档案安全体系建设研究

王维娜

（济宁市公路工程总公司，山东　济宁　272000）

摘　要：档案安全管理工作是档案工作的核心和重点，加强档案安全体系建设可以确保档案整体的安全，对于推进档案质量管理有着十分重要的意义。在目前的发展背景下，尤其是档案数字化管理的趋势，档案安全管理隐患较为复杂，信息安全威胁不断提升，给目前的档案管理带来了诸多的问题，因此必须从目前的管理实际出发，立足信息化发展的背景，加强档案安全体系数字化建设工作，提升档案管理的安全指数，满足人民群众生产生活的需求，推进经济社会的稳定安全发展。

关键词：档案安全；管理体系；措施

档案管理是一项专业且复杂的工作，需要对档案信息进行收集、鉴定、整理、保管等。还需要结合社会发展不断进行更新丰富，保障其准确性和参考性。档案不仅仅是重要信息的记录，更是企业发展的见证，对企业的发展有着重要作用。在信息技术快速发展的现代社会，企业档案管理工作基本完成了信息化建设，现今档案安全保障管理机制也面临新的挑战。只有了解档案安全保障管理的重要意义，并结合企业发展的实际情况，对其管理原则进行分析，才能真正保障档案管理的稳定性与长远性，系统性与全面性。通过科学构建组织管理机制，健全档案风险等级机制，增强安全管理应急机制，提高档案安全保障系数，促进管理工作新的变革。在保障质量的前提下，提高工作人员的工作效率，使档案安全保障管理工作朝着健康科学的方向发展。

1　档案信息安全

档案信息安全是指信息在产生、传输和使用过程中不被有意或无意地修改、泄露或破坏，包含信息自身安全和使用安全两个方面[1]。档案信息安全是档案信息真实、完整、可用的基础，是档案价值属性实现的保证。目前，影响档案信息安全的因素有外在环境、技术因素、人为因素、设施设备、人员素质等，如：误操作、人为故意操作、管理不善、软件漏洞、病毒攻击、软硬件设备不完善等不良因素，影响了数据的真实性、准确性，各业务系统软件不兼容导致信息无法读取，以及删除后没有任何痕迹的问题，而且传统的数据库只有一个中心服务器对数据进行维护，电子档案管理时面临着非授权访问、信息被窃取或篡改、数据完整性被破坏、利用网络传播病毒的威胁和信息存储的长久性问题等，需要从管理制度、法律规范、技术手段、人员选配等方面加强管理和建设。

2　档案信息安全面临的问题

2.1　数据传输安全

档案数据中心存储了海量的档案资源，部分档案信息的机密程度较高，如果泄露或损坏必然会带来非常严重的后果。基于云计算的档案管理工作，将档案信息资源利用网络传送到云计算服务商予以处理时表现出如下几个问题：首先是怎样保障档案信息数据在实际传输时受到有效保护，依靠各种加密技术确保其不会被窃取或篡改；其次是怎样保障云计算服务商获取档案信息后不会把相关数据信息进行泄露；最后是档案信息资源在云端存储状态下，怎样确保用户能够通过完善的权限认证确定其身份并为其提供相应权限的可获取档案数据。

2.2　软硬件的安全问题

数字档案安全管理需要保证载体安全与信息安全。载体安全是保证档案信息安全的基础。如果数字档案存储的硬件遭到破坏，数字档案信息不可避免地被损坏。从数字档案安全防控的整体趋势来看，需要不断提高档案的存储密度，延长存储设备的寿命，防止存储设备破坏对档案安全造成的整体性影响。数字系统的安全问题主要影响档案的运转安全，当信息系统出现错误时会导致档案服务出现瘫痪。档案管理系统主要包括了通信系统、操作系统等部分。通信系统采用有线连接和无线传输的方式进行数据传送。常见的窃取传输数据的方式就是搭线窃取数据，窃取者也可以通过架设接收器的方式来接收无线信号[2]。

2.3　数字档案自身存在信息安全问题

档案信息管理系统中主要有两种形式：第一种是因特网技术，这一技术的实施主要是传输，结合档案信息安全防范机制可以看出，对于其他的切入口防范制度并不完善。另一种是信息技术，这一技术就是档案信息进行数字化的一种方式，通过信息技术可以实现管理功能的提高。虽然信息系统本身结构具有一定的安全性，但信息盗取人员仍可以通过互联网或者是本地登录的方式侵入到档案信息管理系统。还有，数字化档案信息管理技术仍然存在一些缺陷，也需要不断完善和提高。

2.4　内部管理不当问题

过去传统的档案管理强调档案实体安全，对档案人员而言只要严格管理档案实体，就可以有效降低档案信息安全风险。而档案信息管理系统投入使用后，档案资源数字化、信息传递网络化所带来的新风险正逐步显现，其快捷处理、集成存储、传播迅速等优势都将放大档案信息泄露、丢失、损坏等安全问题的风险程度。这些风险问题人力完全难以掌控，成为档案人员在系统建设中长期忧心的顾虑，制约着档案信息管理系统的完善使用。

3　档案安全体系建设研究

3.1　梳理档案工作体系

档案信息管理系统的功能模块几乎可以覆盖档案管理工作全流程，其建设需要综合档案室提供档案管理工作各方面的信息作为支撑。为避免长时间、大范围调试修改，尽快使系统运作进入正轨，档案人员应在建设前期对本单位档案工作体系，包括档案制度、档案分类、档案工作网络等进行全面梳理。具体来说，需要明确本单位所涉及档案类型和相对应档号规则、著录信息项、目录报表及档案管理各环节的工作流程、档案管理工作角色设置等来确定系统内基本框架如何搭建，使之规范化、标准化，才能在初期系统建设中基本达成预期的需求目标。同时档案人员也应注意，在使用档案信息管理系统后是否存在和原有的档案相关制度、移交利用等工作流程相冲突或未纳入的地方并及时修改补充，保证管理系统运行下的档案管理工作能合理合规进行[3]。

3.2　电子信息生态环境建设

在电子档案管理中，电子信息生态安全环境建构最重要

的是安全技术问题。纸质档案查询需要到档案管理所在地实地查询，而电子档案则可以通过互联网方式进行查询。大部分电子档案管理机构都实现了联网工作，可以通过在线方式收录档案与查询档案，这种方式虽然提高了档案管理效率，但是也造成了某些信息安全隐患。在现实中，利用信息技术手段入侵电子档案管理系统，篡改、窃取或泄露各种电子档案信息，给电子档案安全构成威胁，甚至造成无法预料的损失。电子档案管理系统一定要加强信息安全技术研发应用，构建防护等级更高的信息防火墙，防止别有用心的人入侵档案管理系统，确保电子档案信息能够得到充足的安全保护。在电子档案信息环境安全生态构建中还应注意电磁环境的防护，电子档案系统若是处于不合适的电磁环境中，也可能会对安全防护系统造成冲击，从而导致档案数据被破坏或丢失等问题[4]。

3.3 构建云计算安全评估和监管体系

档案管理部门要积极主动和云计算供应商进行沟通联系，委派档案管理人员成立安全评估作业小组，建立完善系统的安全评估方案，明确安全评价指标。应当对云计算环境下的档案信息资源安全状态实施全面监管，对可能出现的风险予以准确评估，同时风险出现后可以第一时间实施有针对性的处理对策。安全评估作业小组要基于评价指标对档案存储风险实施不定期检查，得出准确客观的安全评估工作报告，在其中清楚标注云计算环境下档案存储的安全风险，同时给出有针对性的处理建议，确保安全漏洞与风险能够及时解决[5]。

3.4 加强档案法规的建设

目前，要积极修订数字化档案的管理办法，制定更加科学的数字档案建管标准。例如，出台与数字档案建设相关的标准、流程、法规、制度，细化数字档案管理的基本要求，明确数字档案管理的具体分工。进一步加强现行数字档案制度分析，根据已经暴露的问题修订档案数字化建设制度问题，从而解决数字档案建设过程中的具体问题。数字档案信息化建设应当有法可依，做到各项规章制度与法律法规间的良好配合，保证制度建设逻辑的合理性，从而依托更加简明扼要的规范制度提高数字化档案建设管理水平。

3.5 基于第三方权威认证机构的可信云服务认证

基于第三方权威认证机构的档案数字资源可信云服务认证，可以建立档案机构对云服务商的信任，减少选择的盲目性，从而降低筛选成本。为更好地服务档案机构，需要组织开展面向档案数字资源的可信云服务认证，通过第三方权威认证机构对云服务商进行安全评估和认证。地方档案机构应基于工业和信息化部公布的云计算通用可信云服务认证名单，积极与相关云服务商开展面向档案数字资源的可信云服务认证。首先，参与档案数字资源建设的云服务商须获得工业和信息化部可信云服务认证，并向国家档案局下设的档案信息安全统筹监管职能部门提出评估认证请求，将云服务相关信息（包括基本特征、平台、服务器、网络、应用、服务可用性和稳定性等）和云服务商基本信息认证（包括基本信息、人员和财务情况、资本关系、组织结构等）向监管部门及时汇报。其次，统筹监管职能部门委托由档案领域、云服务行业组织、协会及其他权威专家组成的第三方安全评估认证机构进行考评认证。再者，第三方安全评估认证机构根据档案数字资源可信云服务认证标准对云服务商进行全面考评，并将考评结果提交给信息安全统筹监管部门。最后，档案信息安全统筹监管职能部门对第三方考评结果进行审核，审核通过后对符合资格的云服务商进行可信认证授权，颁发可信云服务认证资格证明[6]。

3.6 应用区块链技术应用落地的对策

应该清醒认识到，世界上没有绝对完美无瑕的事物，技术是一把双刃剑，既可创造价值，也可被恶意利用带来灾难。区块链的应用层通常是被恶意攻击的目标，近年来全球发生的多起数字货币交易平台被黑事件就是很好的警示。从技术原理上来讲区块链技术近乎完美，能够应用于众多领域，但是区块链自身存在着区块容量有限，能耗高，节点越多消耗的计算成本越高速度越慢，多种算法各有特长和弊端等劣势，它只能保证线上交易的可靠，无法控制线下行为，以及受社会习惯、人们理念、接受能力、职业素养和计算机技术高速发展等的制约，其安全问题仍日显突出，为此要加强基础建设、技术开发和防控监管。

3.7 数字档案信息资源的异地备份

对于档案信息的异地备份，就是指将一些重要的数据资源，在另外一个地方的存储空间形成一个副本，如果在本地数据发生危险时，可通过这个副本进行系统的重建工作。档案信息资源及存储的方式中会用到异地备份，随着我国科学技术水平的逐渐提高，更多的信息以计算机为媒介进行公布以及储存，在运行中会受到外界环境的影响，甚至导致大量信息数据受到损坏，在这个时候数据备份就显得尤为重要。

3.8 数字档案信息资源的辅助存储池备份

档案信息资源的存储介质也就是计算机的应用系统，是辅助储存方式中的一种重要策略，云备份是一种现代档案信息存储方式，通过虚拟存储空间利用实体计算机硬件系统，实现数据的收集以及备份辅助存储池，就是针对档案信息资源的主要存储中心建立在一个分散储存场。在整个档案信息的存储中各个分支机构或者是管理部门主要是围绕这一主题展开的。作为中心存储机构其信息储存量是非常大的，在这个储存的过程中，中心位置扮演着决定性的作用，通过对周围分散机构下达对应的指令以及有效控制措施，最终加强各个数字档案信息有效管理。

4 结语

总之，造成数字档案安全隐患的原因是多方面的，现代数字档案管理工作面临的环境是复杂的，还要从档案数字化建设的现状出发，拟定档案数字化建设的综合计划，明确档案数字化安全防控的重点，着力加大软硬件的投入力度，形成先进的安全管理规范，不断更新技术防范方法，从而提高数字档案安全控制的有效性，解决档案数字化建设中的问题，达到全面提高数字化档案质量目标。

参考文献

[1] 闫冬 . 电子档案存档的问题及应对策略研究 [J]. 兰台内外 ,2020(36):32–33.

[2] 周林兴 , 韩永继 . 档案数据安全治理能力成熟度模型构建研究 [J]. 中国档案 ,2020(12):79.

[3] 史秀波 . “互联网 +”时代高校档案信息化管理的探讨 [J]. 白城师范学院学报 ,2020,34(6):126–128.

[4] 秦迎春 . 新时代档案信息化工作的探讨 [J]. 兰台世界 ,2020(S2):6–7.

[5] 张北建 , 孙立业 . 区块链技术在档案信息安全中的应用探讨 [J]. 黑龙江档案 ,2020(6):76.

[6] 王莎白 . 医院档案管理中的安全问题 [J]. 办公自动化 ,2020,25(23):55–56+29.