档案信息化建设中数据安全防护实操方法研究

韦青松

中华人民共和国名誉主席宋庆龄陵园管理处，上海市，200336；

摘要：随着数字经济的不断进步，档案信息化已成为推动国家档案事业发展的重要方向。然而，在这一过程中，数据泄露、篡改及丢失等安全问题也逐渐成为不可忽视的风险。本文以档案数据安全保障中的“实践性”为重点，基于《数据安全法》《档案法》及相关行业标准展开讨论。首先探讨了加强数据安全措施的实际价值，随后深入分析了当前档案信息化进程中存在的技术落后、管理疏漏以及外部威胁等问题。最后，从技术实施、管理制度优化和法律法规对接三个层面出发，提出了包括全生命周期数据加密、分级分类信息脱敏处理以及明确人员责任分配等一系列可操作性强的安全策略，旨在为档案管理部门构建坚实的数据防护体系，并促进其信息化建设健康稳定地向前发展提供理论依据与实践指导[1]。

关键词：档案信息化建设；数据安全防护；实操方法；全生命周期管理；风险管控

DOI：10.69979/3041-0673.26.02.087

引言

近年来，《“十四五”全国档案事业发展规划》明确提出了‘加快推动档案信息化的战略转型，建立以数字化资源为主体的档案管理体系’的目标。随着这一进程的发展，档案管理正逐渐从传统的实体库房模式向更加现代化的数字平台转变。然而，档案资料因其同时具备高度机密性和法律证据价值——不仅涵盖了国家秘密和个人隐私信息，还涉及企业商业机密——其安全性对于维护国家安全、社会稳定及公民权利至关重要。目前，在一些档案管理部门推进信息化的过程中出现了重视建设而忽视安全防护的现象：一方面，它们可能过度依赖于如防火墙这样的传统技术手段，面对勒索软件攻击或针对性网络入侵时显得力不从心；另一方面，则是因为内部管理制度不够健全，导致因员工误操作或与第三方合作过程中发生的信息泄露事件屡见不鲜。因此，探索能够实际应用且易于推广的数据安全保障措施，不仅对于解决当前档案信息安全面临的主要问题具有重要意义，而且也是促使档案信息服务由基本可用迈向高度可信的关键步骤，这在实践和理论研究两个层面都展现出极高的价值[2]。

1 档案信息化建设中数据安全防护实操的重要性

1.1 保障档案数据核心价值的“底线要求”

档案资料作为历史记录的“数字载体”，具有不可替代性。如果因为保护措施不足而导致信息泄露（比如人事档案中个人身份证号码、薪资详情等敏感数据外泄）或被篡改（如工程项目文档中的施工周期、成本估算等关键数值遭到非法修改），不仅会损害个人利益，引发法律争议，更有可能破坏历史的真实性，使档案失去其应有的“证据价值”。举例 2023 年某地方档案馆由于未能实施有效的数据加密技术，导致馆藏民国时期的历史文献扫描件被非法下载并传播开来。尽管这一事件未构成严重的保密风险，但它显然违背了《档案法》关于“档案使用需遵循安全标准”的规定。由此可见，采取实际可行的安全防护策略是维护档案资料“真实性与机密性”底线的基础。

1.2 推动档案信息化可持续发展的“核心支撑”

在推进档案信息化的过程中，需要投入大量的人力和物力资源，比如数字扫描设备的购置以及档案管理系统的研发。然而，如果缺乏有效的实际操作层面的安全防护措施，之前的努力可能会因为一次信息安全事件而付诸东流。典型的案例是 2022 年某企业档案馆遭遇勒索软件攻击后，将近十年的财务记录数字化副本遭到加密处理。由于缺乏有效备份或备份数据已失效，该企业不得不支付巨额赎金但仍未能完全恢复丢失的数据，这直接导致其信息化进程停滞了一年之久。

1.3 满足法律法规合规性的“必然要求”

2021 年颁布的《数据安全法》明确规定，"数据处理者应实施必要的保护措施，确保数据不会遭受泄露、篡改或丢失"；而 2020 年更新版的《档案法》同样强调，在档案数字化的过程中，必须遵守国家的安全保密规定。值得注意的是，这些法律法规不仅仅是宽泛的原则性指导方针，而是具体指出了合规标准（例如数据分类与分级管理、紧急情况应对机制）。如果档案管理部门缺乏

有效的实践防护策略，可能会受到法律制裁——正如2023 年某省一档案馆因未能建立健全的数据安全管理机制而被地方网络信息安全监管机构要求整改，并受到公开批评。由此可见，采取实际操作层面的安全防护措施对于档案机构来说不仅是履行其法律责任所需，也是预防潜在合规风险的关键步骤[2]。

2 档案信息化建设中数据安全防护实操面临的现状

2.1 技术层面：防护手段“单一化”，难以覆盖全生命周期

目前，许多档案管理部门的安全措施仍处于较为被动的状态，主要依赖于防火墙和反病毒软件等基础性设施，未能全面覆盖档案数据从采集到销毁的整个生命周期。具体存在的问题如下：首先，在数据采集阶段，对于敏感信息（如文件上的印章或保密标记）未实施即时脱敏处理，导致原始资料直接暴露在外；其次，在存储方面，一些单位采取的是明文保存或是采用简易加密手段（例如设置简单密码），使得一旦服务器遭受攻击，内部数据极易被窃取；再者，在使用过程中缺乏精细化权限管理机制，普通员工能够访问到机密文档的所有内容，存在越权查看的风险；最后，关于数字档案的删除操作往往不够彻底（仅移除索引而未清除实际数据），这为非法恢复提供了可能。

2.2 管理层面：制度“空转”，人员安全意识薄弱

从一个角度来看，尽管一些档案机构已经制定了《数据安全管理制度》，但其内容多偏向于原则性的陈述（如“严禁泄露档案数据”），而缺乏具体的操作指导——比如，并未详细说明‘档案数据备份的频率、存储介质以及保管责任人’等关键信息，这导致了实际操作中备份工作往往流于表面。另一方面，人员层面的安全意识和技能也存在不足：首先，新进员工在没有接受充分培训的情况下就直接上岗，可能会因为不当操作（例如将保密资料上传至公开云盘）而带来安全隐患；其次，资深员工有时会过于依赖过往的经验行事，比如长时间不更换密码或对钓鱼邮件警告置若罔闻，2024 年某市档案馆发生的网络安全事件就是一个典型案例，正是由于工作人员不慎点击了含有恶意链接的电子邮件，才使得档案管理系统遭受木马攻击[3]。

2.3 外部层面：新型威胁频发，第三方管控存在漏洞

随着互联网技术的进步，档案数据所面临的外部安全挑战变得愈加复杂。首先，针对特定目标的攻击事件有所增加，尤其是那些对档案馆中存储的“高价值数据”（如历史机密文档、重大工程项目记录）发起的精确打击，其攻击方式已经从传统的病毒传播演变为更为隐蔽的供应链攻击（即通过渗透第三方软件来入侵档案管理系统）。其次，勒索软件的威胁成为常态，在 2023 年期间，全国多地发生了多起档案机构遭受勒索的情况，攻击者通过对数字档案进行加密后要求以比特币形式支付赎金，由于缺乏有效的数据备份措施，一些单位不得不屈服于此类威胁。此外，与外部合作伙伴之间的信息安全问题也日益凸显，在档案信息化过程中经常需要依赖外部服务商（例如文件扫描服务提供商、信息系统开发商），但若未与这些第三方签订详细的“保密协议”，并且不对它们的数据处理流程实施严格审查，则可能导致敏感信息被泄露的风险大大增加。

3 档案信息化建设中数据安全防护实操方法的策略探究

3.1 技术实操：构建“全生命周期+多层防御”的技术体系

3.1.1 数据加密：从“单点防护”到“全程加密”

加密技术构成了保障数据安全的关键防线，应当贯穿于档案数据管理的每一个环节，具体实施步骤如下：

①数据保护：利用 AES-256（高级加密标准）对存储于服务器内的数字文档实施加密处理，并引入“密钥分层管理机制”——由档案管理人员持有“访问密钥”，而机构领导则保管“备份密钥”，以此来防止任一人员独占所有密钥的风险；对于那些采用离线方式保存的资料（比如移动硬盘或 U 盘），必须激活“硬件级加密”功能，严禁使用未经加密的存储装置。

②数据加密传输：无论是进行“内部传输”（例如从扫描设备到服务器）还是“外部传输”（比如与其它机构共享档案），均采取 TLS1.3 协议进行加密处理，并且明确禁止使用 HTTP 等存在安全隐患的协议。如果需要通过电子邮件方式发送档案资料，则首先应对文件本身实施加密措施（例如设置压缩包密码保护），随后再以短信形式单独告知接收方相应的解密密码，以此防止“文件+密码”同时经由同一渠道传递可能带来的安全风险。

3.1.2 数据脱敏：结合“分级分类”实现“精准隐藏”

并非所有的档案数据都需要同等程度的安全措施，首先应当对其进行合理的分类与等级划分，随后依据其敏感度采取相应的脱敏处理。基于《档案法》与《数据安全法》的规定，我们将档案资料划分为三个安全级别：第一级为“绝密级”，适用于包含国家核心机密的文件；

第二级是“秘密级”，涵盖企业的商业秘密和个人敏感信息等重要资料；第三级则为“公开级”，指的是那些已经对外公布的历发文档。对于这三个级别的档案，我们建议明确标注其‘安全等级标识’，并在实际存储过程中依据各自的安全需求分别存放于不同的区域，例如，对于最高级别的绝密档案，应采取物理隔离的方式单独保存于特定服务器中[4]。

3.2 管理实操：建立“权责清晰+流程闭环”的管理机制

3.2.1 制度落地：从“条款”到“操作手册”

将理论化的制度框架转化为实际操作流程，并编撰《档案数据安全实操手册》，以明确下列关键要素：

①职位职责列表：明确界定“档案管理员”、“IT 运维员”以及“保密专员”的具体职能——例如，档案管理员需负责“数据录入过程中的脱敏审查”，IT 运维员承担“服务器加密及备份工作”，而保密专员则负责执行“每月一次的安全检查”，以此来防止责任归属不清的问题。

②操作流程标准化：对于核心步骤，制定了详尽的“step-by-step”指南，例如《档案扫描录入流程》中规定了以下几点：在开始扫描之前，必须确认设备已安装反病毒软件；扫描过程中，对涉及敏感信息的部分即时进行匿名处理；扫描完成后，需要两名工作人员共同验证数字版本与原始文件的一致性；最后，在上传至服务器之前，还需再次执行加密措施。

③激励与惩罚机制：对于能够严格遵守安全防护规定的员工，应予以表彰（如授予年度“安全标兵”称号）；而对那些违反规定的行为（例如未经加密即传输文件），则需根据违规行为的具体情况施以相应的处罚措施，从“警告—罚款—暂停工作”逐级递进。若因个人不当行为导致了数据泄露事故的发生，则必须依法承担相应的法律责任。

3.2.2 人员培训：从“灌输”到“实战模拟”

提升人员安全意识需“理论+实操”结合，具体培训方案如下：

培训安排及其内容概述如下：每年四个季度各举行一次关于安全意识的教育活动，涵盖三个主要方面。首先是法律知识的学习，具体包括对《数据安全法》及《档案法》中关键条款的理解；其次是针对潜在威胁的认知能力培养，例如教授如何辨别钓鱼邮件与恶意链接等技巧；最后，则是实践技能的训练，比如掌握加密工具的操作方法以及熟悉紧急情况下的应对流程。

实战模拟训练：每年定期举办两次“安全应急演练”，针对“勒索病毒攻击”与“员工误删数据”等紧急情况，指导员工依据手册完成从“隔离受感染设备—启动远程备份—恢复资料”的一系列操作。每次演练结束后，均会进行回顾总结，识别存在的不足之处，并据此不断优化应急响应流程[5]。

3.3 法规衔接：从“合规”到“主动对标”

为确保数据处理活动符合相关法律法规要求，每年将委托独立第三方机构执行“数据安全合规评估”。该评估依据《数据安全法》、《档案法》以及《信息安全技术档案信息系统安全等级保护基本要求》（GB/T30228-2013）进行，重点检查包括但不限于加密算法的有效性及备份策略的合理性等关键指标。评估完成后，将编制《合规自查报告》，其中列出的所有不符合项均需在规定时间内完成整改。此外，每三年需进行一次等级保护评估，以确保该系统持续符合既定的安全标准。

4 结束语

档案信息化建设中的数据安全保障并非一劳永逸的任务，而是一个需要技术、管理和法规三方面协同作用的动态进程。本文探讨了“全生命周期加密”、“分级分类脱敏”以及“实操手册落地”等策略，旨在解决现有防护手段‘难于实施、缺乏具体性’的问题，为档案管理单位提供一套切实可行的方案。展望未来，随着人工智能与区块链等新兴科技的进步，档案信息安全保护有望迎来新的飞跃，唯有不断探索和创新实际操作模式，才能在档案信息化进程中构建起坚实的‘安全防线’，使数字档案成为真正意义上的‘可靠、可用、可控’的信息财富。

参考文献

[1]李奕婷.档案信息化建设中数据安全风险及防范策略研究[J].办公自动化,2025,30(16):76-78.
[2]王彩霞.企业财务信息化建设中数据安全防护策略与技术创新研究[J].市场瞭望,2025,(12):46-48.
[3]张静.浅析城市管理局档案信息化建设中的安全防护策略[J].四川劳动保障,2025,(10):36-37.
[4]刘艳超.档案信息化建设中的数据安全与隐私保护策略研究[J].信息系统工程,2025,(04):105-108.
[5]周黎芳.粮食储备档案信息化建设中的数据安全保护研究[J].粮油与饲料科技,2025,(01):119-121.

作者简介：韦青松，女，汉族，籍贯：江苏，学历：大学本科，职称：馆员，研究方向：档案管理。