份，防范单点故障。数据组织应规范，元数据完整，便于检索与利用[3]。对于长期保存数据，应关注格式迁移与仿真技术，防止技术过时导致数据不可读。存储阶段还应建立定期巡检与备份恢复演练制度，确保备份有效、恢复可行。

3.3 传输与利用阶段安全管理

传输与利用阶段是档案数据安全风险较高的环节，重点在于防止数据泄露、篡改与滥用。传输方面，应采用加密通道传输数据，确保传输过程不被窃听或篡改；对于重要数据，应采用专线或离线传输方式，降低网络风险。利用方面，应建立严格的权限管理制度，根据用户角色与数据等级分配访问权限，实行最小权限原则；应记录利用行为，包括访问时间、访问内容、操作类型等，实现行为可追溯；对于敏感数据，应采用脱敏、水印等技术，防止二次传播。共享方面，应明确共享范围与条件，签订共享协议，明确双方责任，防止数据失控。

3.4 共享与销毁阶段安全管理

共享与销毁阶段是档案数据全生命周期的末端环

节，安全管理同样不可忽视。共享方面，应建立共享审批制度，明确共享目的、范围、方式与期限，共享过程应有记录与监督；对于跨部门、跨区域共享，应明确数据管理责任，防止共享后失控。销毁方面，应建立销毁审批制度，明确销毁条件、方式与监督要求；销毁方式应根据数据等级选择，一般数据可采用软件擦除，重要数据应采用物理销毁或多次覆写，确保不可恢复；销毁过程应有记录与见证，防止误销毁或恶意销毁。销毁后应及时更新数据台账，确保账实相符。

4 档案数据安全管理体系实施保障

4.1 组织保障与责任落实

组织保障是档案数据安全管理体系有效实施的前提。应建立由单位领导牵头、档案部门主导、信息技术部门配合、相关部门参与的安全管理组织架构，明确各部门职责分工。档案部门负责制度制定、业务指导与监督检查，信息技术部门负责技术防护与系统运维，业务部门负责本部门数据的安全管理。应落实安全责任制，将安全责任分解到岗位与个人，实行“谁主管、谁负责，谁操作、谁负责”。同时应建立安全协调机制，定期召开安全工作会议，研究解决安全问题，推动体系持续改进。

4.2 技术保障与投入机制

技术保障是档案数据安全管理体系有效实施的基础，充足的技术投入与先进的技术手段能够有效提升防护能力。应加大技术投入，配备必要的安全设备与软件，包括防火墙、入侵检测、加密设备、备份系统、审计系统等，形成多层次技术防护体系。应加强档案管理系统的安全建设，确保系统符合等级保护要求，定期开展漏洞扫描与渗透测试，及时修复安全隐患。对于采用云服务的单位，应加强云服务商安全管理，明确安全责任，签订安全协议，定期开展安全评估，防范供应链风险。应建立技术更新机制，关注零信任架构、区块链存证、隐私计算等新技术发展，及时引入适用的安全技术，提升防护能力[4]。同时应做好技术文档管理，确保系统配置、操作流程、应急预案等技术资料完整可查，为系统运维与应急处置提供依据。通过持续的技术投入与更新，保持安全防护的有效性与先进性。

4.3 评估改进与持续优化

评估改进是档案数据安全管理体系持续优化的动力，只有通过定期评估与持续改进，才能保持体系的适应性与有效性。应建立定期评估制度，对体系运行情况进行全面检查，评估内容包括制度执行、技术防护、人员操作、安全事件处置等，做到全覆盖、无死角。评估方法可采用自查、互查、第三方评估等方式，确保评估客观公正，避免自说自话。评估结果应形成报告，指出问题与不足，提出改进建议，明确整改责任与时限。应建立整改跟踪机制，对评估发现的问题限期整改，整改结果纳入下一轮评估，形成闭环管理。同时应关注外部环境变化，包括法规更新、技术发展、威胁演变等，及时调整体系内容，确保体系与国家要求同步、与技术发展同步、与威胁变化同步。通过评估—反馈—整改—优化的循环机制，推动档案数据安全管理体系不断完善，为档案数据长期安全提供持续保障。

结束语

本文从管理、技术、制度、人员四个维度构建了档案数据安全管理体系，该体系以分类分级为基础、以全生命周期为主线、以四维协同为支撑，形成覆盖采集、存储、传输、利用、共享、销毁各环节的管理闭环，可为档案数据长期安全保存与合规利用提供系统性保障。随着人工智能、区块链、零信任架构等新技术发展，档案数据安全面临新的机遇与更复杂的威胁环境。不同类型、不同规模的档案机构应结合实际，细化分类分级标准、优化技术选型、完善制度执行，推动安全管理从框架构建走向落地实施，确保档案数据在数字化进程中始终安全可控。

参考文献

[1] 赵乐. 智慧医院背景下档案数字化转型路径与安全管理研究 [J]. 兰台内外，2025(32):4-6.

[2] 郝瑞英. 档案数字化转型背景下人事档案管理模式创新与路径优化 [J]. 办公自动化,2026,31(5):77-79.

[3] 田戈. 数字化转型背景下档案治理现代化路径研究——以中国第一历史档案馆为例 [J]. 办公自动化,2026,31(10):53-55,92.

[4] 邱子桉. 数字化转型背景下的电子档案长期保存策略 [J]. 机电兵船档案，2026(2)：34-36.