

数字档案馆环境下档案信息安全保障

周贝贝

滨州市滨城区档案馆

[摘要]随着社会的发展,传统的纸质档案管理出现了越来越多的问题,信息技术的广泛应用为档案管理带来了新的方法和策略。电子档案的发展时间远短于纸质档案,其面临的安全问题也比纸质档案复杂。因此,探索电子档案安全管理系统的构建方法,对保障电子档案的安全具有重要意义。实现电子档案的长远发展必须解决的问题。数字档案面临的安全问题日益突出,呈现出与数字档案相关的软硬件、环境和内部控制等问题,对数字档案的使用构成威胁。为提高数字档案的质量和效率,需要加强档案数字化的安全建设,针对档案数字化中存在的实际问题采取有效措施。

[关键词]档案数字化; 安全防控; 应对措施

[DOI] 10.12252/j.issn.2096-627X.2021.09.477

1 前言

从我国近年来数字档案信息管理的现状来看,虽然其管理指标呈上升趋势,但整体管理质量却不尽如人意,尤其是在风险管理方面,容易受到各种因素的影响,如由于存储环境、管理理念、管理技术等因素,从而影响最终的风险管理效果。这在一定程度上会给用户带来麻烦,严重的甚至会损害国家利益。因此,从整体安全的角度,不断加强数字档案信息的管理势在必行。

2 数字化档案安全的相关概念

2.1 数字档案管理的特点

数字档案是依托信息技术而存在的电子化、数字化、信息化档案。数字档案除了具有一般的信息记录价值外,还可以依托网络媒体发挥作用,呈现出不同于传统档案的特点。例如,数字档案的存储密度更高,档案可以存储在较小的载体上。可以将数字文件载体与信息分离,利用信息技术提取和使用数据信息。此外,数字档案具有易于复制的特点。如果没有其他标准限制,数字档案的原件就不是唯一的。数字文件易于修改,可以使用不同的载体多次读写。作为一种传递效率更高、存储形式更多样化的文件形式,数字文件管理难度更大,安全风险更高。数字档案是信息技术飞速发展的产物,对各行各业的发展起到了重要的支撑作用。在共享思维的影响下,构建了更加优质的档案信息交流环境,可以发挥档案在决策支持、信息供给和数据分析等方面的作用。数字档案冲击了传统的档案理念,强调采用规范、科学的档案管理方法,构建完整的档案运行体系,确保档案的广泛共享和有效控制下的应用。

2.2 数字档案安全的目标

数字档案安全管理的主要任务是确保数字档案的可用性,构建完整的档案安全体系,将技术与管理相结合,防止档案被意外或外部恶意泄漏、损坏或篡改。数字档案安全管理的主要目标是确保数字档案能够有序运行,档案信息完整可用。一方面,要防止文件信息泄漏,防止在互联网上传输的应用程序文件被非法盗窃,防止文件本身受到损害。另一方面,保证档案信息不失真,保持档案原始信息记录的真实性。在信息化环境

中,还需要保证档案的完整性,满足信息使用者对档案的使用需求,实现档案生命周期内相关数据信息的完整性。数字档案不同于一般档案,它可以在互联网环境下高速运行,可以通过查询系统进行间接管理、查询、阅读和利用。数字档案要保证强大的可用性,体现档案的数字信息价值,更好地利用数字档案信息。

3 现阶段数字档案信息风险管理中存在的主要问题分析

3.1 数字档案信息风险管理理念有待更新

目前,部分档案管理单位在实施数字档案信息风险管理时仍沿用传统的管理理念,具体体现在以下三个方面:一是部分档案管理单位仍采用传统的纸质档案管理模式进行管理。数字档案信息。管理层认为,只要对数字档案进行备份,更换存储介质,就可以保证数字档案的安全。这种错误的认知不仅会降低数字档案信息的管理质量,还会对其实际使用带来诸多不利影响。其次,虽然一些档案管理单位会采用先进的软件技术来管理数字档案信息,但在相关管理系统的建设中却极为忽视,导致数字档案信息在管理过程中往往无法依靠。糟糕的情况不仅会降低档案信息的安全性和利用率,而且会给用户的切身利益带来很大的风险,特别是那些属于机密的档案信息或数据,如果不按照国家保密要求进行安全存储,将造成严重后果,给国家利益造成巨大损失;最后,一些档案管理单位缺乏协同管理意识,在管理数字档案信息时无法加强与其他部门的合作,认为只要加强自身档案管理的技术水平,更新管理方式就能提高应用价值。数字档案信息。相对而言,智能化和信息化建设被极度忽视,这将在一定程度上大大降低数字档案信息风险管理的效率,进而使数字档案信息在存储和利用过程中面临更大的网络安全风险。

3.2 数字档案信息风险管理体系有待完善

目前,我国针对数字档案信息安全管理制定的相关管理制度还存在诸多不完善之处,尤其是数字档案信息管理体系建设方面,并未全面涵盖内容、组织、技术等方面。数字档案信息管理、以及载体等方面,这将在很大程度上增加数字档案信息的管理难度,并使部分信息经常面临被黑客攻击的风险。

例如,由于目前对数字档案信息的归档范围、保存期限、转换标准、转换环境等都没有明确的规定,这就为不法分子利用不正当手段盗取一些重要的数字档案信息提供了可乘之机,给人民利益和国家财产造成巨大损失。

3.3 数字档案信息风险管理方式有待创新

在数字档案信息的产生、流通、传输、存储和利用过程中,由于是在开放的计算机和网络环境中进行的,极易受到病毒攻击和黑客攻击,进而造成数据丢失、非法拦截并发生盗用现象。虽然相关管理单位会采取相应的技术措施来控制 and 预防这些问题,例如:防火墙技术、数字签名技术、数字认证技术、网络监控技术等。但是,随着数字档案的形式和种类越来越多并且更加多元化和个性化,如果这些安全风险技术不及时更新,势必与当前数字档案信息风险管理的要求背道而驰。此外,缺乏高精尖数字档案风险管理人才也是数字档案信息风险管理水平低的重要原因之一。

4 确保数字档案信息安全保障的策略

4.1 加强信息安全保障机制的建设,提高治理水平

4.1.1 建立健全数字档案信息保障体系

根据国家颁布的相关法律和条例,建立一个的信息安全系统,以确保数字信息的安全。应实施与信息安全有关的法律和条例,如《中华人民共和国档案法》、《中华人民共和国国家安全法》、信息安全保护管理系统和国际计算机信息网络安全管理系统。在处理具体事件时,正在建立牢固的安全屏障。此外,应当建立一个永久和有效的信息安全系统,以确保所保存信息的可靠性、完整性、可得性、保密性和其他收集、分类和使用;培养公法知识使用方面的良好习惯。

4.1.2 开发数字档案档案的共同系统

标准管理是推进档案进程的基础。档案部门应根据相关国家法律和条例的规定,制定更严格的监管制度和措施,使其符合其实际工作,如数字流程管理、存储媒体管理、电子文档传输、接收管理和电子文件元数据管理。

4.2 利用相关安全技术,提高保障能力

做好技术层面的工作,采用新型的技术手段构建档案信息安全保障体系,是保护档案信息安全的關鍵。

4.2.1 做好软件安全保障工作

软件是计算机系统的核心,必须严格控制这一过程,并在整个开发过程中引入安全和安保概念。第一,根据档案的实际运作选择档案管理系统的类型,将能够有效地整理所保存的信息和数据,并充分利用这些信息和数据。第二,引入了安全防范安全风险的安全保护软件。第三,根据使用保存的信息改进和开发新的功能软件。

4.2.2 加强信息安全技术领域的协同作用

在各级采用适当的技术手段,加强保护信息安全风险的保护。首先是数据加密,通过公开密码获得原始数据。第二是电子签字技术,该技术核查用户身份并确保信息的完整性。第三是水印技术。有水印的信息是安全的,从而减少了篡改或伪造的情况。第四,穿透探测技术可以通过探测未经授权的用户来防止黑客。第五,安全审计技术,以便有效发现网络安全漏洞和改进系统完整性。六是备份技术。为了防止丢失档案数据,应加强档案数据的保存工作,以确保档案资料的安全管理。

4.3 敦促档案工作人员继续改进信息并维持安全

人是一切的本質。在信息安全問題日益增加的時候,應通過加強安全基礎來提高對檔案人員安全責任的認識。

4.3.1 提高對檔案信息處工作人員安全責任的認識

檔案工作人員是檔案管理的主题。檔案工作人員對因特網環境的責任感和安全管理日益增強。這是負責多個層次的安全和安保系統,並有專門的安保管理人員,以確保問責制,嚴格遵守安全的紅線,定期進行保密和安全培訓,對工作人員進行安全教育,提高他們對安全責任的認識。

4.3.2 優化信息服務人員的知識結構,提高安全防範能力

信息時代對檔案館工作人員提出了更大的要求。為了確保妥善管理保存的信息,必須改進檔案工作人員的知識結構,並建立培訓檔案工作人員的長期機制。第一,應加強關於檔案安全的知識、信息學專業的理論、仔細分析案件、總結經驗教訓以及加強識別和發現風險的能力。第二,檔案管理員應熟悉相關管理程序,並掌握操作各種信息安全設備的技能。第三,檔案管理員積極參與技能培訓,並不斷努力提高他們的職業資格,以適應時代的需要。

5 結語

我國社會經濟水平在不斷提升,這就要求檔案事業要適應新發展形勢,抓住新發展機遇。同時,放眼全世界,在信息化背景下,信息技術的應用使檔案的載體形式發生了巨大的變化。檔案信息化建設需要進一步提高,這不但有益於公開檔案信息和共享檔案資源,還對檔案信息安全的 yêu求更加嚴格。檔案信息安全作為檔案工作之底線,無疑是檔案工作之根基,決不容忽視檔案信息安全工作,紅線意識必須強化,確保檔案信息資源的管理和使用有序、完備。

參考文獻

- [1] 齊峰. 數據時代檔案信息安全保障策略研究[J]. 智能城市, 2019(09): 27-29.
- [2] 蘇秀梅. 關於構建數字檔案信息安全保障體系的思考[J]. 科技展望, 2020(10): 40-41.
- [3] 黃偉明. 檔案信息安全體系建設思考[J]. 辦公室業務, 2019(09): 12-13.