

# 浅谈如何做好档案信息的安全管理

刘锦

中国人寿保险股份有限公司陕西省分公司

**摘要:**随着我国大数据技术的快速发展与广泛应用, 各行各业的信息数据量大量增多, 档案信息的安全管理工作也面临前所未有的压力与挑战。对于传统纸质档案而言, 档案信息安全管理主要是指对于物理损毁、人为遗失、夹带偷盗为主的防护模式。这一模式显然已无法满足大数据时代下网络化、数学化的档案信息安全管理需要。如何处理好海量档案信息资源在数字化时代的安全管理, 是全社会当下都值得探讨的重要话题。因此, 需要档案管理人员积极适应时代发展需求, 建立与完善档案信息安全管理机制, 主动利用大数据技术, 研究探索大数据时代背景下档案信息安全管理的具体改革方式。本文就是对大数据时代档案信息安全管理策略开展的一些分析与研究。

**关键词:** 档案管理; 安全; 措施

**【DOI】** 10.12252/j.issn.2096-6288.2022.03.155

**前言:** 随着档案信息资源的逐步增多, 纸质档案的使用率与利用率日益降低, 海量的档案信息数据对传统档案系统造成强烈的冲击, 档案管理开始探索与建立满足时代需求的全新管理方式。而大数据技术的发展与广泛应用, 虽提升了传统档案信息管理工作效率, 但受电子信息管理自身性质的特点影响, 其仍然有被篡改、摄取、丢失、泄密等多方面的安全隐患风险。因此, 提高大数据时代下档案信息的安全管理水平是当下档案管理的重要工作内容。该文主要分析大数据时代档案信息安全管理价值与要求, 讨论与探究新形势下, 档案信息安全管理的具体策略。

## 一、大数据背景下档案信息安全风险

### (一) 网络风险

数字化档案信息的安全风险来自多个层面, 包括外界的网络、内部的工作人员以及内部的信息设备等。在互联互通的大数据时代, 网络黑客的攻击以及病毒传播是数字化档案第一个要面临的风险, 即使是外部隔离内部局域网仍可能产生网络失密、窃密风险。由于数字化档案信息的主要功能就是向公众人群提供网络平台查询利用服务, 在这一过程中就为黑客或病毒提供了非法入侵窃密的可能。在一些单位的内部的局域网中也有不少安全风险, 虽然这些部门服务的用户有特定的限制, 不对公众开放, 但是依旧存在非法获取信息的行为, 比如有外国机构在一些理工类关键科研院所周边布设探测校内WiFi热点, 伺机散布木马病毒以实施窃密行为。还有一些权限内的档案信息合法使用者出于牟利的目的, 跨权限或者利用自身的权限非法拷贝复制内部局域网的档案信息, 然后出售牟利, 或者是为了显示自己技术较好, 故意控制档案信息管理程序, 使信息受到破坏。由此可见, 有效应对网络失密窃密风险是档案信息安全工作核心重点。

### (二) 系统风险

档案信息平台所保存的档案信息, 有时真实性、完整性和其他方面的一些性能会受到影响, 数字档案信息的安全首先要保证电子文档的真实性, 经得起检验, 具有完整的特点。然而由于采集、归档、录入、维护等环节存在的人为控制删改的主观因素导致档案信息不真实, 或在操作计算机时可能出现的难以预料的机械故障等客观因素导致虚假保存, 或计算机操作系统、档案管理系统因更新软件错误导致档案数据格式化清除覆盖, 或是旧数字编码被无法被新的操作系统识别, 而旧操作系统已淘汰无法重新启用。对于上述问题, 就必须要求数字化档案信息平台的系统运行逻辑具备AI高容错性, 能够在用户操作失误时及时提醒或主动备。但目前本人见到的一些档案信息平台容错性设计不足, 一旦发生异常情况, 数据不能够得到保护, 难以逆操作恢复, 从而影响档案信息的安全。

## 二、大数据时代档案信息安全管理的要求

### (一) 转变管理观念, 紧跟技术进步

随着我国科技进步, 社会整体信息技术的水平不断提高, 大数据技术也被频繁地使用在各行各业中, 档案管理在新的信息技术的加持下, 信息安全管理技术也有了质的提升。作为管理层必须高度重视新技术对档案管理安全性的提升, 以紧跟时代新兴技术作为发展的首要目标, 主动将信息技术与大数据技术应用在档案管理安全中。这就需要优化管理手段作为管理理念, 将探索多元化、多样化的管理模式作为核心工作目标, 开发出适用于与大数据技术相适配的新型管理模式, 以此来保障档案管理的先进性与安全性, 最终达到安全管理与安全共享。

### (二) 保证档案信息资源的存储安全性

在数字化腾飞发展的时代, 网络信息技术不断加速更新迭代, 各行业对信息技术的需求促进了数字化档案

数量急速剧增，而海量数据又催生了“规模漏洞”，即数据越多、代码越多，防线越长，则可以攻击的漏洞就越越多。在黑客的攻击技术与攻击手段花样翻新，美国全球窃听窃密更是让国家层级黑客攻击大白天下。此外，对软件自身主观或客观存在的底层后门或技术缺陷导致的存储数据信息外泄，档案管理人员却束手无策。因此，档案信息数据资源存储作为档案安全管理环节中的重要环节，档案管理者一是必须根据自身发展状况，加强新型技术的学习，提高相关人才的引进与培养力度，并对管理理念与管理模式做出相应的优化与创新，充分提高档案数据的安全性；二是严格遵守信息安全规则，做到涉密档案管理避免外包，信息数据未经安全审查禁止外流，档案信息涉密设备严格限制使用权限，不使用外企设备设施及软件系统，数据库数据信息存储仅限国内等。只有严格遵循安全防护规则，才能尽最大限度降低档案信息资源存储风险。

### （三）技术上兼顾利用安全与利用效率的统一

通过对现代网络技术、信息技术与大数据技术的充分、科学、合理的使用，在众多档案软件秉承服务第一的，构建人性化的服务体系的设计开发理念下，为档案信息管理提供更多优秀的管理模式、便捷的操作方式和信息共享便利，为检索者提供更加便利的操作模式与质量更高的检索信息拓展关联，为档案信息赋予了更高的价值成为档案信息平台设计开发的首选项。然而，万物互联的多应用场景下催生档案信息价值最大化的同时，档案管理者必须兼顾信息安全设置与便捷管服的对立统一。必须在确保安全的前提下，为检索者提供检索便利、满足其在检索信息时的各项需求，是档案安全管理中的核心理念，即利用效率不应超出利用安全。要从信息检索平台底层设计上入手，做好接入方式、查询模式的安全设计，严格按照档案信息安全设置规则对信息检索使用设置不同程度、不同环节、不同验证，开发出安全性强、操作性强、实用性强的服务平台。

## 三、大数据时代档案信息安全管理存在的问题

### （一）网络安全技术不完善

档案信息资源管理工作中的资源整合与开发利用主要通过局域网与WEB网络两种媒介进行档案信息管理。两种网络下的管理模式虽都设置了一定的安全保护措施，但受网络高度开放特性的影响，档案信息资源仍容易受到各种恶意攻击，危害档案信息资源安全。与此同时，随着现代网络技术的不断创新与完善，新兴的技术病毒也使档案信息安全管理受到的恶意攻击类型逐渐增多。因此，若档案信息安全管理的安全技术止步不前，则会使档案信息的安全管理水平逐步降低，增加档案信

息资料出现窃取或泄漏等众多的安全隐患风险。

### （二）信息存储安全问题

我国档案信息管理经历了人工纸质文档存储、计算机磁盘、光盘和硬盘储存几个阶段。虽然每个阶段储存媒介的转变提高了档案信息资源存储的工作效率，也改善了档案信息资源的可移植性，但相较于传统的人工纸质文档的存储，仍存在部分缺点。其缺点主要体现于电子产品的存储方式会受产品的磨损率减少其使用寿命，从而为档案信息管理带了存储时间的制约性。此外，随着大数据技术的发展，海量的文档信息资源为存储工作带来巨大的挑战与压力，容易出现档案信息混乱和损坏的现象，进而影响档案信息资源存储的安全性。

### （三）非法访问问题

在传统的档案信息管理中，主要以管理实体文档为主，所以在其安全管理方面主要是对实体信息资料进行管理，大多以定期核查的方式检查全部的档案信息资料，进而确保档案信息资料的健全。而随着网络技术的不断升级，计算机非法访问的数量也随之增多，网络中的不法分子会通过非法访问的方式对档案信息进行偷盗与窃取。我国非法入侵网络的安全事件众多，深入剖析此类型事件的共同特点，可以发现其发生非法入侵事件的主要原因是由于众多档案信息管理工作人员对网络安全防范意识不足，计算机操作应用不熟练，致使电脑查杀软件安装设置不当、防火墙配置有误，WiFi热点公私混用，以及文档信息管理系统密码简单易破解等多方面问题，给不法分子的非法入侵提供便利条件，最终导致档案信息安全管理难以有效落实与应用，档案信息安全系数降低。

### （四）存在受到网络攻击的风险

网络技术的不断发展，为人们生活与工作提供了便利，但也带来了众多的网络威胁。而在档案信息安全管理过程中，也经常收到各种未知邮件和链接等各种形式的网络攻击，给档案信息的安全管理构成威胁。因此，如何提高档案信息的安全管理水平，降低档案信息管理受到网络攻击的风险是现在面临的重要问题。

## 四、加强企业档案安全管理措施

（一）制定完善的管理制度，推进档案安全管理制度规范化

在大数据背景下，档案管理以一种新的形式出现，如果规章制度的建立和完善跟不上发展的步伐。档案管理的效果就无法达到预期，档案信息的安全性自然也无法得到充分保障。因此，与传统档案管理相比，现代档案管理有着广阔的发展空间，但确保档案数据信息的安全不是一次性的任务，构建科学合理的档案信息安全管理制度的完善档案管理体系的重中之重。从某种程度上

来说,完善的安全策略与管理制度的信息系统安全性的根基。所以,无论是信息安全技术或信息安全管理策略都应将其视作核心进行选择及应用,若在信息安全管理策略方面出现漏洞,则一定会导致未来工作中出现纰漏或安全事故。由此可知,网络平台和信息系统的安全性与科学合理的管理制度之间存在必然的因果关系。在档案管理过程中,档案信息准入制度及监督管理制度是需优先考虑的问题,并以制度为标准、以制度为规范,实行严格的分级管理。有效的监管制度能防患于未然,并能更好的避免不作为或失职的行为,最终能够切实保护档案数据安全,有效提升档案管理水平及效率。

在充分了解网络技术对档案信息的安全保障能力后,应将该技术应用至档案管理工作中的各个环节。比如在日常通过网络信息系统办公并使用某些安全工具与技术手段时,应通过构建完善科学的相关管理制度对其进行约束,使其发挥出正确的作用与价值,避免因胡乱使用信息技术或网络技术造成的重要信息外漏或丢失。比如在编辑电子文件或进行数据档案备份时,应养成异地备份保管的习惯,避免因数据丢失而造成工作无法有效进展或影响工作质量。

## (二) 增加管理人员培训

现实中,不少档案管理人员习惯于传统档案管理,对档案信息化管理知识掌握有限,对信息安全与数据技术也是一知半解,不能完全胜任大数据背景下数字档案的管理工作。这就要求档案管理部门、相关单位主动加大对档案管理人员的档案信息化体系的培训力度,保证档案工作人员熟练地掌握信息技术,并运用到日常的档案管理工作中。培训的形式可以多种多样,可以是开座谈会现场交流,可以是远程指导在线核查,可以是行业培训在职进修,可以是内部学习督查考核。还可以考虑引进具有高信息技术水平的新员工加入到档案管理队伍,这样也能够提高系统的安全性。

(三) 提升新兴网络安全技术的应用,强化档案信息安全措施

档案信息安全管理涉及的相关安全技术应随着新兴网络技术同步发展,这样才能同步提高档案安全管理水平,保障档案信息资源的安全性。与此同时,不光要注重技术的同步,还应强化档案信息安全措施,参考国家相关法律以及政策规定,建立完善档案资料信息管理服务系统的安防规则与安防等级。其具体安全防护措施应包括对网络上的非法文件档案,以及重要涉密档案的严格审查与管理。并利用大数据安全技术,定期对档案信息安全管理系统进行安全升级,确保档案信息的安全存储、查阅与迁移。此外,还要不断完善档案信息安全应

急方案措施,确保在出现病毒、非法攻击等问题时能快速得到有效处置,保障档案信息资料等安全。

## (四) 建立档案数据库,保证档案信息安全

逐步完善档案信息数据库的建设是确保档案信息安全管理的基础与重点工作内容。在大数据时代背景下,档案信息数据库的信息资源内容与档案信息安全之间有着直接的联系。但受档案信息资源数量、类型以及结构复杂等特征影响,使档案信息数据库的搭建与维护较为复杂,也使数据库中档案信息数据的精准识别与挖掘变得困难。此外,随着大数据时代档案信息资源的大量涌现,传统的档案信息管理不足以支撑海量档案数据信息的安全。所以,通过网络技术建立数据库或大型数据中心是档案信息管理的重要工作内容之一,也是保障档案信息安全的必要手段。

## 结束语

概而言之,经上文的详细分析和阐释,我们可以了解到,在大数据时代下,海量的档案信息为档案管理工作增加了难度,也使档案信息的安全管理问题越来越受到重视。因此,为加强档案信息的安全管理,应进一步强化档案信息安全措施,利用新兴技术完善与升级档案数据库,同时制定全面的安全管理制度,增强网络防御能力,进而有效提高档案信息安全管理水平,促进档案信息管理的长期健康发展。

## 参考文献

- [1] 安安. 大数据时代档案信息安全管理策略探讨[J]. 兰台内外, 2021(25): 31-32.
- [2] 齐丽萍. 大数据时代档案信息安全管理策略研究[J]. 卷宗, 2020, 10(5): 90-91.
- [3] 袁少娟. 大数据时代档案信息安全管理要点探讨[J]. 科学与财富, 2021(18): 357, 375.
- [4] 喻平. 大数据时代档案信息安全管理探析[J]. 科技传播, 2020, 12(1): 118-119.
- [5] 袁少娟. 大数据时代档案信息安全管理要点探讨[J]. 科学与财富, 2021(18): 357, 375.
- [6] 程风刚. 大数据时代档案信息资源安全治理及其实现路径[J]. 盐城师范学院学报(人文社会科学版), 2020, 40(04).
- [7] 诸悦. 浅析大数据背景下的档案信息安全保障[J]. 电脑知识与技术, 2020, 16(05).
- [8] 林明香, 安一硕. “大数据”时代档案信息安全管理浅析[J]. 兰台世界, 2018(S2): 167.
- [9] 蒋爱军. 大数据时代下不动产登记档案管理信息化建设研究[J]. 山东农业工程学院学报, 2020, 37(10): 189-192.