 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i7.30325

Information security risks and prevention and control strategies of archives in new era public institutions

Liang Xu

Etuoke Front Banner Confidentiality Technology Service and Confidential Carrier Destruction Center, Ordos, Inner Mongolia, 016200, China

Abstract

As digitalization continues to advance, the management of archives in public institutions is increasingly moving towards informatization and networking. However, this shift has also brought about growing concerns over information security risks. In the new era, archive information, as a core asset of organizations, has become a critical factor in ensuring business continuity and the stability of government operations. Public institutions currently face a variety of archive information security risks, including data breaches, tampering, loss, and system intrusions. These risks stem from inadequate management systems, lagging technical defenses, weak employee awareness, and frequent external attacks. To address these challenges, this paper examines the manifestations and root causes of archive information security risks in public institutions from three perspectives: information technology, management systems, and personnel competence. It proposes a comprehensive prevention and control strategy that includes technical protection, mechanism building, and supervision and assessment, aiming to provide theoretical support and practical guidance for enhancing the level of archive information security in public institutions.

Keywords

public institutions; archive management; information security; risk identification; prevention and control strategies

新时代事业单位档案信息安全风险与防控策略

徐良

鄂托克前旗保密技术服务和涉密载体销毁中心，中国·内蒙古 鄂尔多斯 016200

摘　要

随着数字化建设的持续推进，事业单位档案管理逐步向信息化、网络化方向发展，但随之而来的信息安全风险问题也日益凸显。在新时代背景下，档案信息作为组织核心资产之一，其安全性已成为保障单位业务连续性和政务运行稳定性的关键要素。当前事业单位面临的档案信息安全风险类型多样，包括数据泄露、篡改、丢失、系统入侵等问题，风险成因既有管理制度不完善、技术防护滞后，也涉及员工意识淡薄与外部攻击频繁等复杂因素。针对这一现实挑战，本文从信息技术、管理制度与人员素养三个维度出发，系统分析事业单位档案信息安全风险的表现形式与形成根源，提出了涵盖技术防护、机制建设、监督考核在内的综合防控策略，旨在为提升事业单位档案信息安全水平提供理论支撑与实践参考。

关键词

事业单位；档案管理；信息安全；风险识别；防控策略

1 引言

新时代背景下，事业单位在推动政务公开、信息共享和数字化办公进程中，档案管理工作迎来深刻变革。传统纸质档案逐步向电子档案转型，信息资源的集中存储与联网使用提高了工作效率，也带来了前所未有的信息安全挑战。档案信息一旦遭受破坏、篡改或泄露，不仅会影响单位正常运作，甚至可能引发行政责任或法律风险。尤其在涉及涉密、民生、财务等领域档案时，其安全性与完整性更为敏感与关键。当前，部分事业单位在档案安全防护方面仍存在制度缺失、技术薄弱、人员操作随意等问题，亟须构建起一套系统化、可持续的风险识别与防控机制。为此，本文聚焦档案信息安全风险的种类、成因与防控路径，探讨其在制度设计、技术应用与队伍建设中的优化对策。

2 事业单位档案信息安全面临的新形势

信息化建设持续推进带动事业单位档案管理工作全面升级，从传统纸质载体向数字化、网络化管理模式快速转型。电子档案生成数量呈指数增长，对存储容量、检索效率、数据完整性等方面提出更高标准。新技术的引入使档案管理系统与单位办公平台实现深度整合，提高了档案利用效率与协同处理能力。同时，信息化环境下的档案管理需适应数据跨平台流转、多设备访问与系统异构等复杂应用场景，对档案

【作者简介】徐良（1988–），男，中国内蒙古鄂尔多斯人，本科，中级馆员，从事档案管理研究。

安全性、保密性与可追溯性提出更高要求。信息技术对档案工作的赋能既拓展了管理边界，也加大了风险暴露面，推动单位亟须更新管理理念、提升安全保障手段，构建与信息化水平相匹配的档案安全体系。部分单位在系统建设中未配置完整的防护链条，使得档案系统容易成为攻击突破口。此外，信息安全事故影响范围从单一部门扩展至单位整体运转，甚至可能引发外部法律追责或声誉危机，档案信息安全问题已不再局限于技术层面，而是演化为多维度综合性挑战。

3 事业单位档案信息安全主要风险类型分析

3.1 电子档案存储介质的物理损毁与技术故障风险

电子档案依赖磁盘、固态硬盘、光盘等介质进行存储，随着使用年限增长，介质表面损耗、读写错误率升高，极易造成数据不可读、丢失或错位。存储设备遭遇意外断电、电压不稳、水火灾害时，也可能直接造成物理性损毁。部分单位在建设档案库房时忽视温湿度、静电、防磁等环境要求，进一步加剧介质失效概率。同时，系统故障、文件格式损坏、软件兼容性差亦可能导致档案数据无法正常调用或解析。传统存储模式缺乏冗余备份与异地灾备机制，存储路径不规范、恢复机制不健全，导致数据一旦损坏无法有效恢复，严重影响档案信息的可用性与完整性。

3.2 网络攻击与数据泄露引发的信息外泄风险

事业单位广泛使用的办公自动化系统、电子档案管理系统普遍接入外网，数据传输与存储过程面临网络攻击威胁。攻击方式包括 SQL 注入、DDOS 攻击、系统漏洞利用等，攻击者可获取用户凭证、权限信息甚至访问核心档案库。部分单位未实施访问权限分级控制，导致普通用户可获取大量敏感信息，增加泄密概率。电子档案在移动存储介质、邮件、云平台等渠道传输过程中，若未加密处理，极易被第三方窃取或篡改。单位内部网络未设隔离机制，病毒入侵后可迅速蔓延，影响范围扩大至整个信息系统。数据泄露事件不仅损害单位声誉，更可能违反国家保密法规，带来严重行政与法律后果。

3.3 人员操作不当导致的档案篡改、丢失风险

档案管理过程中人员因素是引发信息安全事故的重要环节。部分工作人员因缺乏专业培训，对档案系统操作不熟悉，在日常管理中出现误删除、误格式化、误修改等操作，导致档案数据损坏或丢失。少数员工因安全意识薄弱，使用弱密码或在公共设备上登录管理系统，造成账号被盗或权限滥用，进而发生非法修改、导出或破坏档案的行为。在权限配置不合理的环境下，一线操作人员可能拥有过多敏感信息访问权，形成安全隐患。单位在工作交接、人员离岗时若未及时回收账号权限、转移资料归属，也可能导致重要档案流失。人为操作带来的非预期性事件，是当前档案信息管理中最具不确定性和突发性的风险来源。

4 档案信息安全风险形成的根源因素

4.1 管理制度滞后与岗位职责划分不清

部分事业单位档案管理制度尚未与信息化发展相适应，缺乏与网络安全、数据治理相关的管理细则，对电子档案的生成、归档、存储、销毁等关键环节未形成闭环机制。规章制度笼统、条款空泛，未能明确风险识别、分级防控、事件响应等关键职责，导致管理人员无所适从。岗位职责划分不清，安全责任未能落实到人，出现问题时互相推诿、处理滞后。在权限审批、数据审计、系统维护等方面缺乏日常规范流程，也缺乏制度化考核机制，致使安全管理流于形式。制度与实际脱节，无法有效指导操作实践，是档案信息安全难以保障的重要诱因。

4.2 技术保障薄弱与信息系统防护能力不足

部分事业单位在档案信息化建设中投入不足，系统硬件老旧、软件版本落后，缺乏主动防御和安全监测能力。信息系统未部署入侵检测、防病毒、行为分析等安全组件，系统更新维护滞后，存在大量已知漏洞未修补，极易成为攻击入口。档案数据未实行加密存储与传输，缺乏完整的备份机制，一旦遭受攻击或意外损坏，数据恢复难度极高。运维力量薄弱，缺乏专职技术人员从事网络与数据安全维护，外包技术服务缺乏监督约束，存在安全配置错误、维护不及时等问题。防护体系建设滞后，严重制约档案信息安全水平的提升。

4.3 员工安全意识淡薄与违规行为频发

在管理方面，部分事业单位未建立档案信息安全培训机制，员工普遍缺乏安全风险认知和应对能力。工作人员在操作系统时随意设置密码、重复使用账号、使用外部 U 盘拷贝文件等行为普遍存在，极易形成系统漏洞。缺乏保密责任意识，处理涉密档案时未履行审批程序或使用不合规设备传输资料。在网络环境中存在将档案资料上传至无监管平台、使用社交工具传送敏感文件等违规现象。单位对违规行为缺乏警示与惩处机制，导致违规行为频发却未被纠正，进一步放大风险传导链条。人员行为不可控性是档案信息安全中最难防范的风险点，需要通过制度建设与意识提升双重机制予以约束和管控。

5 事业单位档案信息安全防控的技术路径

5.1 构建多层防火墙与访问权限控制体系

档案信息系统需通过纵深防御理念构建多层次网络安全结构，将单位内部网络划分为多个安全区域，在各关键节点部署防火墙设备，实现访问边界隔离与非法流量拦截。根据使用岗位与职能不同，制定精细化权限分级策略，采用“最小权限原则”控制用户访问范围，确保每一类档案数据的读取、修改、删除操作均在授权范围内进行。结合用户身份验证机制、双因素认证和动态权限调整等技术手段，提升系统抗渗透能力。对于高敏感度档案，应启用访问记录功能与实

时告警设置，防止越权操作与未授权下载，形成从入口管控到行为追踪的闭环防护体系。

5.2 推进档案数据加密与容灾备份机制建设

在档案信息管理过程中，应全面引入数据加密技术，实现存储加密与传输加密双重保障。采用国密算法或 AES 高强度加密标准对关键档案数据进行加密封装，防止信息在存储介质或网络通道中被截获或解密。为提升系统抗灾能力，应建设异地数据备份中心，设置实时同步机制与定期全量备份机制，确保在突发情况下可通过镜像数据迅速恢复档案内容。备份系统需配套防篡改功能与访问控制策略，防止备份文件被恶意修改或删除。对关键档案还可引入分布式存储技术，增强容灾能力，降低单点故障影响，保障档案信息在突发事件中的完整性与可用性。

5.3 应用日志审计与异常行为识别等智能监测手段

信息系统应配置完善的日志记录机制，对用户登录、文件操作、权限变更、系统设置等行为进行实时记录与归档管理。通过日志审计工具对历史数据进行回溯分析，可追踪违规操作来源与责任人，形成有效的行为约束机制。在此基础上引入智能监测模块，利用行为模式识别算法建立用户行为基线，对访问频次、操作路径、文件调用等异常行为进行自动识别与预警。系统可设定风险等级分级响应方案，当异常行为触发阈值时自动发出告警、冻结账户或锁定敏感数据，提升威胁应对时效性。智能化手段增强了对未知威胁的识别能力，为档案系统提供主动防御支撑。

6 事业单位档案信息安全防控的管理策略

6.1 完善制度体系与岗位责任制落实机制

建设统一规范的档案信息安全制度体系，应覆盖电子档案生成、存储、传输、使用、销毁等全生命周期管理环节，并明确各岗位的安全职责边界。制度中应细化档案分类分级管理标准、安全访问权限配置要求及违规操作处置流程，推动管理工作流程化、标准化。通过将档案信息安全目标纳入单位年度绩效考核指标，强化责任制传导机制，确保安全管理要求落实到具体科室和人员。对于关键岗位应设立安全责任人，并建立定期安全检查与问题反馈机制，形成从制度设计到执行监督的完整闭环，提升制度在工作中的操作性与有效性。

6.2 强化人员培训与日常操作规范化管理

事业单位应定期组织档案管理与网络安全相关的专项培训，提升员工对档案信息风险的认知水平与防护能力。培训内容应涵盖电子档案系统操作规程、保密要求、安全操作习惯等，结合典型案例讲解违规操作可能带来的后果，增强风险意识。操作规程应以文字手册、视频演示等多种形式下发并定期更新，保障操作标准的一致性。在工作中加强对 USB 设备、外网登录、资料下载等高风险操作环节的流程监管，防止因随意操作引发系统漏洞。针对新进人员与岗位变动应设置岗前培训机制，建立动态适应的操作规范体系，推动安全管理常态化、精细化。

6.3 健全监督考核与信息安全事件应急处置机制

构建全周期的信息安全监督机制，应包括常态化安全巡查、突发事件排查、违规行为追责三类监督路径。单位应设立安全监督专岗，负责定期检查权限配置、日志记录、系统漏洞等关键内容，发现问题及时整改。对信息安全管理执行情况开展定期评估，并与单位考核、奖惩机制挂钩，提升全员履责主动性。应急处置机制需建立快速响应与分级处置流程，涵盖突发病毒感染、系统崩溃、数据泄露等常见场景，明确信息报送、技术响应、责任追溯等具体环节。通过预案演练、应急培训等方式提升队伍协同处置能力，确保安全事件在最短时间内得到控制与修复。

7 结语

档案信息安全已成为新时代事业单位治理体系中的关键环节，关乎组织运行稳定与信息资产完整。面对信息技术快速演进与风险类型持续扩展的双重挑战，必须从制度、技术与人员三方面协同发力，构建全面、精准、高效的防控体系。在推动档案管理数字化、智能化转型的过程中，安全保障不能滞后于管理创新，防控机制必须嵌入各环节、全流程。唯有形成制度明晰、责任落实、措施得当的安全格局，方能有效防范潜在威胁，保障档案信息安全稳定运行，为事业单位高质量发展提供有力支撑与制度保障。

参考文献

[1] 刘真. 新媒体视野下机关事业单位声像档案开发研究[J].兰台内外,2025(18):72-74.

[2] 史洁. 基于大数据的事业单位办公室文书档案管理研究[J].兰台内外,2025(19):5-7.

[3] 莫晶. 基层事业单位档案管理中电子信息化建设的实践分析[J].兰台内外,2025(19):20-22.

[4] 陈少敏. 关于事业单位人事档案管理信息化建设的分析[J].兰台内外,2025(19):26-28.