加强档案管理安全风险防控的措施探讨

杨静
巨野县人民医院

摘　要：随着社会经济快速向前发展，人们生活方式发生了翻天覆地的变化，各行各业都取得了突破性进展，不仅面临着诸多机遇，同时也面临着更多挑战。在大数据背景下，传统的档案管理工作方法、理论等都面临挑战，档案管理工作必须紧跟时代发展步伐，及时革新基础理论、优化工作方式，以此提高工作的可靠性、安全性、有序性、高效性。作为档案管理工作人员，必须了解大数据时代背景，并着手将大数据信息技术用于档案管理，才能确保档案管理安全风险防控工作的质效。

关键词：档案管理；安全风险；防控
【DOI】10.12252/j.issn.2096-6288.2022.04.052

引言

通过科学合理、现代高效的方式对档案信息进行分类整理及开发使用，可以有效总结事业单位在发展运行中的历史经验。在管理中，事业单位可以明确自己的不足及薄弱之处，制定方案，落实贯彻，从而解决问题，让档案的功能发挥得到最大化。当前，事业单位在档案管理安全风险防控工作方面所呈现的整体情况并不理想，依旧有一些问题制约档案功能的发挥，不利于事业单位的健康稳定发展。

一、档案管理相关概述

档案管理指的是人们对社会活动中形成的、具有应用价值的材料信息进行保存管理的工作，该工作能够保障档案信息的真实性和可靠性。在事业单位发展过程中，档案管理能够提升档案资料的保存、调阅、管理效率，为事业单位各项工作的开展提供有力参考和支持，对事业单位的长远发展有着不可忽视的重要价值。就事业单位的实际发展情况来看，其工作内容具有一定复杂性，形成的档案信息往往涉及社会、经济、政治等多个领域，对这部分档案信息进行妥善保存和应用，是进一步推动事业单位发展进步的重要工作。目前，已经有越来越多的事业单位认识到档案管理的必要性，并通过建立档案管理制度等方式，优化档案管理工作。

二、档案管理中存在的风险隐患

（一）档案管理认知不充分

各级各类档案管理部门或单位中的多数人员常年在传统管理模式中工作，对大数据相关技术的认知不够，即使建设信息化管理系统，仍采用较为传统的思维认知关键去开展工作，管理方式与思维高度无法做到与时俱进。同时，缺少较为完善的信息化管理规范，没有统一的标准体系，集中管控、资源整合力度不够，无法充分发挥大数据时代档案管理的优势。在信息资源管理、分析、挖掘、利用等方面仍然处于较低水平状态，整体工作层次较低，严重制约了档案行业的快速发展。

（二）缺少专业性档案管理人员

工程档案管理本质上为一项严谨、科学、系统性工作，现实中事业单位往往会忽视工程档案管理工作的专业性，工作人员多为普通文员或新入职员工，缺乏足够的专业知识体系以及档案管理技能，进而导致档案管理工作多为被动接收，且由于工程类档案资料种类多、收集难度大，缺失专业性人员，更易引起档案质量不高、资料不全、整理效率低等问题。

（三）档案信息安全受到冲击

档案安全是档案工作的底线和红线。信息技术的飞速发展，既为档案安全提供了安全外衣，但也面临着新技术的冲击。近年来，事业单位按照《文书类电子档案检测一般要求》《档案信息系统安全保护基本要求》等工作标准，在电子档案的检测和管理等方面积累了丰富的经验和做法。重要档案资料实行异地备份、异质管理、多套备份等形式。但是，近十年来，伴随大数据、互联网+、人工智能等技术全面渗透到机关事业单位信息化的全流程，智慧化管理成为档案信息化的现实指向，但是这些技术相较传统的网络通信数据库等比较成熟的技术，其安全性和稳定性显然还不够。这也正是近年来频频曝出大数据侵犯个人资料和隐私等问题的原因。档案的原始性、真实性决定其出现安全问题是不可挽回的损失。档案信息安全与数据隐私保护的威胁与日俱增，信息安全风险产生一系列的连锁反应。从档案的管理、利用、数字档案室的运营各环节都需要进行重塑或安全防护。物联网技术在事业单位机关档案管理中广泛应用于档案实体、建筑硬软件中，但是也面临着“信息安全”有关的挑战。主要是档案具有保密的属性，有些档案资源的利用有限度和要求，超出一定的范围和层

次，可能会给部分群体和社会公众带来危害。因此，档案的保密性要求某些档案信息不能随意上网公开，需要分级利用、有序开放。

（四）档案安全性没有实现全流程覆盖

在事业单位档案信息化建设过程中，电子设备高度依赖于各类网络，网络安全水平没有随着信息化工作的开展而提升。由于互联网环境多种多样、繁多复杂，在每个环节都存在不少危险因素，对已形成的电子档案资源造成不小的威胁。存储介质的损坏或者故障，会直接导致数据丢失；网络黑客、病毒的入侵，会使系统崩坏，严重影响正常工作开展；地震、洪水等自然灾害，很有可能对档案数据造成不可逆伤害。所以，安全性问题必须引起各事业单位高度关注。事业单位的综合档案管理与单项档案管理不同，存在很多级别类型的涉密档案，档案管理人员的业务水平、职业道德如果没有得到专业的培训，保密意识、法律意识达不到要求，很容易踏入违法红线，造成麻烦。

三、加强档案管理安全风险防控的措施

（一）扩宽应用渠道，提高数据安全性

将大数据信息技术应用于档案管理工作能有效开发数据信息，还赋予档案管理更多价值。社会不断发展背景下，工作人员需扩宽应用渠道，展现数据的优势，进而推动行业的发展。工作人员应主动学习大数据信息技术，认识大数据信息技术与服务的关系，革新理念，积极发挥信息技术作用，将有价值的信息持续提供给用户；此外，工作人员可用大数据技术分析用户获取资料的流程，明确用户需求，确保准确掌握管理工作的关键点、明确关键数据内容。已收集的信息中，工作人员需再次利用信息技术挖掘信息价值，保障数据真实有效，同时，将有价值的信息分享给用户，确保数据发挥作用。为确保每项管理工作有序展开，工作人员需将已有的资源进行整合，发挥网络、计算机及大数据信息技术的优势，创建新的管理平台。同时简化操作程序，提高操作的便捷度，保障数据安全。根据工作要求，充分发挥出大数据信息技术的优势，整合工作流程，提高管理工作的质效；同时加深档案管理信息技术的应用深度，提高应用水平，持续构建网络化的管理平台。此外，不断完善工作制度，强化管理工作，保障信息安全。

（二）强化档案安全性

事业单位应该注重档案数字化管理安全制度的建设与完善。档案作为一个具有较高参考价值和机密性的资料，其中有部分可以对外公示，但有的部分则需要保密管理。做好安全管理就显得尤为重要。在档案数字化安全管理中不仅应该包含硬件安全管理，也包含软件系统的安全管理。第一，在硬件安全管理中，相关人员应该在采购过程中严格把控好信息储存载体的质量，保障硬件使用期限，为电子文件管理提供基础保障。对于储存电子文件的设备以及介质都应该委派专门人员负责，以避免硬件设备长期使用出现故障问题，导致电子文件完整性受损；第二，在软件管理中，技术人员需要对软件安全防护系统建设并定期优化升级。对外，建设完善的网络防火墙和监管系统，一旦发现非法入侵或攻击行为及时预警；对内，结合各部门工作需求设置软件系统访问权限和密码管理，避免电子档案数据信息泄漏，给事业单位带来不良影响；第三，在档案数字化建设进程中，不少事业单位会将其外包给专业机构。在这一过程中，从档案收集、整理、录入、操作再到重新入库整个过程中都存在被泄漏风险。对此，应该明确好外包人员的工作职责、任务要求、质量保证及保密要求等，必须使用合同、规章制度等对其约束。在数字化档案建设完成后，专业承办机构的服务器及终端文件需要全部移交给档案管理部门，并要彻底删除外部资料。此外，事业单位还应该利用信息技术在档案数字化管理系统中对档案数据信息展开实时监测，对于其中存在的问题及时修复与干预，避免发生档案管理安全隐患。这样就能够实现标准统一、规范科学的档案数字化管理模式，保障档案安全。

（三）识别收集非结构化数据

（1）识别收集非结构化数据（电子图像文件），能够将显式知识转化为结构化数据并有效保存。通过知识图创建主题，并根据不同的项目维度查询、汇总和上传相关档案材料的主题结果。通过纸质档案数字化和增量档案电子化管理档案资源，提供统一集中的管理平台，实现合规审批和权限管理；（2）提供固化的业务流程和审批内容，为事件跟踪提供有力证据。同时，高性能备份和恢复可以确保文件数据的高效和快速备份，并确保元数据、扩展元数据和对象存储数据的一致性，平均备份和恢复速度高达300MB/s，能够有效解决海量文件数据的备份问题。通过规范多类别、多格式和多类型档案的元数据管理，可以有效整合、存储、发布和利用各类档案数据，为档案管理与业务的互联互通奠定坚实基础，成为信息资源中心，促进数字化转型。其优点主要在于：一是能够实现档案全生命周期管理，创新性地将内容管理平台与文件系统相结合，实现电子文件管理向前端业务的延伸。依靠内容总线架构和丰富内容服务，实现文件管理、保存和利用，最终将“死”文件转

化为“活”数据。二是能够实现档案收集自动化，提供多种标准接口，支持与上游业务系统的无缝连接，实现各类档案数据的自动采集、电子文档接收后的自动归档以及四性检测的自动归档。三是能够实现智能文件搜索，海量数据的毫秒级快速检索能力支持通过全面搜索、图像搜索、知识搜索和推荐，精确检索文本、图片、音频、视频和其他类型的文件。同时，基于语义分析，可以理解用户的搜索意图，通过智能图像识别准确搜索图片，并通过知识网络主动推荐知识文档，还能够折叠类似的结果，以使搜索结果更准确。

（四）明确数据边界，确保数据保密

设定档案数据安全区域边界，保障整个档案数据全流程的正常安全运转，同时提升防御内外部攻击和入侵的能力，是档案数据安全管理的关键。参考云数据安全防护技术，可对进出档案管理流程的数据进行基于应用协议和应用内容的访问控制，做到病毒查杀、流量管理、VPN等安全功能防护，在实现应用级细粒度访问控制的基础上，同时具备恶意代码防范、网络带宽优化、远程加密的接入能力，并提供可靠持续性的防护，做到档案数据边界明确。

（五）档案资料云储存

事业单位档案管理工作具有一定复杂性，将信息技术应用到档案管理工作中，是保证档案管理效率、防止档案资料丢失的重要手段。在具体应用过程中，工作人员往往利用扫描仪等设备，将档案资料从纸质文件转换成电子文件，并利用特定的终端存储设备将其保存，为了避免电子档案丢失，还需要将文件备份。值得注意的是，为了确保档案信息的安全性，在充分发挥云存储技术积极作用的前提下，也可以利用可靠的数据加密技术逐级验证访问者的身份信息，以此避免档案资料丢失等一系列问题。另外，为了保证档案资料云储存效果，档案管理工作人员还需要合理利用先进的信息技术，在综合考虑事业单位档案管理工作具体需求的基础上，增设档案管理系统的功能模块。特别需要提到的是，为了让事业单位档案资料云储存取得实质性效果，工作人员可以充分运用虚拟化技术对特定设备进行虚拟化处理，从而为档案资料云储存打下坚实的基础，还需要通过合理利用数据加密技术提升档案资料的安全性，在保证档案资料正常使用的基础上，避免黑客入侵、病毒传播等带来的安全隐患。同时，还可以利用身份认证识别技术，对档案资料予以安全保障，通过用户名加密的形式完成用户身份的识别和认证，避免非法用户入侵等一系列问题，确保事业单位档案管理工作的安全有效性。

（六）推动专业人才培养

随着社会各界网络系统性安全能力提升需求的增加，相关上级部门应愈加重视档案行业网络与信息安全人才培养，逐步构建并完善人才成长体系。一要以产业发展、工作实践、市场需求为动力和准则，立足于补齐网络安全人才及创新能力的短板，形成政府机构、学校、事业单位等多方紧密协作和共同参与的人才培养机制。二是要形成政府和档案主管部门、网络安全产业研究和人才服务机构、教育培训实施主体以及用人单位多方共建模式，通过举办各种比赛、竞赛，提供实战场景，以赛促学，从而发现和培养更多安全人才，促进网络安全人才能力标准不断完善。三要在社会中广泛开展全民数字素养和网络安全意识提升行动，落实国家安全教育规划中的网络安全进单位、进学校相关政策，通过完善的职业教育、学历教育专业布局和人才培养模式改革，建立一个导向和分工明确，指导和保障有力，方法和标准先进的网络安全人才发展体系。

结语

综上所述，事业单位档案安全风险管理是一项重要的工作，引进新型管理技术迫在眉睫。因此，事业单位不仅要加强制度建设，还要提升档案管理人员的素质，升级档案信息化管理的管控机制，从而确保档案管理安全风险防控工作为事业单位发展发挥最大价值。

参考文献

[1]邓梦茹.大数据技术在网络安全分析中的应用研究[J].无线互联科技，2021，18（12）：19-20.

[2]王雪.企业档案管理存在的问题和解决措施[J].兰台内外.2021，（36）.41-42.

[3]张雁翔.高校数字档案信息系统的网络安全策略研究[J].科技资讯，2018，16（06）：15+17.

[4]朱一姝，吴涵宇，马明.大数据技术在信息时代网络安全管理系统中的应用概述[J].通讯世界，2019，26（11）：155-156.

[5]刘维红.简论企业档案管理风险防控[J].中小企业管理与科技.2019，（22）.

[6]欧清.浅谈档案信息系统的网络安全保护技术[J].云南档案，2009（05）：29-30.

[7]薛涛，刘潇潇，纪佳琪.大数据时代的计算机网络信息安全技术应用——评《大数据与计算机技术研究》[J].中国科技论文，2021，16（08）：938.

[8]林秋利.解析事业单位档案信息安全管理问题[J].经济学，2020，3（3）：72-73.